МАТЕМАТИЧНІ МЕТОДИ В СУСПІЛЬНИХ І ГУМАНІТАРНИХ НАУКАХ

DOI: 10.31319/2519-8106.1(42)2020.207015
УДК 004:048
К.М. Ялова, к.т.н., доцент, yalovakateryna@gmail.com
К.В. Яшина, к.т.н., доцент, yashinaksenia@gmail.com
В.О. Коротка, магістр кафедри програмного забезпечення систем
Дніпровський державний технічний університет, м. Кам'янське

НЕЙРОННА МЕРЕЖА ДЛЯ КРИПТОГРАФІЧНОЇ СИСТЕМИ З ВІДКРИТИМ КЛЮЧЕМ

У статті наведено результати розробки нейронної мережі типу багатошарового персептрону, яка використовується для збільшення швидкості шифрування та дешифрування інформації в криптографічній системі з відкритим ключем на прикладі криптографічної системи Ель-Гамаля. Представлено результати моделювання роботи криптосистеми Ель-Гамаля на матричних групах із використанням нейронної мережі і без неї. Здійснено співставлення швидкості шифрування та дешифрування криптосистеми. Обґрунтовано доцільність застосування нейромережевого алгоритму для підвищення швидкодії криптосистеми. Середнє прискорення шифрування із застосування нейронної мережі склало 5%, розшифрування — 11 %.
***Ключові слова**: нейрокриптографія; криптосистема Ель-Гамаля; нейронна мережа; багатошаровий персептрон.*

The results of multilayer perceptron neural network development and its using for increasing of the information encryption and decryption speed in the public-key cryptographic system are presented in the article. The results of the El-Hamal cryptosystem on matrix group operation modelling with the use of a neural network and without it are described. Comparison of the El-Hamal cryptosystem encryption and decryption rate is performed. Expediency of the neural network algorithm using for improving cryptosystem speed is substantiated. The average acceleration of information encryption using the neural network is 5%, the average acceleration of information decryption is 11 %.
***Keywords**: neural cryptography; El-Hamal cryptosystem; neural network; multidimensional perceptron.*

Постановка проблеми

Криптографія — це технологія, основна мета якої надати інформаційну безпеку для комунікації або комп'ютерних систем, яка передбачає перенесення даних до шифрованого коду, що може бути переданий по відкритому чи закритому каналу передачі даних із подальшим дешифруванням [1].

Криптосистеми з відкритим ключем характеризуються тим, що відкритий ключ передається по незахищеному каналу і застосовується в подальшому для перевірки електронного підпису і шифрування даних [2]. Створення електронного підпису або розшифрування повідомлення здійснюється із використанням закритого ключа. Криптосистеми можуть будуватися на основі симетричних шифрів, як то: AES (Advanced Encryption Standard), DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) тощо, і асиметричних шифрів, наприклад: RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm), шифр Ель-Гамаля (El

Hamal Cryptosystem), шифр обміну ключами Діффі-Хелмана (Diffie-Hellman), ECDSA (Elliptic Curve Digital Signature Algorithm) [3]. Основна відмінність симетричних і асиметричних шифрів полягає в тому, що для симетричного шифрування використовується один ключ, а для асиметричних — два пов'язаних між собою ключа. Кожний із шифрів має свої особливості та галузі застосування, переваги і недоліки використання.

Необхідність підвищення якості та надійності криптосистем і стрімкий розвиток інформаційних технологій сприяли впровадженню нейромережевих алгоритмів до криптографії. Останнім часом криптографія, як технологія, що використовує нейронні мережі (НМ), стає дедалі популярнішою. Галузь науки, яка досліджує способи застосування стохастичних алгоритмів, НМ для криптоаналізу та шифрування даних називають нейрокриптографією [4]. Основною метою застосування НМ у криптографічних системах є підвищення ефективності їх функціонування та зменшення часу, необхідного для шифрування та/або дешифрування даних або створення електронного підпису, підвищення стійкості до атак та криптоаналізу. При цьому використовуються такі властивості НМ як: взаємне навчання, самонавчання, стохастична поведінка і низка чутливість до шуму і неточностей [5]. Застосування НМ для реалізації криптографічної системи дозволяє отримати наступні переваги:

– зменшення часу шифрування/дешифрування: швидкодія НМ більше залежить від її архітектури, ніж від вхідних даних;

– ускладнення визначення закритого ключа за ваговими коефіцієнтами НМ, а в деяких випадках відсутність можливості встановлення алгоритму шифрування;

– ускладнення пошуку вразливостей криптосистеми: кожний нейрон містить у собі малу частину інформації необхідної для точної роботи криптосистеми, тому для її взлому необхідно проаналізувати всі частини НМ.

Аналіз останніх досліджень та публікацій

Основоположниками криптографії вважаються У. Діффі та М. Хеллман, які в 1976 році дали опис та задали властивості для криптографічних систем із відкритим ключем, що знайшли застосування в завданнях розробки електронного підпису, шифрування повідомлень та застосовуються в мережевих протоколах для захисту даних. Криптосистему з відкритим ключем Ель-Гамаля було розроблено в 1985 році, її було покладено в основу ряду систем шифрування та створення цифрового підпису, які застосовуються і тепер.

Ідея застосування НМ для реалізації алгоритмів шифрування вперше була втілена С. Дроленсом у 1995 р., коли він розробив НМ для інвертування S-перестановок у шифрі DES. Такі науковці, як: Червяков Н. І. Євдокимов А. А., Галушкин А. І., Лавриненко А. В., Лавриненко І. Н., Laskari E. C., Meletiou G. C., Stamatiou Y. C., Vrahatis M. N. [5-6] та інші присвятили свої роботи дослідженню проблем та переваг застосування НМ у криптографічних системах. Етапи та тенденції розвитку нейрокриптографії досліджуються в роботах Куперштейна Л. М., Татарчука А. Є. [7]. Задачі проектування НМ, ефективного застосування нейронномережевих технологій для задач криптографії, підвищення криптостійкості систем та аналіз впливу НМ на цю властивість досліджуються в роботах таких авторів, як: Авдошин С. М., Савельєва А. А., Гридін В. Н., Солодовников В. І. [8-9] та інших.

Формулювання мети дослідження

Не зважаючи на велику кількість наукових робіт та науковців, які присвячують свої дослідження питанню ефективного застосування НМ різного типу в криптоситемах, це питання потребує подальшого розвитку та залишається актуальним науково-практичним завданням сучасної науки. Основною метою даної статті є опис результатів розробки та застосування НМ для системи з відкритим ключем на прикладі криптосистеми Ель-Гамаля (КЕГ). Для досягнення мети дослідження були здійсненні наступні етапи роботи: розроблено архітектуру НМ для реалізації КЕГ; програмно реалізовано спроектовану НМ; проведено навчання та тестування отриманої НМ; створено програмне забезпечення й інтерфейс користувача для моделювання роботи КЕГ із різними вхідними значеннями із застосуванням розробленої НМ та без неї; проаналізовано отримані дані щодо швидкодії КЕГ.

Виклад основного матеріалу

КЕГ є представником асиметричного відкритого шифрування і може використовуватися як для шифрування повідомлення, так і для створення цифрового підпису або узгодження загального ключа. Для організації такої системи створюється закритий (секретний) і відкритий ключі, значення яких пов'язані між собою, але обчислити закритий ключ із відкритого практично неможливо [10]. КЕГ базується на властивостях дискретного логарифму, її основною перевагою є відсутність необхідності попереднього передавання секретного ключа по захищеному каналу зв'язку, крім того в ній відсутня можливість підробки цифрового підпису під деяким повідомленням без визначення закритого ключа. Основними етапами реалізації КЕГ є генерування пар ключів, здійснення шифрування та дешифрування повідомлення. Узагальнений алгоритм генерації ключів складається з наступної послідовності дій:

1. Генерування випадкового простого числа p довжиною n біт.

2. Визначення довільного цілого числа a, яке є примітивним коренем по модулю числа p. Числа a і p можуть передаватися у відкритому вигляді і бути узагальненими для всіх користувачів каналу зв'язку.

3 Визначення випадкового числа x із інтервалу $(1, p)$, яке є взаємно простим із $p-1$.

4. Обрахування $y = a^x \pmod p$, де y — відкритий ключ, x — закритий ключ.

Узагальнений алгоритм шифрування вхідного повідомлення m, сформованого першим користувачем, містить такі кроки:

1. Вибір випадкового числа k для першого користувача, яке є взаємно простим із $p-1$.

2. Створення шифротексту (r, e) для передавання другому користувачу, де $r = a^k \pmod p$, $e = m \cdot y^k \pmod p$.

Узагальнений алгоритм дешифрування повідомлення містить наступні кроки:

1. Отримання шифротексту (r, e) другим користувачем.

2. Визначення вхідного повідомлення за формулою $m = r^{-x} \cdot e \pmod p$, враховуючи, що $m = e \cdot r^{p-1-x} \pmod p$.

Основна ідея методу шифрування Ель-Гамаля полягає в тому, що не існує ефективного методу порівняння $a^x == b \pmod p$. Класичний опис цієї системи передбачає застосування мультиплікативних груп кінцевих полів простого порядку, що робить цю систему вразливою. Для підвищення якості КЕГ в роботі [11] пропонується застосовувати матричні групи, де G — матрична група порядку n, яка створюється елементом g, а x — елемент G, де елемент m із Z_n є логарифмом елемента матричної групи.

Оскільки реалізація асиметричного шифрування потребує значних обчислювальних ресурсів, то підвищення швидкості шифрування/дешифрування може реалізовуватися, наприклад, за рахунок застосування НМ [5]. Використання НМ дозволяє реалізувати незалежну паралельну обробку кожного символу вхідного повідомлення, яке необхідно зашифрувати. Для реалізації КЕГ із застосуванням НМ обрано модель багатошарового персептрону (multi level perseptron) (рис. 1), який є мережею прямого поширення з можливістю емулювання будь-яких співвідношень входів та виходів.

Перевагами застосування саме багатошарового персептрону є можливість безпечного обміну інформацією і отримання загального ключа користувачами каналу зв'язку [12]. Вхідними умовами для організації багатошарового персептрону є наступне:

– закритий ключ не повинен бути доступний або обчислений з проміжних значень НМ;

– заключні ваги не повинні бути доступними для обчислення з проміжних ваг НМ, навченої за індивідуальними ключами;

– для навчання НМ можливо отримання однакових вагових коефіцієнтів незалежно від порядку використання закритого ключа.

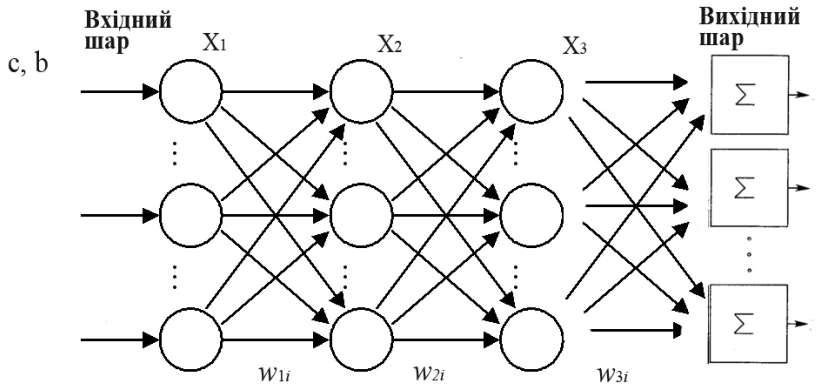

Рис. 1. Структура багатошарового персептрону

Структура багатошарового персептрону для КЕГ буде мати вигляд, як це показано на рисунку 1 і складатися з вхідного шару $n \times k$ нейронів, двох проміжних шарів із n і k нейронів та вихідного шару з n нейронами. Беручи до уваги підхід застосування матричних груп із роботи [11] та впроваджуючи НМ типу багатошаровий персептрон, можна звести алгоритми етаетапів реалізації КЕГ до наступного:

Генерація ключів:

1. Генерування k випадкових простих чисел t_i лінійної матричної групи $T = \prod_{i=1}^{i=k} t_i$, $G = GL_n(Z_m)$, $1 \le i \le k$, $T \ge m$.

2. Обрання матриці a порядку p, де $a \in G$.

3 Визначення випадкового цілого числа x з інтервалу $(1, p-1)$.

4. Формування відкритого ключа (T, a, a^x) і закритого ключа x.

Шифрування повідомлення B, яке передається у вигляді матриці, буде здійснюватися за наступними кроками:

1. Вибір випадкового числа r_i, в якості сеансового ключа.

2. Створення НМ для обчислення c і b в $GL_n(Z_{t_i})$.

3. Обчислення значень першого шару X_1 НМ $c = a^{r_i}$, $b = Ba^{xt_i}$. Ваги першого шару — це одиничний вектор.

4. Обчислення ваг другого шару НМ здійснюється за формулою [11]:

$$w_{2i} = \frac{X_1}{X_{1i}} \cdot \left(\left(\frac{X_1}{X_{i1}} \right)^{-1} \bmod X_{1i} \right). \tag{1}$$

5. Обчислення значень другого шару НМ здійснюється наступним чином:

$$X_2 = w_{2i} \cdot X_{1i}. \tag{2}$$

6. Обчислення значень вихідного шару НМ відбувається за допомогою формули:

$$X_3 = \sum_{i=1}^{i=k} w_{3i} \cdot X_{2i}. \tag{3}$$

Ваги третього шару — одиничний вектор. Отримання значень матриць c і b з елементів $GL_n(Z_{t_i})$.

7. Створення шифротексту F, який представляється у вигляді матриці $F_{n \times 2n}$ в G, де:

$$F = \begin{bmatrix} c_{11} & \dots & c_{1n} & b_{11} & \dots & b_{1n} \\ \dots & & \dots & \dots & & \dots \\ c_{n1} & \dots & c_{nn} & b_{n1} & \dots & b_{nn} \end{bmatrix}.$$

Дешифрування повідомлення B відбувається наступним чином:

1. Отримання шифротексту F другим користувачем.

2. Створення матриць c і b з елементів матриці $F_{n\times 2n}$:

$$c = \begin{bmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ \dots & \dots & \dots & \dots \\ f_{n1} & f_{n2} & \dots & f_{nn} \end{bmatrix}, \qquad b = \begin{bmatrix} f_{1n+1} & f_{1n+2} & \dots & f_{12n} \\ f_{2n+1} & f_{2n+2} & \dots & f_{22n} \\ \dots & \dots & \dots & \dots \\ f_{nn+1} & f_{nn+2} & \dots & f_{n2n} \end{bmatrix}.$$

3. Формування НМ для обчислення $\left(c^x\right)^{-1}$ в $GL_n\left(Z_{t_i}\right)$.

4. Обчислення значення першого шару X_1 НМ, де $X_1 = \left(c^x\right)^{-1}$. Ваги першого шару — це одиничний вектор.

5. Обчислення ваг другого шару НМ за формулою (1). Обчислення значень другого X_2 і третього X_3 шару НМ за формулами (2)-(3).

6. Формування НМ для обчислення b в $GL_n\left(Z_{t_i}\right)$.

7. Визначення значення першого шару X_1 НМ, де $X_1 = b\left(c^x\right)^{-1}$. Ваги першого шару — це одиничній вектор.

8. Обчислення ваг другого шару НМ за формулою (1). Обчислення значень другого X_2 і третього X_3 шару НМ за формулами (2) — (3).

Для реалізації НМ та моделювання роботи КЕГ було розроблено програмне забезпечення засобами мови програмування PHP. Функціональність розробленого програмного застосунку полягає у виконанні наступних дій: введення повідомлення для шифрування; шифрування повідомлення на основі КЕГ із застосуванням НМ та без неї на вибір користувача; фіксування швидкості шифрування та дешифрування вхідного повідомлення; формування звітної інформації стосовно швидкодії КЕГ.

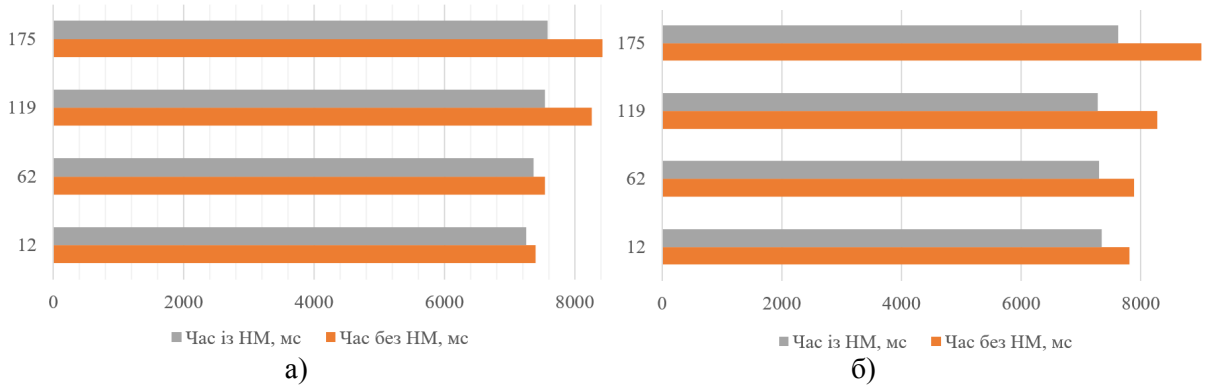

Рис. 2. Моделювання роботи КЕГ: а — шифрування; б — дешифрування

Результати моделювання роботи КЕГ надали можливість обґрунтувати перспективність застосування НМ типу багатошаровий персептрон для підвищення швидкості шифрування та дешифрування вхідного повідомлення. На рис. 2 наведено результати моделювання КЕГ на матричних групах із застосуванням розробленої НМ та без неї. Для отримання порівняльних да-

них моделювання здійснювалося серіями з однаковими значеннями відкритого $\left(T, a, a^x\right)$ і закритого x ключів, з різним об'ємом та символами вхідного повідомлення.

На рис. 2а наведено результати порівняння швидкості шифрування даних, а на рис. 2б — результати порівняння швидкості розшифрування вхідного повідомлення. З наведених на рис. 2 даних можна сформулювати наступні висновки:

1) Характеристики швидкості шифрування/дешифрування КЕГ із застосуванням НМ і без неї відрізняються несуттєво для випадків, коли вхідне повідомлення має невеликих розмір або містить невелику кількість символів.

2) Зі збільшенням обсягу вхідного повідомлення збільшення часу обробки даних відбувається не пропорційно, а система із НМ демонструє кращі показники швидкості шифрування/дешифрування даних.

3) Застосування НМ дозволяє прискорити процес створення ключів криптосистеми.

4) Середнє значення прискорення роботи криптосистеми з використанням НМ складає 5% для процесу шифрування і 11% для процесу дешифрування.

Висновки та перспективи подальших досліджень

Застосування відкритих алгоритмів шифрування дозволяє не організовувати секретних каналів зв'язку для попереднього обміну ключами і мінімізувати взломи шифру. Переваги застосування криптосистем із відкритим ключем базуються на складності обчислення логарифмів [8]. У представленій роботі описано результати розробки багатошарового персептрону, який використовувався для реалізації КЕГ на матричних групах. Розроблена НМ складається з трьох шарів та використовує сигмоїдну функцію активації. Для оцінювання ефективності застосування НМ у КЕГ було розроблено програмне забезпечення із інтерфейсом користувача, що дозволяє задавати вхідне повідомлення та фіксувати час процесу шифрування та дешифрування в КЕГ із використанням НМ і без неї. Результати моделювання роботи КЕГ підтверджують доцільність і перспективність застосування нейронномережевих алгоритмів для криптосистем.

Окрім параметрів швидкості шифрування та дешифрування основним якісним показником криптосистеми є її стійкість до атак та небажаних втручань. Питання аналізу криптостійкості КЕГ, яка реалізовується із застосуванням НМ, оптимізація архітектури розробленої НМ, наприклад за рахунок додавання згорткових шарів, є завданням подальших наукових розвідок .

Список використаної літератури

1. Mao W. Modern Cryptography: Theory and Practice. New Jersey: Pearson Education, 2005. 768 p.
2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004. 173 с.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.
4. Protic D.D. Neural cryptography. *Military technical courier*. 2016. Vol. 64. № 2. P. 483–495.
5. Laskari E.C., Meletiou G.C., Stamatiou Y.C., Vrahatis M.N. Studying the performance of artificial neural networks on problems related to cryptography. *Nonlinear analysis: real world applications*. 2006. №7. P. 937 — 942.
6. Куперштейн Л.М., Татарчук А.Є. Аналіз тенденцій розвитку нейрокриптографії. *Вісник Вінницького національного технічного університету*. Вінниця. 2018. №2. С. 25–29.
7. Червяков Н.И. Евдокимов А.А., Галушкин А.И., Лавриненко А.В., Лавриненко И.Н. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: ФИЗМАТЛИТ, 2012. 280 с.
8. Авдошин С.М., Савельева А.А. Проблемы оценки криптозащищенности информационных систем. *Бизнес-информатика*. 2008. № 2(04). С. 3–15.
9. Гридин В.Н., Солодовников В.И. Исследование вопросов криптостойкости и методов криптоанализа нейросетевого алгоритма симметричного шифрования. *Известия ЮФУ*. Ростов-на-Дону. 2016. № 7(180). С. 114–122.

10. Бондарчук С.І., Ковальчук В.Н., Ковальчук А.М., Ефіменко А.А. Реалізація та дослідження криптографічного захисту даних з відкритим ключем на основі нейронної мережі. Вісник Житомирського державного технологічного університету. 2018. №2(82). С. 195–203.
11. Зюляркина Н.Д. Элементы больших порядков в линейных группах и модификация системы Эль-Гамаля. *Вестник УрФО*. 2015. №5(15). С. 47–50.
12. Haghipour S., Sokouti B. Approaches in RSA cryptosystem using artificial neural network. *Oriental journal of computer science and technology*. Tabriz. 2009. № 2(1). P. 11–17.
13. Червяков Н.И., Ляхов П.А., Бабенко М.Г., Лавриненко И.Н., Лавриненко А.В. Компьютерные вычисления на основе модулярной алгебры: монография Ставрополь: Фабула. 2015. 210 с.
14. Молчанова А.А. Криптосистема Эль-Гамаля. *Технические науки в России и за рубежом*. Москва. 2016. №2. С. 8–10.
15. Arboleda E. Secure and fast chaotic El Gamal cryptosystem. *International Journal of engineering and advanced technology*. 2019. Vol. 8. № 5. P. 1693–1699.

NEURAL NETWORK FOR THE PUBLIC KEY CRYPTOGRAPHIC SYSTEM

Yalova K.M., Yashyna K.V., Korotka V.O.

Abstract

The necessity to improve the quality and reliability of cryptosystems and the rapid development of information technologies have contributed to the introduction of neural network algorithms in cryptography. Nowadays neural cryptography, as a science using neural networks and stochastic algorithms for cryptanalysis and data encryption, has become increasingly popular. In spite of numerous scientific works devoted to the search for effective application of various neural network in cryptosystems, this scientific and practical task remains relevant and requires further development.

The main goal of the article is to present the results of the neural network development and application for a public key cryptosystem using the El Gamal cryptosystem as an example. In order to achieve the goal of the article the following tasks were carried out, namely: the neural network architecture for the El Gamal cryptosystem implementation was designed; software for the created neural network implementation was developed; neural network training and testing was conducted; El Gamal cryptosystem with neural network operation was simulated; El Gamal cryptosystem performance data was analyzed.

The three level perseptron to implement the El Gamal cryptosystem on matrix group was created. The sigmoid activation function was used to operate the neural network. Software and user interface were developed in order to evaluate the effectiveness of the neural network application. The software allows to enter the input message and record the encryption and decryption process time in the El Gamal cryptosystem when using the neural network and without it. The results of the El Gamal cryptosystem work simulation confirm the expediency and perspective of neural algorithms using. Comparison of the El Gamal cryptosystem encryption and decryption rate is performed. The average acceleration of information encryption using the neural network is about 5%, the average acceleration of information decryption is about 11%. Analysis of the El Gamal cryptosystem cryptographic resistance created with the proposed neural network, and the neural network architecture optimization by convolutional layers adding are the tasks of the further research.

References

[1] Mao, W. (2002). *Modern Cryptography: Theory and Practice*. New Jersey: Pearson Education [in English].
[2] Ryabko, B.Ya., & Fionov, A.N. (2004). *Osnovyi sovremennoy kriptografii dlya spetsialistov v informatsionnyih tehnologiyah [Fundamentals of modern cryptography for information technology professionals]*. Moscow: Science world [in Russian].

[3] Shnayer, B. (2002). *Prikladnaya kriptografiya. Protokolyi, algoritmyi, ishodnyie tekstyi na yazyike Si [Applied acryptography. Protocolsm, algorithms, source code in C*. Moscow: Triymf [in Russian].
[4] Protic, D.D. (2016). Neural cryptography. *Military technical courier*, 64, 2, 483 — 495 [in English].
[5] Laskari, E.C., Meletiou, G.C., Stamatiou, Y.C., & Vrahatis, M.N. (2006). Studying the performance of artificial neural networks on problems related to cryptography. *Nonlinear analysis: real world applications, 7*, 937–942 [in English].
[6] Kupershtein, L., & Tatarchuk A. (2018). Analiz tendentsii rozvytku neirokryptohrafii. [Analysis of trends in the development of neurocryptography]. *Visnyk Vinnytskoho tekhnichnoho universytetu – Visnyk of Vinnytsya technical university, 2*, 25-29 [in Ukranian].
[7] Chervyakov, N.I., Evdokimov, A.A., Galushkin, A.I., Lavrinenko, A.V., & Lavrinenko, I.N. (2012). *Primenenie iskusstvennyih neyronnyih setey i sistemyi ostatochnyih klassov v kriptografii. [Using of artificial neural networks and residual class systems in cryptography]*. Moscow: FIZMATLIT [in Russian].
[8] Avdoshin, A.A., & Saveleva A.A. (2008). Problemyi otsenki kriptozaschischennosti informasionnyih system. [Problems of assessing the cryptographic security of information systems]. *Biznes-informatika – Business Informatics*, *2(04),* 3–15 [in Russian].
[9] Gridin, V.N., & Solodovnikov, V.I. (2016). Issledovanie voprosov kriptostoykosti i metodov kriptoanaliza neyrosetevogo algoritma simmetrichnogo shifrovaniya [Investigation of a cryptographic strength and cryptanalysis methods for the neural network algorithm of a symmetric encryption]. *Izvestiia YuFU – Proceedings of YuFU, 7(180)*, 114–122 [in Russian].
[10] Bondarchuk, S.I, Kovalchuk, V.N., Kovalchuk, A.M., & Efimenko, A.A. (2018). Realizatsiia ta doslidzhennia alhorytmu kryptohrafichnoho zakhystu danykh z vidkrytym kliuchem na osnovi neironnoi merezhi [Implementation and research of the algorithm of cryptographic protection of data with the public key based on the neural network]. *Visnyk Zhytomyrskoho derzhavnoho tekhnolohichnoho universytetu – The Journal of Zhytomyr state technological university, 2(82)*, 195–203 [in Ukranian].
[11] Zulyarkina, N.D. (2015). Elementyi bolshih poryadkov v lineynyih gruppah i modifikatsiya sistemyi El-Gamalya [Elements more order linear groups, and modification of the El Gamal]. *Vestnik YrFO – Proceedings of YuFU*, *5(15)*, 47 — 50 [in Russian].
[12] Haghipour, S., & Sokouti, B. (2009). Approaches in RSA cryptosystem using artificial neural network. *Oriental journal of computer science and technology*, *2(1)*, 11–17 [in English].
[13] Chervyakov, N.I., Lyakhov, P.A., Babenko M.G., Lavrinenko, I.N., & Lavrinenko, A.V. (2015). *Kompyuternyie vyichisleniya na osnove modulyarnoy algebryi [Computer Calculations Based on Modular Algebra]*. Stavropol: Fabula [In Russian].
[14] Molchanova, A.A. (2016). Kriptosistema El-Gamalya [El Gamal cryptosystem]. *Tehnicheskie nauki v Rossii i za rubezhom – Technical science in Russia and abroad*, *2*, 8–10 [in Russian].
[15] Arboleda, E. (2019). Secure and fast chaotic El Gamal cryptosystem. *International Journal of engineering and advanced technology, Vols. 8, 5*, 1693–1699 [in English].