www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2022.2.3

УДК 004.056
ББК 16.8

НЕЙРОКРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Арина Валерьевна Никишова

Кандидат технических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
nikishova.arina@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Екатерина Михайловна Глыбина

Преподаватель,
Волгоградский филиал
Московского государственного гуманитарно-экономического университета
v-filial@mail.ru
ул. Поддубного, 15, 400040 г. Волгоград, Российская Федерация

Михаил Юрьевич Умницын

Руководитель группы аналитики и оценки информационной безопасности,
ООО «ИЦ РЕГИОНАЛЬНЫЕ СИСТЕМЫ»
resp@ec-rs.ru
ул. Социалистическая, 17, 400001 г. Волгоград, Российская Федерация

Аннотация. Вместе с быстрым развитием цифровых технологий коммуникации, позволивших передавать сообщения в разных формах по сети, возросла и потребность в защите передаваемых данных от доступа к ним третьих лиц. Одним из основных способов защиты данных является их шифрование. Главный принцип таких алгоритмов состоит в том, что передатчики приемника должны заранее знать алгоритм шифрования и ключ к сообщению, без которых информация представляет собой не имеющий смысла набор символов. Поскольку с повышением производительности вычислительной техники отмечается рост эффективности методов криптоанализа, возникла необходимость в применении более сложных подходов к шифрованию. В частности, в использовании такого перспективного подхода, как нейронные сети, для шифрования данных – нейрокриптографии. Благодаря тому, что вычислительная мощность технических средств продолжает возрастать, на сегодняшний день нашли применение на практике самые разные реализации нейронных сетей. Любой алгоритм шифрования основывается на генерации различных вариантов искаженного кода, который может быть распознан или восстановлен используемой нейронной сетью с заданными характеристиками и включает в себя следующие этапы: предварительный, осуществляющий предварительную обработку данных и формирование обучающей выборки; формирования нейронной сети, включающий обучение; и основной, осуществляющий шифрование или дешифрование. В статье рассматривается вопрос повышения эффективности защиты данных средствами нейрокрип-

тографии. Повышение эффективности достигается за счет выбора такой группы криптографических примитивов, реализация которых в виде нейронной сети является наиболее эффективной. Под эффективностью при этом подразумевается отношение скорости шифрования данных ко времени формирования нейронной сети.

Ключевые слова: шифрование, нейронная сеть, замена, перестановка, блочная одинарная перестановка.

Проведен анализ нейрокриптографии, в результате которого был сделан вывод, что вне зависимости от того, какая нейронная сеть будет взята за основу нейрокриптографической системы, для шифрования могут использоваться либо симметричные, либо асимметричные алгоритмы шифрования [2]. В статье рассматриваются симметричные алгоритмы шифрования, поскольку они не требовательны к вычислительным ресурсам, отличаются высокой скоростью шифрования и обладают теоретической стойкостью в отличие от асимметричных алгоритмов.

Проанализированы некоторые существующие методы нейрокриптографии [1]. В результате анализа выбран метод шифрования на основе нейронной сети RBF, поскольку он обладает низкой вычислительной сложностью, низкой сложностью обучения и достаточной криптостойкостью [3].

Функциональная модель, выполнена в соответствии с методологией IDEF0, предназначенной для формализации и описания процесса защиты данных средствами нейрокриптографии.

При декомпозиции функционального блока [4] были выделены следующие его составляющие (см. рисунок):

а) блок «Сформировать обучающую выборку»;

б) блок «Обучить нейронную сеть»;

в) блок «Зашифровать документ».

В блоке «Сформировать обучающую выборку» заданы:

а) входные данные – открытый текст;

б) управляющая информация, в качестве которой выступает алгоритм шифрования;

в) механизмы, необходимые для формирования обучающей выборки, – специалист по защите информации и программный комплекс.

В результате данных воздействий на выходе функции получается обучающая выборка.

В блоке «Обучить нейронную сеть» заданы:

а) входные данные – обучающая выборка;

б) управляющая информация, в качестве которой выступает алгоритм обучения обратного распространения ошибки;

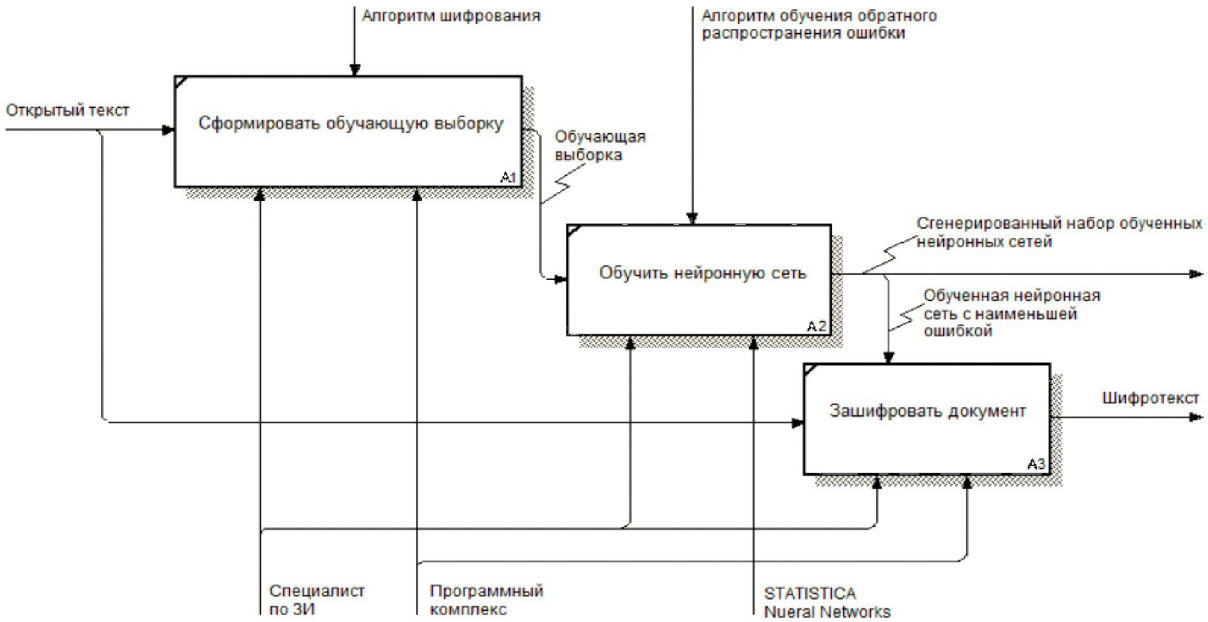

Рис. 1. Декомпозиция функционального блока «Защита данных средствами нейрокриптографии»

в) механизмы, необходимые для формирования обучающей выборки, – специалист по защите информации и STATISTICA Nueral Networks (SNN).

В результате данных воздействий на выходе функции получается сгенерированный набор обученных нейронных сетей.

В блоке «Зашифровать документ» заданы:

а) входные данные – открытый текст;

б) управляющая информация, в качестве которой выступает алгоритм обученная нейронная сеть с наименьшей ошибкой;

в) механизмы, необходимые для формирования обучающей выборки, – специалист по защите информации и программный комплекс.

В результате данных воздействий на выходе функции получается шифротекст.

Проведены экспериментальные исследования. Задачей экспериментальных исследований является определение наилучшего метода защиты данных средствами нейрокриптографии с помощью расчета показателя эффективности при помощи программного комплекса.

Для решения поставленной задачи необходимо провести следующие эксперименты:

а) анализ защиты данных средствами нейронной сети, построенной на базе шифра Цезаря;

б) анализ защиты данных средствами нейронной сети, построенной на базе шифра блочной одинарной перестановки.

В результате проведенных экспериментов получены следующие значения эффективности для защиты данных средствами нейронных сетей, построенных на базе шифра Цезаря и на базе шифра блочной одинарной перестановки:

а) эффективность защиты данных средствами нейронных сетей, построенных на базе шифра Цезаря, – 629;

б) эффективность защиты данных средствами нейронных сетей, построенных на базе шифра блочной одинарной перестановки, – 1157.

Из результатов экспериментальных исследований можно сделать вывод, что использование шифра блочной одинарной перестановки является более эффективным для защиты данных средствами нейрокриптографии, поскольку обучение такой нейронной сети занимает меньше времени.

СПИСОК ЛИТЕРАТУРЫ

1. Бахарева, П. С. Примеры нейронных сетей в криптографии / П. С. Бахарева // Материалы XIII Международной студенческой научной конференции «Студенческий научный форум». – 2018. – Режим доступа: https://scienceforum.ru/2021/ article/ 2018027592.

2. Григорьева, Д. Р. Симметричные криптографические системы: учеб.-метод. пособие по дисциплине «Информационная безопасность» / Д. Р. Григорьева, Г. А. Гареева, Р. Р. Басыров. – Набережные Челны : НЧИ КФУ, 2018. – 30 с.

3. Дрон, К. К. О перспективах совместного использования методов квантовой и классической криптографии / К. К. Дрон // Вестник ХГУ им. Н.Ф. Катанова. – 2018. – № 24. – С. 10.

4. Gupta, V. Encryption and Decryption using one pad time algorithm in MAC layer / V. Gupta, S. Sharma // International Journal of Innovative Research in Science, Engineering and Technology. – 2013. – Vol. 2, № 6. – P. 2248.

REFERENCES

1. Bakhareva P.S. *Primery nejronnykh setej v kriptografii* [Examples of Neural Networks in Cryptography]. *Materialy XIII Mezhdunarodnoj studencheskoj nauchnoj konferentsyi «Studencheskij nauchnyj forum»* [Proceedings of the 13th International Student Scientific Conference “Student Scientific Forum”], 2018. URL: https://scienceforum.ru/2021/ article/2018027592.

2. Grigoryeva D.R., Gareeva G.A., Basyrov R.R. *Simmetrichnye kriptograficheskie sistemy: ucheb.-metod. posobie po discipline «Informatsyonnaya bezopasnost»* [Symmetric Cryptographic Systems. Textbook on “Information Security”]. Naberezhnye Chelny, NChI KFU, 2018. 30 p.

3. Dron K.K. O perspektivakh sovmestnogo ispolzovaniya metodov kvantovoj i klassicheskoj kriptografii [On the Prospects for the Joint Use of Quantum and Classical Cryptography Methods]. *Vestnik KhGU im. N.F. Katanova* [Bulletin of KhSU Named After N.F. Katanov], 2018, no. 24, p. 10.

4. Gupta V., Sharma S. Encryption and Decryption Using One Pad Time Algorithm in MAC Layer. *International Journal of Innovative Research in Science, Engineering and Technology*, 2013, vol. 2, no. 6, p. 2248.

NEUROCRYPTOGRAPHIC INFORMATION PROTECTION

Arina V. Nikishova

Candidate of Sciences (Engineering), Associate Professor,
Department of Information Security,
Volgograd State University
nikishova.arina@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Ekaterina M. Glybina

Lecturer,
Volgograd Branch of the Moscow State University of Humanities and Economics
v-filial@mail.ru
Poddubnogo St, 15, 400040 Volgograd, Russian Federation

Mikhail Yu. Umnitsyn

Head of the Analytical Group and Information Security Assessment,
EC Regional Systems
resp@ec-rs.ru
Sotsialistheskaya St, 17, 400001 Volgograd, Russian Federation

Abstract. Along with the rapid development of digital communication technologies, which allowed to transmit messages in different forms over the network, the need to protect transmitted data from access by third parties has increased. One of the main ways to protect data is encryption. The main reason for encryption is that users must be aware of encryption methods and keys, without which information is meaningless in the form of symbols. As the efficiency of cryptanalysis methods has increased with computational performance, there has been a need for more sophisticated approaches to encryption. In particular, the use of such a promising approach as neural networks for data encryption – neurocryptography. Due to the fact that the increased power of technological tools continues to grow, today's neural networks have been used in practice. Any encryption algorithm is based on generating different variants of a distorted code that can be recognized or reconstructed by a neural network with specified characteristics, and includes the following stages: preliminary, performing preliminary data processing and formation of a training sample; formation of a neural network, including training; and the main one, performing encryption or decryption. The article deals with the issue of increasing the efficiency of data protection by means of neurocryptography. Improving efficiency is achieved by selecting a group of cryptographic primitives, the implementation of which in the form of a neural network is the most effective. Efficiency in this case means the ratio of data encryption speed to the time of formation of the neural network.

Key words: encryption, neural network, replacement, permutation, block single permutation.