НЕЙРОКРИПТОГРАФИЧЕСКАЯ СИСТЕМА РЕКУРРЕНТНЫХ КОНВЕРГЕНТНЫХ НЕЙРОСЕТЕЙ ЗАЩИТЫ ИНФОРМАЦИИ

Власов К.А.[1]

Аннотация.

Цель работы: *построение алгоритма преобразования информации рекуррентными конвергентными нейросетями с заданным набором локальных минимумов функционала энергии для последующего его применения в области защиты информации.*

Метод: *анализ существующих нейросетевых парадигм, применимых для классификации образов. Синтез нейрокриптографичекой системы с использованием метода аналогии, рекуррентных конвергентных нейронных сетей, алгоритмов помехоустойчивого кодирования и блочного шифрования.*

Полученный результат: *предлагается перспективная нейрокриптографическая система, которая может быть использована для разработки алгоритма помехоустойчивого кодирования, симметричного или потокового шифрования данных, основанного на генерации различных вариантов искажающих образов, представляющих собой последовательность бит, маскирующих исходное сообщение. Создан алгоритм блочного симметричного шифрования данных, основанного на базе нейронных сетей типа Хопфилда. Ключевая информация включает информацию о выбранных (с помощью радиальных базовых функций) структурных характеристиках потенциала с заданным набором энергетических минимумов, определяющего динамику нейронной сети как потенциальной динамической системы, чьи аттракторы являются символами (объединением нескольких символов) алфавита входного текста. Размеры ключа напрямую зависят от мощности алфавита исходного сообщения и от формы представления функционала энергии. Предложенная нейрокриптографическая система может быть также использована в системе аутентификации.*

Ключевые слова: *нейрокриптография, помехоустойчивое кодирование, симметричное шифрование, блочный шифр, система аутентификации, нейронная сеть с обратной связью, потенциальная динамическая система, радиальная базовая функция.*

DOI: 10.21681/2311-3456-2020-04-44-55

1. Введение

Одним из перспективных направлений в современной криптографии является разработка и исследование алгоритмов шифрования, построенных на основе математического аппарата искусственных нейронных сетей, – нейрокриптография [1-2]. В настоящее время разрабатываются криптографические методы, реализованные с использованием искусственных нейронных сетей, способные с необходимой эффективностью решать задачи классической криптографии, такие как обеспечение конфиденциальности, целостности, невозможности отказа от авторства и т.п. [3-7]. Предпосылкой использования нейросетевого подхода объясняется тем обстоятельством, что особенностью ряда нейронных сетей является способность восстановления искаженных кодов и распознавания объектов, имеющих характеристики отличные от эталонных [8-11]. Дополнительным преимуществом данной технологии является параллельность вычислений нейросетевых алгоритмов, что позволяет увеличить скорость обработки данных при аппаратной реализации. Плохая изученность криптостойкости нейросетевых методов шифрования делает актуальной задачу исследования характерных особенностей и поиска уязвимостей нейросетевых криптографических алгоритмов. В данной работе проведены анализ и построение алгоритма преобразования информации рекуррентными конвергентными нейросетями с заданным набором локальных минимумов функционала энергии для последующего его применения в области защиты информации.

2. Построение нейронной сети

Предлагаемый алгоритм преобразования информации может быть отнесен к блочному, что обусловлено структурными особенностями нейронных сетей, а именно фиксированным числом входных элементов и внутренним представлением данных. Для создания универсальности будем рассматривать алгоритм обработки некоторой информации, представленной в любом формате, т.е. будем оперировать, например, символами ASCII и их кодами. Таким образом, предла-

1 Власов Константин Александрович, старший научный сотрудник, Краснодарское высшее военное училище имени генерала армии С.М.Штеменко, г. Краснодар, Россия. E-mail: meavit@yandex.ru

гаемый алгоритм применим для любого потока данных.

Во многих парадигмах нейронных сетей используются сигмоидные (логистические) и радиальные базисные функции. В [12-15] качестве инструментария для получения и обработки результирующего текста могут быть рассмотрены нейросетевые парадигмы, применимые для классификации образов – такие, как многослойный персептрон MLP, радиальные RBF, вероятностные PNN и конкурирующие LVQ – сети, а также комитетов нейросетей. Алгоритм обработки информации основан на генерации различных вариантов искаженного кода, которые могут быть распознаны или восстановлены используемой нейронной сетью с заданными характеристиками. Для его реализации необходимо рассмотрение следующих основных этапов:

- построение нейронной сети – генерация ключевого файла, задающего значения весовых коэффициентов и областей притяжения;
- основной этап, на котором происходит процесс преобразования информации.

В предложенной нейронной сети значения X_i входного вектора $\vec{X} = \{X_1, \dots X_i, \dots, X_N\}$ лежат в промежутке [0, 1], где вектор $\vec{X}$ – текущее состояние сети, *N* – размерность вектора, зависящая от размерности шифруемого блока данных. Выходные сигналы нейронов являются одновременно входными сигналами сети: $\vec{X}(t) = \vec{Z}(t-1)$, где *t* – номер такта, время. *K* – количество образов (символов в алфавите), которым «обучена» сеть, тогда вектор $\overrightarrow{S^k}$ – обучающий образ, где *k* = 1, 2, ..., *K* [16-19].

Создание сети, как правило, эквивалентно формированию потенциала *V* с заданным набором минимумов в точках $\vec{X} = \overrightarrow{S^k}$, $1 \le k \le K$. Динамика нейронной сети, состояние которой непрерывно зависит от времени *t*, может быть определена уравнениями потенциальной динамической системы:

$$\frac{dx}{dt} = -\nabla V(x), \tag{1}$$

где: *x* – выход нейронной сети, действительное число.

Потенциал *V* может быть задан с помощью радиальных базовых функций, используемых для многомерной интерполяции данных, поэтому (1) представим в виде системы *N* динамических уравнений:

$$\begin{cases} \frac{dX_1}{dt} = f_1(X_1, \dots, X_i, \dots, X_N), \\ \dots, \\ \frac{dX_i}{dt} = f_i(X_1, \dots, X_i, \dots, X_N), \\ \dots, \\ \frac{dX_N}{dt} = f_N(X_1, \dots, X_i, \dots, X_N). \end{cases} \tag{2}$$

Данная потенциальная динамическая система для алгоритма раскодирования может быть преобразована следующим образом:

$$\begin{cases} f_1(X_1, \dots, X_i, \dots, X_N) = -\frac{\partial U(X_1,\dots,X_i,\dots,X_N)}{\partial X_1}, \\ \dots, \\ f_i(X_1, \dots, X_i, \dots, X_N) = -\frac{\partial U(X_1,\dots,X_i,\dots,X_N)}{\partial X_i}, \\ \dots, \\ f_N(X_1, \dots, X_i, \dots, X_N) = -\frac{\partial U(X_1,\dots,X_i,\dots,X_N)}{\partial X_N}; \end{cases} \tag{3}$$

$$\begin{cases} -\frac{\partial U(X_1,\dots,X_i,\dots,X_N)}{\partial X_1} \approx -h\frac{U(X_1+H_1,\dots,X_i,\dots,X_N)-U(X_1,\dots,X_i,\dots,X_N)}{H_1}, \\ \dots, \\ -\frac{\partial U(X_1,\dots,X_i,\dots,X_N)}{\partial X_i} \approx -h\frac{U(X_1,\dots,X_i+H_i,\dots,X_N)-U(X_1,\dots,X_i,\dots,X_N)}{H_i}, \\ \dots, \\ -\frac{\partial U(X_1,\dots,X_i,\dots,X_N)}{\partial X_N} \approx -h\frac{U(X_1,\dots,X_i,\dots,X_N+H_N)-U(X_1,\dots,X_i,\dots,X_N)}{H_N}, \end{cases} \tag{4}$$

где: $H_i = \Delta X_i$.

Согласно теореме Эйлера, при заданном шаге h наша система динамических уравнений, представленная формулами (2), (3) и (4) примет следующий вид:

$$\begin{cases} X_{1,t+1} \approx X_{1,t} - h\dfrac{U(X_{1,t}+H_1,\ldots,X_{i,t},\ldots,X_{N,t})-U(X_{1,t},\ldots,X_{i,t},\ldots,X_{N,t})}{H_1}, \\ \ldots \\ X_{i,t+1} \approx X_{i,t} - h\dfrac{U(X_{1,t},\ldots,X_{i,t}+H_i,\ldots,X_{N,t})-U(X_{1,t},\ldots,X_{i,t},\ldots,X_{N,t})}{H_i}, \\ \ldots \\ X_{N,t+1} \approx X_{N,t} - h\dfrac{U(X_{1,t},\ldots,X_{i,t},\ldots,X_{N,t}+H_N)-U(X_{1,t},\ldots,X_{i,t},\ldots,X_{N,t})}{H_N}. \end{cases} \quad (5)$$

Применив теорему Колмогорова-Арнольда о представлении непрерывных функций, можно построить рекуррентную конвергентную нейронную сеть, представленную рисунками (рис. 1...3).

В общем виде N-мерной нейронной сети для метода Эйлера (рис. 1) в первом слое расположено n нейронов, во втором слое n подсетей по три слоя каждый. Подсеть U (рис. 3) N-мерной нейронной сети состоит из трех слоев. В первом слое $n(2n+1)$ нейронов, во втором $2n+1$, третий слой состоит из одного нейрона-сумматора.

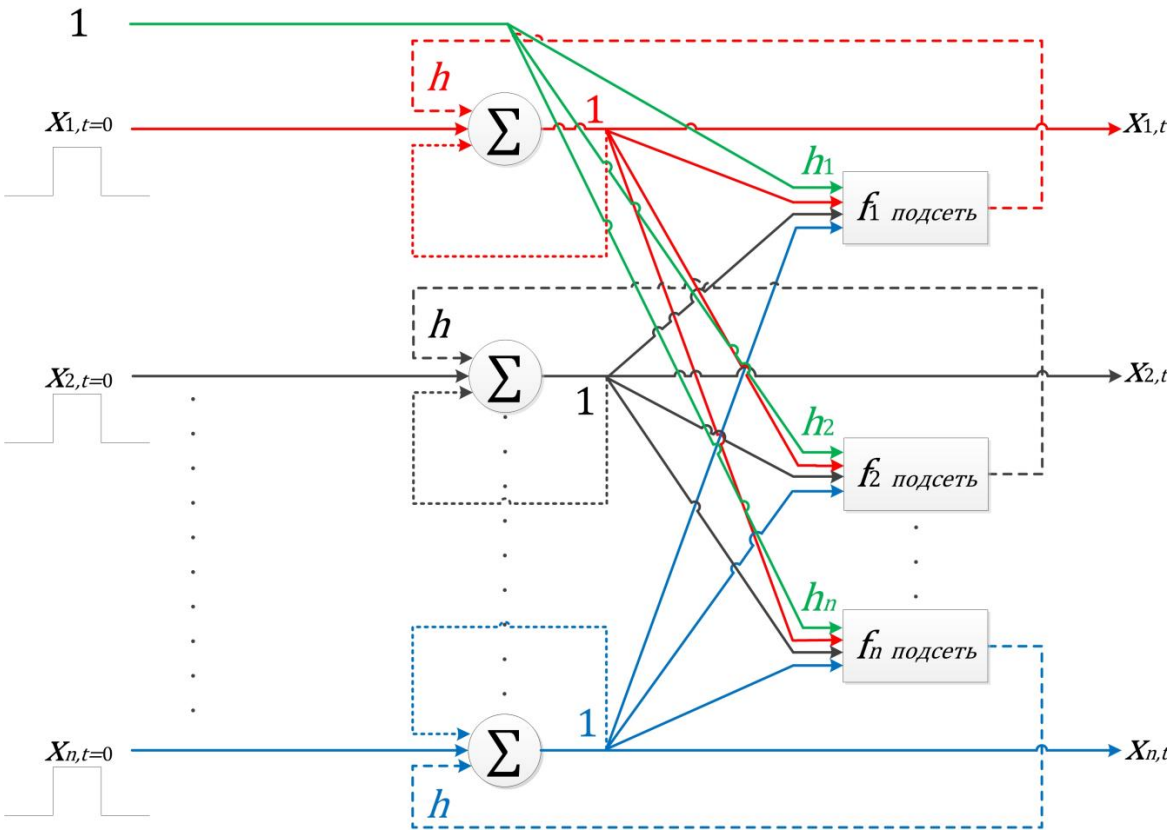

Рис. 1. Общий вид N-мерной нейронной сети для схемы Эйлера

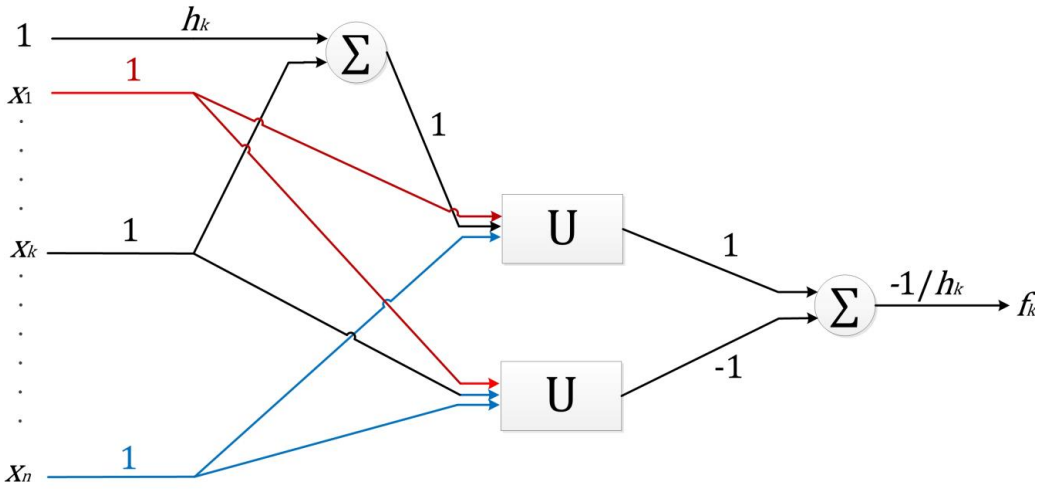

Рис. 2. Подсеть f_k N-мерной нейронной сети для схемы Эйлера

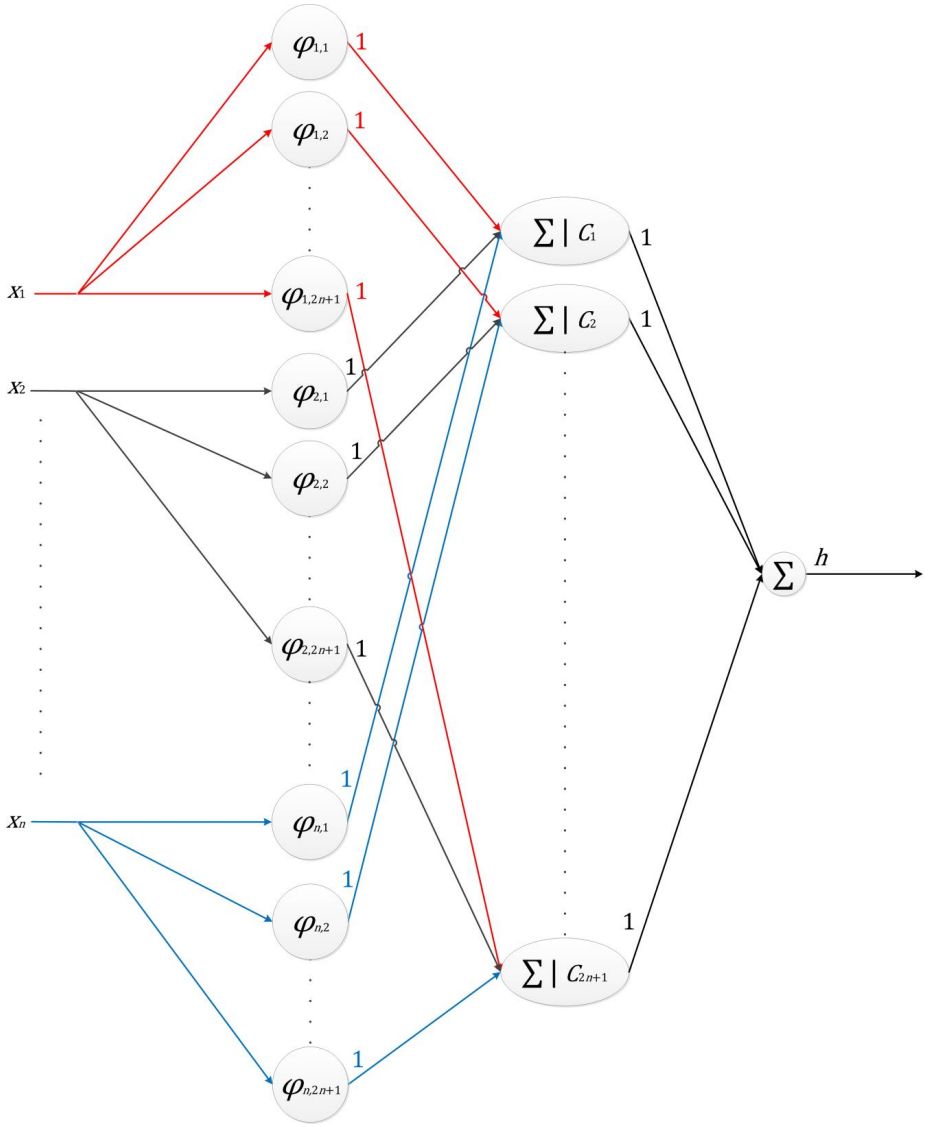

Рис. 3. Подсеть U N-мерной нейронной сети для схемы Эйлера

Для повышения точности вычислений схема Эйлера первого порядка точности может быть заменена схемой Рунге-Кутта четвертого порядка точности, тогда внешний вид нейронной сети, представленный рисунками (рис. 1, 2) будет заменен на вид, представленный рисунками (рис. 4...6).

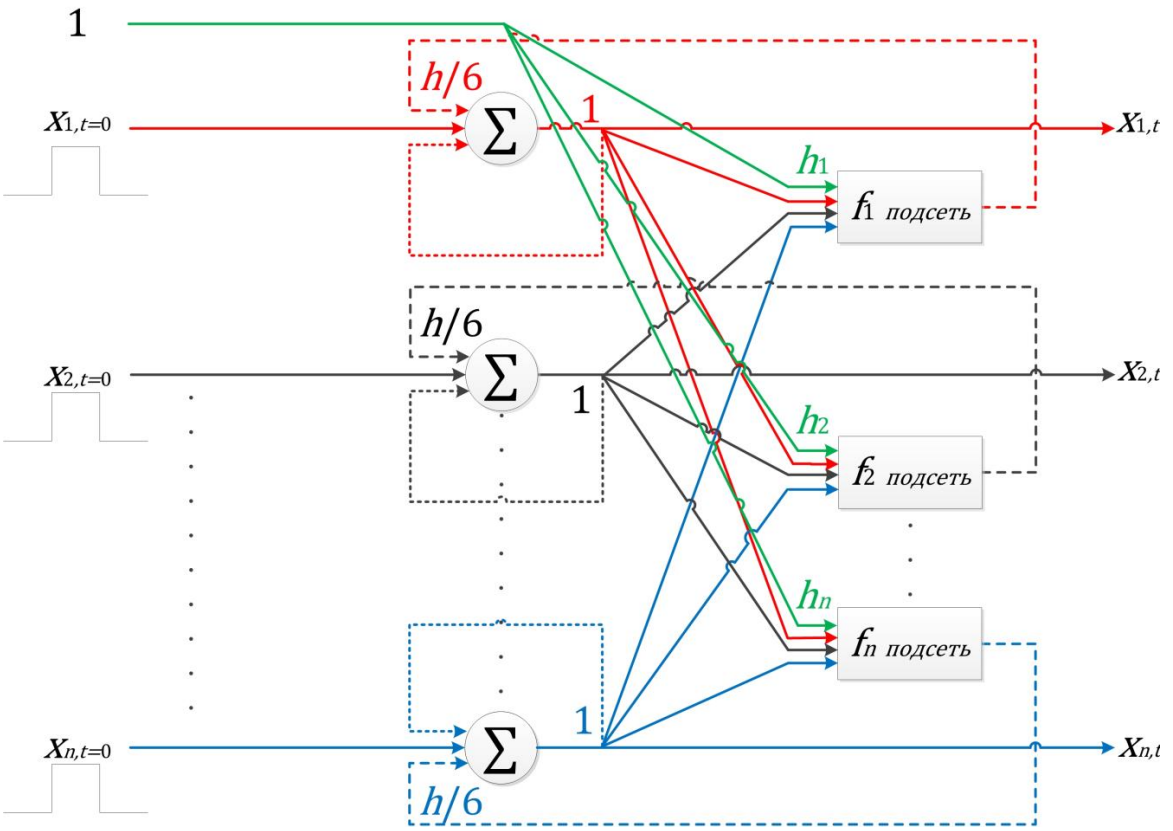

Рис. 4. Общий вид N-мерной нейронной сети для схемы Рунге-Кутта

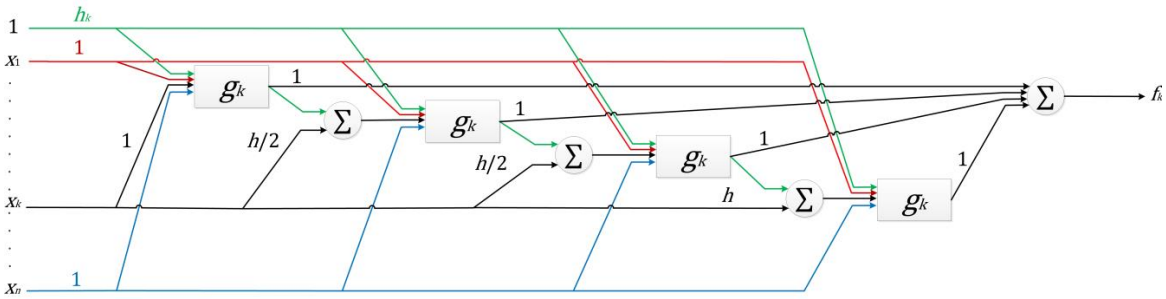

Рис. 5. Подсеть f_k N-мерной нейронной сети для схемы Рунге-Кутта

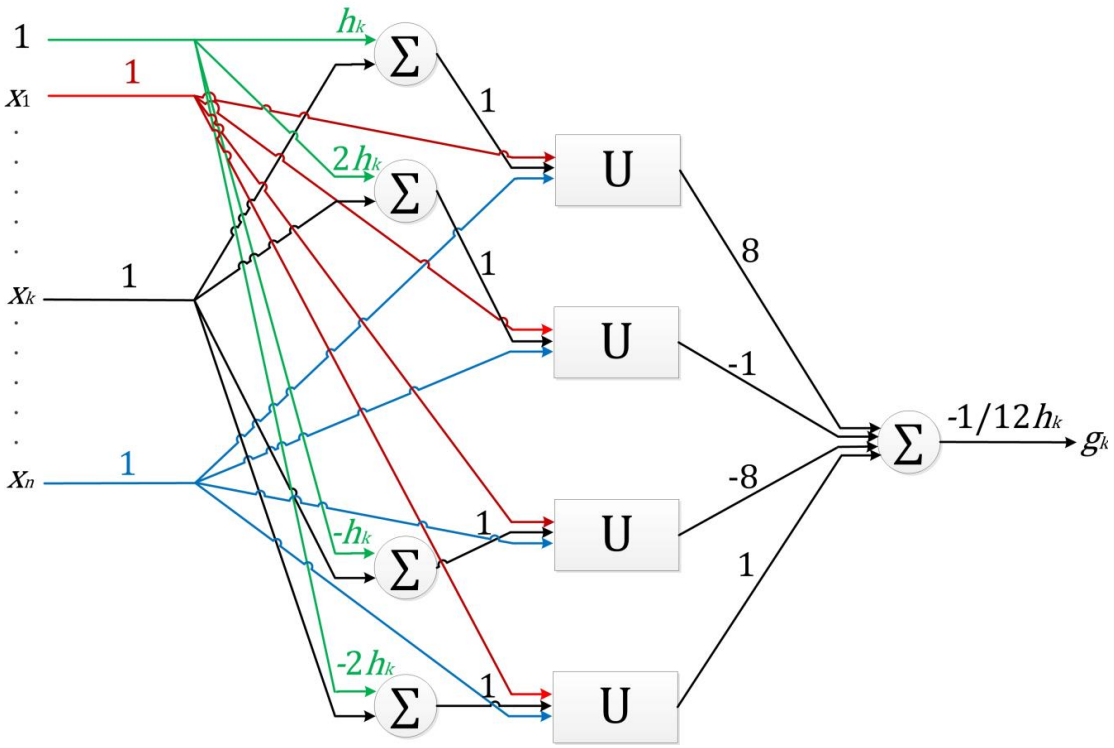

Рис. 6. Подсеть g_k N-мерной нейронной сети для схемы Рунге-Кутта

Для наглядности производимых операций в предлагаемом алгоритме динамика нейронной сети может быть распределена на плоскости, тогда (1) представляется системой двух динамических уравнений:

$$\begin{cases} \frac{dx}{dt} = f_1(x,y), \\ \frac{dy}{dt} = f_2(x,y). \end{cases} \quad (6)$$

Формулы (2)-(5) в данном случае преобразуются в следующий вид:

$$\begin{cases} x_{t+1} \approx x_t - h\frac{U(x_t+a,y_t)-U(x_t,y_t)}{a}, \\ y_{t+1} \approx y_t - h\frac{U(x_t,y_t+b)-U(x_t,y_t)}{b}, \end{cases} \quad (7)$$

где: $a = \Delta x, b = \Delta y$.

Согласно теореме Колмогорова, для функции двух переменных:

$$U(x_t, y_t) = \sum_{q=1}^{5} C_q[\varphi_q(x_t) + \Psi_q(y_t)]. \quad (8)$$

Тогда нейронная сеть для всей системы динамических уравнений двух переменных с рекуррентной связью будет иметь вид, изображенный на рисунках (рис. 7, 8).

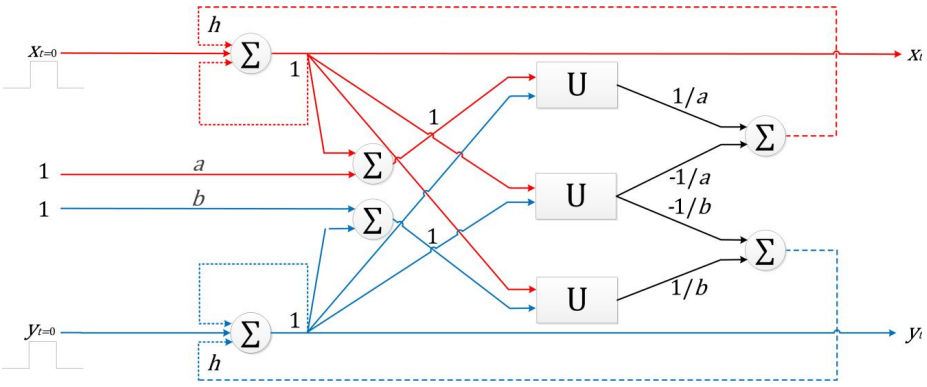

Рис. 7. Общий вид двухмерной нейронной сети для схемы Эйлера

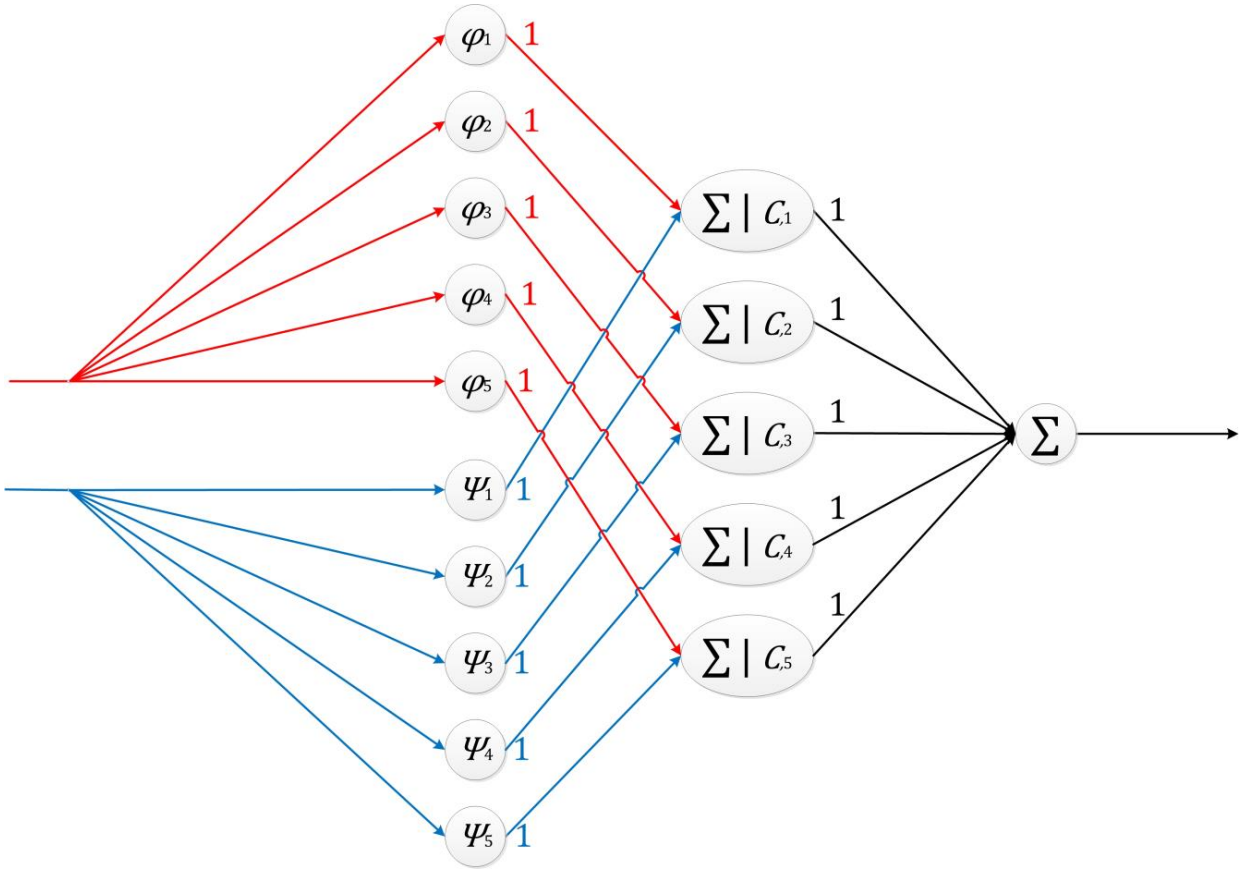

Рис. 8. Подсеть U двухмерной нейронной сети для схемы Эйлера

Стоит отметить, что на вход первого слоя на нулевом такте однократно поступает начальный сигнал $x_{t=0}$ и $y_{t=0}$, который без изменений следует на последующие слои, а также на выход нейронной сети. На первом такте уже вместо начального сигнала на вход первого слоя уже поступают два значения – предыдущие значения результирующих сигналов (на первом такте будут $x_{t=0}$ и $y_{t=0}$) и результат функции f_k с весом *h*. Дальше нейронная сеть работает аналогичным образом до точки останова (например, до определенного количества тактов).

Предложенный вариант построения сети разбивается на два уровня. Первый уровень (рис. 7) раскрывает теорему Эйлера, второй уровень (рис. 8) раскрывает теорему Колмогорова. Это позволит в дальнейшем модифицировать нейронную сеть, заменяя один из уровней и оставляя без изменений другой.

Представленную нейронную сеть можно использовать не только в качестве помехоустойчивого кодирования, но и в качестве алгоритма шифрования. Тогда к его достоинству относится высокая устойчивость ключевой информации к полному перебору. При использовании одной и той же ключевой информации и неизменного исходного текста на выходе будут получаться различные криптограммы ввиду использования случайного «толчка» в начале процесса шифрования. Созданный алгоритм позволяет шифровать не только каждый символ в отдельности, что существенно ослабляет криптостойкость, но и произвольными блоками данных.

К недостаткам можно отнести большую избыточность получаемых криптограмм, объем которых может превышать исходный текст в 2 раза и более (в зависимости от числа бит и байт на действительное число), причем, чем меньше исходный алфавит, тем больше будет избыточность. Однако подобная избыточность позволяет увеличить размеры ключа также в 2 раза или более при неизменном блоке оперируемой информации. Например, при работе с блоком размерностью 128 байт, ключевая информация может достигать длины 2048 бит, что существенно выше возможностей современных симметричных алгоритмов шифрования.

3. Алгоритм шифрования

В качестве примера алгоритма шифрования возьмем радиальную базисную функцию:

$$D(z) = -Ae^{-\frac{|z|^2}{\varepsilon^2}}, \quad (9)$$

где: *A* определяет глубину минимума, ε – его ширину.

Если теперь в качестве функционала энергии выбрать

$$V(x) = \sum_k D\left(\left\|x - S^k\right\|\right) + V_2(x), \quad (10)$$

где $V_2(x)$ обеспечивает глобальное притяжение к окрестности нуля (например, квадратичный полином), то получим требуемое: энергетические минимумы в нужных символах S^k алфавита, а если

$$\left\|S^i - S^j\right\| \gg \varepsilon, \quad (11)$$

то эти минимумы практически не будут влиять друг на друга.

Таким образом, построенный по (9)-(11) для шифрования функционал имеет вид:

$$V(x) = \sum_k \left(-A_k e^{-\frac{\left\|x-S^k\right\|^2}{3{\varepsilon_k}^2}} + \frac{{\varepsilon_k}^2 \left\|x-S^k\right\|^2}{4*K} \right). \quad (12)$$

Процесс преобразования информации для наглядности покажем на примере алфавита из 4 символов «А, Б, В, Г», тогда матрица кодов символов алфавита $\vec{S} = \{\{0,0\};\{0,1\};\{1,0\};\{1,1\}\}$. В качестве ключа для алгоритма шифрования возьмем вектор $\vec{\varepsilon} =$ {0,2; 0,15; 0,3; 0,25} и A_k=2. Тогда функционал энергии (12) примет вид, представленный рисунками (рис. 9, 10).

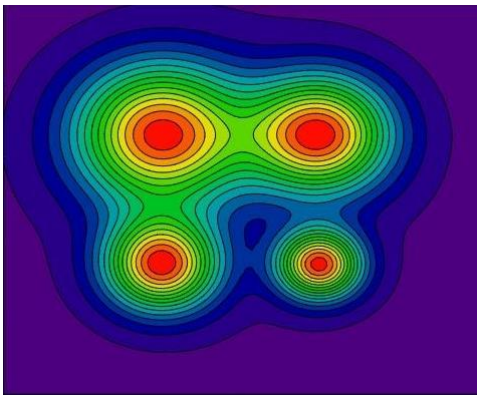

Рис. 9. Линии уровня функционала энергии на плоскости

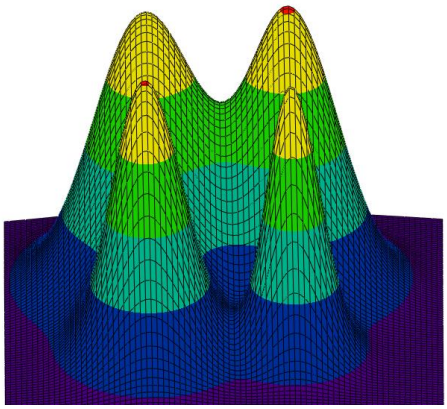

Рис. 10. Поверхность («рельеф») функционала энергии для преобразования информации

Из рисунков видно, что центрам «холмов» соответствуют координаты символов А, Б, В и Г, то есть {0,0}, {0,1}, {1,0}, {1,1}, а также наглядно заметно влияние параметра $\vec{\varepsilon}$ на ширину этих «холмов». Процесс преобразования информации построен на расчете антиградиента функционала энергии:

$$-\nabla V(x) = \quad (13)$$
$$= \sum_{k=0}^{K} \left(A_k e^{-\frac{\left\|x-S^k\right\|^2}{3\varepsilon_k^2}} \frac{-2(x-S^k)}{3\varepsilon_k^2} - \frac{{\varepsilon_k}^2 (x-S^k)}{2K} \right).$$

Для кодирования символа необходимо дать некоторый «толчок» в «дно ямы», координаты которой будут соответствовать минимальному значению между центрами «холмов». В нашем конкретном случае центром «дна ямы» соответствует точка с координатами {0.59, 0.259}. Числовое значение толчка должно быть несущественным, чтобы в процессе шифрования не ушло за пределы наших «холмов». Например, после зашумления сообщения АБВГ мы получили набор числовых значений {{0,1; 0,04}; {0,09; 0,93}; {0,99; 0,02}; {0,96; 0,95}}. После чего необходимо решить систему дифференциальных уравнений (1), например, методом Рунге-Кутта, наш «зашумленный» текст играет роль начального условия и в качестве входного вектора, а вектор (13) со знаком минус является правой частью системы дифференциальных уравнений (1).

В результате получаем псевдослучайную комбинацию числовых значений:

{{0,671; -0,703}; {0,588; 0,246}; {0,593; 0,246}; {0,592; 0,263}}. Три пары вблизи с центром «дна ямы», а первая пара вышла за пределы наших «холмов». Данные последовательности можно уже передавать в открытом виде.

Для обратного преобразования полученных последовательностей необходимо также решить систему дифференциальных уравнений (1) методом Рунге-Кутта с такими же параметрами, но в качестве входного вектора играет роль закодированный текст, а (13) является правой частью системы дифференциальных уравнений (1), то есть функционал энергии примет перевернутый вид, который представлен рисунком (рис. 11).

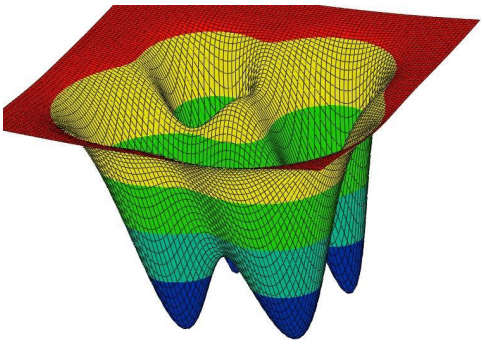

Рис. 11. Поверхность функционала энергии для обратного преобразования информации

DOI:10.21681/2311-3456-2020-04-44-55

Из (рис. 11) видно, что под действием сил притяжения, входные числовые последовательности закодированного текста неминуемо «скатятся» в одну из четырех «ям», координаты которым соответствует наш входной алфавит.

3.1. Перспективы данного алгоритма

К достоинствам данного алгоритма можно отнести высокую устойчивость ключевой информации к полному перебору, так как длина вектора $\vec{\varepsilon}$ равно количеству элементов используемого алфавита, то есть для ASCII мы имеем 256 различных значений. Также значение *A* можно представить в виде вектора, что еще больше усложнит подбор ключевой информации. Для улучшения алгоритма возможно представление «холмов» и «ям» не только радиально-симметричными (13), но еще и гауссианами, когда каждый элемент вектора $\vec{\varepsilon}$ представлен, например, матрицей размером 2x2. В данном случае линии уровня функционала энергии на плоскости примут вид, представленные рисунком (рис. 12).

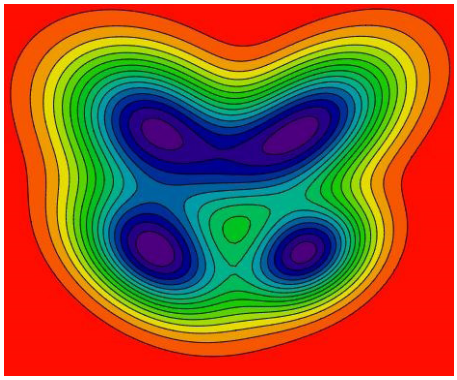

Рис. 12. Линии уровня функционала энергии на плоскости алгоритма с гауссианами

Более того, алгоритм позволяет распределять вершины «холмов» не строго по битам, а в произвольной кодировке. Например, для шифрования цифр 0, 1, ..., 8, 9 можно использовать алфавит, состоящий из 10 символов на плоскости в следующей кодировке: {-2, -1}, {-1, -2}, {0, -3}, {1, -2}, {2, -1}, {-2, 1}, {-1, 2}, {0, 3}, {1, 2}, {2, 1}. Тогда при одинаковых элементах векторов *A* и $\vec{\varepsilon}$ функционал энергии примет вид, представленный рисунками (рис.13, 14).

При выполнении процесса преобразования нескольких цифр получаем псевдослучайную комбинацию числовых значений, например:

$$0: (\{-2,-1\}) \rightarrow \{-1{,}022;\ -0{,}027\};$$
$$1: (\{-1,-2\}) \rightarrow \{-0{,}026;\ -1{,}015\};$$
$$2: (\{0,-3\}) \rightarrow \{0{,}001;\ -1{,}016\};$$
$$4: (\{2,-1\}) \rightarrow \{0{,}833;\ -0{,}303\};$$
$$8: (\{1,2\}) \rightarrow \{0{,}262;\ 0{,}867\}.$$

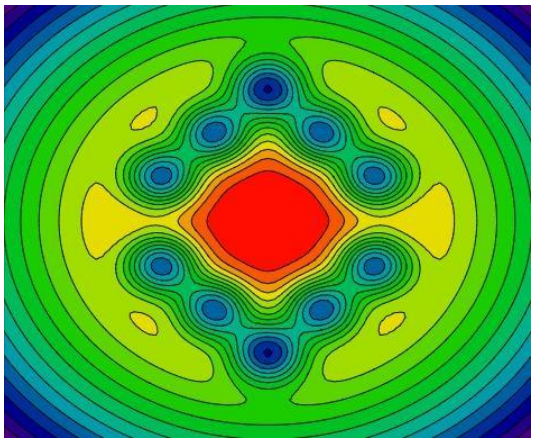

Рис. 13. Линии уровня функционала энергии на плоскости для цифр

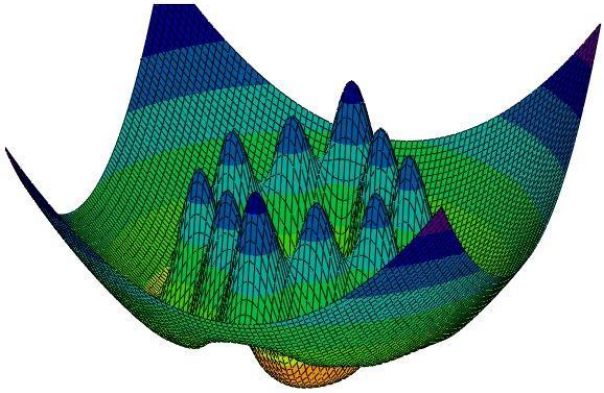

Рис. 14. Поверхность («рельеф») функционала энергии для цифр

Таким образом, сгенерированную кодировку исходных символов также можно включать в ключевую информацию.

Дальнейшее развитие алгоритма включает и организацию псевдослучайных возмущений («толчков») так, чтобы значения полученных последовательностей были различны между собой и не обязательно близки к центру «дна ямы».

При использовании одной и той же ключевой информации и неизменного исходного текста на выходе будут получаться различные криптограммы ввиду использования случайного «толчка» в начале процесса шифрования.

4. Построение протокола аутентификации

Предложенная нейрокриптографическая система может быть также использована в системе аутентификации. В качестве секретной информации, которой владеют доказывающая сторона *абонент_А* и проверяющая сторона *абонент_Б*, будет использоваться ключевая информация параметров нейронной сети *K* (набор весовых коэффициентов). Пусть D_K – алгоритм распознавания данных нейронной сетью с набором весовых

коэффициентов *K*, *H* – значение хеш-функции, вычисленное от сообщения *M* с использованием некоторой специфицированной хеш-функции *h: H = h(M)*.

Протокол аутентификации с доказательством знания, использующий предложенную модель нейронной сети, включает в себя следующие шаги:

1. проверяющая сторона генерирует некоторую псевдослучайную последовательность *C* (зашумленный текст) и передает ее *абоненту_А* в качестве запроса*;*
2. доказывающая сторона демонстрирует владение секретной информацией *K* и использует нейронную сеть для распознавания данных из шума *C: M = D_K (C)*, а затем вычисляет значение хеш-функции от полученного результата *M: H = h(M).* После этого *абонент_А* отправляет *абоненту_Б* значение *H* в качестве своего ответа;
3. проверяющая сторона тоже использует свою нейронную сеть с набором весовых коэффициентов *K* для распознавания данных из шума *C: M = D_K (C)*, а затем вычисляет значение хеш-функции от полученного результата *M: H = h(M).* После этого *абонент_Б* сравнивает значение хеш-функции *H* с полученным ответом *абонента_А*. Если равенство выполняется, то проверяющий принимает доказательство, если равенство не выполняется, то отвергает;
4. чтобы *абоненту_А* убедиться в том, что *абонент_Б* действительно является *абонентом_Б*, необходимо повторить шаги 1-3, но уже с другим зашумленным текстом, и *абонент_А* теперь является проверяющей стороной, а *абонент_Б* – доказывающей.

В результате абоненты *А* и *Б* убеждаются в достоверности друг друга. Если же один из абонентов является нарушителем, то он не сможет подобрать необходимое значение хеш-функции в качестве своего ответа. В случае, когда нарушитель перехватывает данные между абонентами *А* и *Б*, то никакой полезной информации получить не сможет.

В предложенном протоколе аутентификации безопасность информации напрямую зависит от криптостойкости нейронной сети, то есть от уникальности и количества возможных получаемых образов после распознавания данных из зашумленного текста. Поэтому актуальной задачей является правильное построение нейронной сети.

5. Выводы

Проведен системный анализ нейрокриптографичекой системы кодирования и шифрования данных, предложена рекуррентная конвергентная нейронная сеть, реализующая потенциальную динамическую систему. Минимумы потенциальной энергии (аттракторы) динамической системы связаны с образами исходных сообщений, области притяжения аттракторов содержат искажающие образы, представляющие собой последовательность бит, маскирующих исходное сообщение.

Данная нейрокриптографичекая система рекуррентных конвергентных нейросетей может быть использована для разработки алгоритма помехоустойчивого кодирования или симметричного блочного шифрования данных. Преимуществом данной технологии является параллельность вычислений нейросетевых алгоритмов, что позволяет увеличить скорость обработки данных при аппаратной реализации.

Разработан алгоритм преобразования информации, основанный на генерации различных вариантов искажённого кода, которые могут быть распознаны или восстановлены используемой нейросетью. Он может быть использован также в качестве алгоритма помехоустойчивого кодирования, симметричного шифрования данных, в системе аутентификации. Ключом алгоритма шифрования может служить информация о выбранных структурных характеристиках потенциала с заданным набором энергетических минимумов, определяющего динамику нейронной сети как потенциальной динамической системы. Размеры ключа напрямую зависят от длины алфавита исходного сообщения и от формы представления функционала энергии.

Полученные результаты позволяют добиться высокой криптостойкости предложенного алгоритма шифрования. Также с целью повышения имитостойкости и помехозащищенности в процессе передачи данных предложена реализация протокола аутентификации с доказательством знания, основанного на нейрокриптографичекой системе.

Литература

1. Юрьев Р.А. Обзор моделей нейрокриптографии // Вестник научных конференций, 2015, № 4-2 (4). С. 160-164.
2. Гридин В. Н., Солодовников В. И. Построение алгоритма симметричного шифрования на основе нейросетевого подхода // Новые информационные технологии в автоматизированных системах, 2015, №18. с. 98-107.
3. Бобров Р.Б., Вершинин В.Е. Криптографические методы защиты данных с использованием искусственных нейронных сетей // Электронный журнал: наука, техника и образование, 2015, № 3. С. 9-14.
4. Шемякина М.А. Состояние, перспективы и принципы использования нейросетевых технологий в криптографии // Форум молодых ученых, 2018, № 12-4 (28). С. 721-728.
5. Мельников В.А., Шниперов А.Н. Подходы к применению искусственных нейронных систем в криптографических задачах // Актуальные проблемы авиации и космонавтики, 2018, т. 2, № 4 (14). С. 232-234.
6. Пятницкий И. А. Применение нейронных сетей в шифровании // Безопасность информационного пространства – 2017: XVI Всероссийская научно-практическая конференция студентов, аспирантов, молодых ученых. Екатеринбург, 12 декабря 2017 года. Екатеринбург: Изд-во Урал. ун-та, 2018. С. 44-46.

7. Protic Danijela D. Neural cryptography // VOJNOTEHNICKI GLASNIK, 2016, Vol. 64. № 2. p. 483-495.
8. Пьявченко А.О., Лищенко А.В. Нейронные сети адаптивного резонанса - как средство решения задачи распознавания аномальных образов // Аллея науки, 2018, т. 4. № 11 (27). С. 91-100.
9. Баранов К.А., Чайчиц Н.Н. Распознавание образов и обработка данных с использованием нейронных сетей // Актуальные направления научных исследований XXI века: теория и практика, 2018, т. 6. № 6 (42). С. 37-38.
10. Бабич Н.А. Анализ эффективности применения интерференционной нейронной сети для решения задачи распознавания образов // Вестник современных исследований, 2019, № 2.3 (29). С. 5-8.
11. Асяев Г.Д., Никольская К.Ю., Али М.М. Применение нейронной сети для распознавания искусственно сгенерированных образов // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2017. т. 17. № 3. С. 135-141.
12. Гридин В.Н., Солодовников В.И., Евдокимов И.А. Нейросетевой алгоритм симметричного шифрования // Информационные технологии, 2015, т. 21, № 4. С. 306-311.
13. Солодовников В.И., Евдокимов И.А. Анализ криптостойкости нейросетевого алгоритма симметричного шифрования // Новые информационные технологии в автоматизированных системах, 2016, № 19. С. 263-269.
14. Гридин В. Н., Солодовников В. И. Исследование вопросов криптостойкости и методов криптоанализа нейросетевого алгоритма симметричного шифрования // Известия Южного федерального университета. Технические науки, 2016, №7 (180). С. 114-122.
15. Солодовников В.И. Улучшение криптостойкости нейросетевого алгоритма симметричного шифрования за счет использования комитетов нейронных сетей // Новые информационные технологии в автоматизированных системах, 2017, №20. С.176-180.
16. Байбурин В.Б., Розов А.С., Хороводова Н.Ю. Кодирование информации на основе динамических систем электроники // Информационная безопасность регионов, 2015, № 3(20). С. 5-8.
17. Гайфулина Д.А., Котенко И.В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 1 // Журнал «Вопросы кибербезопасности», 2020, № 3 (37). – с. 76-86.
18. Диченко С.А., Финько О.А. Гибридный крипто-кодовый метод контроля и восстановления целостности данных для защищённых информационно-аналитических систем // Журнал «Вопросы кибербезопасности», 2019, № 6 (34). – с. 17-36.
19. Тарасов Я.В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Журнал «Вопросы кибербезопасности», 2017, № 5 (24). – с. 23-29.

Рецезент: *Финько Олег Анатольевич, профессор, доктор технических наук, профессор кафедры, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко, г. Краснодар, Россия, E-mail: ofinko@yandex.ru*

NEURAL CRYPTOGRAPHIC INFORMATION SECURITY SYSTEM OF RECURRENT CONVERGENT NEURAL NETWORKS

***Vlasov K.A.*[2]**

Abstract.

The purpose: *to construct an algorithm for information transformation by recurrent convergent neural networks with a given set of local minima of the energy functional for its subsequent application in the field of information security.*

Method: *system analysis of the existing neural network paradigms that can be used for classification of images. Neural cryptographic system synthesis is with analogy methods, recurrent convergent neural networks, noise- resistant encoding and block ciphers algorithms.*

The result: *a promising neural cryptographic system is proposed that can be used to develop an algorithm for noise-resistant coding, symmetric or stream data encryption based on the generation of various variants of the distorted image representing the sequence of bits to mask the original message. An algorithm for block symmetric data encryption based on Hopfield-type neural networks has been created. Key information includes information on the selected (using radial basic functions) structural characteristics of the potential with a given set of energy minima, which determines the dynamics of the neural network as a potential dynamic system, whose attractors are symbols*

2 Konstantin Vlasov, Krasnodar higher military school named after general of the army S.M. Shtemenko, Krasnodar, Russia. E-mail: meavit@yandex.ru

(several symbols) of the alphabet of the input text. The size of the key depends on the power of the alphabet of the original message and the form of representation of the energy functional. The presented neural cryptographic system can also be used in the authentication system.

Keywords: *neural cryptography, noise-resistant coding, symmetric encryption, a block cipher, authentication system, neural network with feedback, potential dynamical system, radial base function.*

References

1. Yur'ev R.A. Obzor modelej nejrokriptografii // Vestnik nauchnyh konferencij, 2015, № 4-2 (4). S. 160-164.
2. Gridin V.N., Solodovnikov V.I. Postroenie algoritma simmetrichnogo shifrovaniya na osnove nejrosetevogo podhoda // Novye informacionnye tekhnologii v avtomatizirovannyh sistemah, 2015, №18. S. 98-107.
3. Bobrov R.B., Vershinin V.E. Kriptograficheskie metody zashchity dannyh s ispol'zovaniem iskusstvennyh nejronnyh setej // Elektronnyj zhurnal: nauka, tekhnika i obrazovanie, 2015, № 3. S. 9-14.
4. SHemyakina M.A. Sostoyanie, perspektivy i principy ispol'zovaniya nejrosetevyh tekhnologij v kriptografii // Forum molodyh uchenyh, 2018, № 12-4 (28). S. 721-728.
5. Mel'nikov V.A., SHniperov A.N. Podhody k primeneniyu iskusstvennyh nejronnyh sistem v kriptograficheskih zadachah // Aktual'nye problemy aviacii i kosmonavtiki, 2018, t. 2, № 4 (14). S. 232-234.
6. Pyatnickij I. A. Primenenie nejronnyh setej v shifrovanii // Bezopasnost' informacionnogo prostranstva – 2017: XVI Vserossijskaya nauchno-prakticheskaya konferenciya studentov, aspirantov, molodyh uchenyh. Ekaterinburg, 12 dekabrya 2017 goda. – Ekaterinburg: Izd-vo Ural. un-ta, 2018. S. 44-46.
7. Protic Danijela D. Neural cryptography // VOJNOTEHNICKI GLASNIK, 2016, Vol. 64. № 2. P. 483-495.
8. P'yavchenko A.O., Lishchenko A.V. Nejronnye seti adaptivnogo rezonansa - kak sredstvo resheniya zadachi raspoznavaniya anomal'nyh obrazov // Alleya nauki, 2018, t. 4. № 11 (27). S. 91-100.
9. Baranov K.A., CHajchic N.N. Raspoznavanie obrazov i obrabotka dannyh s ispol'zovaniem nejronnyh setej // Aktual'nye napravleniya nauchnyh issledovanij XXI veka: teoriya i praktika, 2018, t. 6. № 6 (42). S. 37-38.
10. Babich N.A. Analiz effektivnosti primeneniya interferencionnoj nejronnoj seti dlya resheniya zadachi raspoznavaniya obrazov // Vestnik sovremennyh issledovanij, 2019, № 2.3 (29). S. 5-8.
11. Asyaev G.D., Nikol'skaya K.YU., Ali M.M. Primenenie nejronnoj seti dlya raspoznavaniya iskusstvenno sgenerirovannyh obrazov // Vestnik YUzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Komp'yuternye tekhnologii, upravlenie, radioelektronika. 2017. t. 17. № 3. S. 135-141.
12. Gridin V.N., Solodovnikov V.I., Evdokimov I.A. Nejrosetevoj algoritm simmetrichnogo shifrovaniya // Informacionnye tekhnologii, 2015, t. 21, № 4. S. 306-311.
13. .Solodovnikov V.I., Evdokimov I.A. Analiz kriptostojkosti nejrosetevogo algoritma simmetrichnogo shifrovaniya // Novye informacionnye tekhnologii v avtomatizirovannyh sistemah, 2016, № 19. S. 263-269.
14. Gridin V. N., Solodovnikov V. I. Issledovanie voprosov kriptostojkosti i metodov kriptoanaliza nejrosetevogo algoritma simmetrichnogo shifrovaniya // Izvestiya YUzhnogo federal'nogo universiteta. Tekhnicheskie nauki, 2016, №7 (180). S. 114-122.
15. Solodovnikov V.I. Uluchshenie kriptostojkosti nejrosetevogo algoritma simmetrichnogo shifrovaniya za schet ispol'zovaniya komitetov nejronnyh setej // Novye informacionnye tekhnologii v avtomatizirovannyh sistemah, 2017, №20. S.176-180.
16. Bajburin V.B., Rozov A.S., Horovodova N.YU. Kodirovanie informacii na osnove dinamicheskih sistem elektroniki // Informacionnaya bezopasnost' regionov, 2015, № 3(20). S. 5-8.
17. Gajfulina D.A., Kotenko I.V. Primenenie metodov glubokogo obucheniya v zadachah kiberbezopasnosti. CHast' 1 // ZHurnal «Voprosy kiberbezopasnosti», 2020, № 3 (37). – s. 76-86.
18. Dichenko S.A., Fin'ko O.A. Gibridnyj kripto-kodovyj metod kontrolya i vosstanovleniya celostnosti dannyh dlya zashchishchyonnyh informacionno-analiticheskih sistem // ZHurnal «Voprosy kiberbezopasnosti», 2019, № 6 (34). – s. 17-36.
19. Tarasov YA.V. Issledovanie primeneniya nejronnyh setej dlya obnaruzheniya nizkointensivnyh DDoS-atak prikladnogo urovnya // ZHurnal «Voprosy kiberbezopasnosti», 2017, № 5 (24). – s. 23-29.