УДК 004.896

В. Н. Гридин, д-р техн. наук, проф., директор, e-mail: info@ditc.ras.ru,
В. И. Солодовников, канд. техн. наук, ст. научн. сотр., e-mail: info@ditc.ras.ru,
И. А. Евдокимов, мл. науч. сотр., e-mail: info@ditc.ras.ru
Центр информационных технологий в проектировании (ЦИТП) РАН, г. Одинцово, МО

Нейросетевой алгоритм симметричного шифрования*

Рассмотрены вопросы применения нейронных сетей для криптографической защиты информации. Проведен анализ особенностей использования ряда нейросетевых парадигм. Предложены алгоритмы шифрования, дешифрования и предобработки данных. Проанализирован ключ шифрования и его влияние на криптостойкость. Исследована возможность применения частотного криптоанализа. Предложена общая схема подсистемы шифрования.

Ключевые слова: *нейронные сети, персептрон, RBF-сети, LVQ-сети, криптографическая защита, шифрование, дешифрование*

Введение

Данные являются ценным ресурсом, доступ к которому необходимо строго контролировать и регламентировать. В целях предупреждения возможной угрозы несанкционированного доступа наиболее часто используют методы криптографической защиты. В настоящее время единственно надежным способом шифрования является метод "одноразового блокнота", предложенный в 1917 г. Гильбертом Вернамом (Gilbert Vernam), поскольку доказана его безусловная секретность, т. е. секретность по отношению к лицу, которое стремится получить несанкционированный доступ к информации и обладает неограниченными временем и вычислительной мощностью. Поэтому непрерывно идет поиск новых подходов и алгоритмов, которые обеспечивали бы надежную сохранность информации. В качестве основы одного из таких подходов предлагается использование нейросетевых технологий. Это объясняется тем обстоятельством, что особенностью ряда нейронных сетей является способность восстановления искаженных сигналов и распознавания объектов, имеющих характеристики, отличные от эталонных. Вместе с тем многие асимметричные криптосистемы основаны на использовании односторонних функций f с секретом, для которых инвертирование функции затруднено. К таким функциям можно отнести сигмоидные (логистические) и радиальные базисные функции, вычисление обратных значений которых проблематично, если неизвестны значения их коэффициентов. Эти же функции используют во многих парадигмах нейронных сетей [1, 2], причем поиск обратного значения здесь усложняется, поскольку это значение может находиться в некоторой области, связанной с функцией некоторым набором правил. Эта сложность зависит от характеристик области (линейные или нелинейные границы, связная или несвязная область и т. д.). Именно эти принципы и положены в основу предлагаемого подхода. Кроме того, алгоритмы на основе нейронных сетей реализуются аппаратно, что позволяет увеличить скорость шифрования и дешифрования данных.

* Работа выполняется по Программе фундаментальных исследований ОНИТ РАН, проект № 2.4.

Общий принцип шифрования на базе нейронных сетей

Предлагаемый алгоритм может быть отнесен к блочным шифрам, что обусловлено структурными особенностями нейронных сетей, а именно фиксированным числом входных элементов и внутренним представлением данных. Без потери общности будем рассматривать алгоритм шифрования некоторой текстовой информации, т. е. будем оперировать символами или наборами символов (классами) и их кодами. В случае необходимости аналогичные рассуждения могут быть проведены для любых кортежей вида $(x_1, ..., x_s)$, состоящих из 0 и 1, где s — размерность блока шифруемых данных. Таким образом, предлагаемый алгоритм применим для любого потока данных.

Системы шифрования обычно включают следующие основные компоненты [3]:

- ключ шифрования;
- алгоритм шифрования, который определяет способ преобразования исходных данных в зашифрованные с помощью ключа шифрования;
- ключ дешифрования;
- алгоритм дешифрования, который задает, как с помощью ключа дешифрования преобразовать зашифрованные данные в исходные.

Рассмотрим, как соотносятся указанные компоненты с нейросетевым подходом. Так, в систему могут быть включены несколько шаблонов различ-

ных нейронных сетей (многослойный персептрон, сети с радиальными базисными функциями RBF, LVQ-сети и т. д.) [1, 2]. Выбранную парадигму для конкретного случая можно считать одной из составных частей ключа шифрования и дешифрования. Чтобы использовать сеть, необходимо задать ее структурные характеристики: число слоев, число нейронов в слое, значения весовых коэффициентов, функции активации, пороговые значения и т. д. Эти характеристики используются как еще одна составная часть ключа. Они определяют алгоритмы шифрования и дешифрования и, с одной стороны, зависят от нейронной сети, а с другой стороны, определяются представлением кода — его длиной, числом одновременно кодируемых символов и т. п.

Алгоритм шифрования основывается на поиске искаженного кода, который может распознать или восстановить используемая сеть с заданными характеристиками [4]. В наиболее общем случае можно выделить два варианта:

- если известна область, в которой допустимы искажения кода символа или группы символов, код выбрасывается датчиком случайных чисел в этой области;
- если такая область неизвестна, датчик случайных чисел выбрасывает произвольный код; этот код пропускается через нейронную сеть; если требуемый код не удается восстановить, процесс повторяется до тех пор, пока не будет восстановлен код.

Таким образом, важным вопросом при построении нейросетевой системы шифрования является подготовка данных и формирование областей допустимых искажений кода. С одной стороны, это обусловлено тем обстоятельством, что во втором случае, когда генерируется произвольный код, процесс шифрования может занимать довольно длительные промежутки времени. С другой стороны, для улучшения стойкости получаемого шифротекста необходимо стремиться к равномерному распределению кодов символов (классов) в пространстве шифрования, что способно сильно затруднить процесс частотного криптоанализа.

Алгоритм дешифрования заключается в распознавании поступающего на вход сети шифротекста. В результате на выходе пользователь получает набор исходных символов (кодов классов).

Алгоритм шифрования

Для реализации алгоритма шифрования необходимо рассмотреть следующие основные этапы [4]:

- предварительный этап, на котором осуществляется предобработка данных [5] и формируется обучающее множество с учетом частотности появления символов из исходного алфавита (формирование кластеров);
- построение нейросети — выбор нейросетевой парадигмы, определение структуры нейронной сети и задание значений весовых коэффициентов (обучение);
- основной этап, на котором происходит процесс шифрования.

Предварительный этап и формирование нейросети обязательно должны предшествовать этапу шифрования, однако после получения обученной сети процесс шифрования может осуществляться многократно.

На рис. 1 представлены основные составляющие блока шифрования.

Предварительный этап. Для создания обучающего множества используется информация о частотности появления символов (групп символов) из исходного алфавита. Если такие данные отсутствуют, то проводится анализ исходного текста и рассчитывается частота вхождения каждого символа в шифруемом сообщении $\alpha(n_1...n_t)$, где t — число различных символов в исходном тексте; n_i — число вхождения i-го символа в исходный текст.

Формирование областей (кластеров) пространства шифрования, в границах которых будут осуществляться искажения кодов символов, состоит из следующих шагов.

1. Автоматически генерируется число областей для каждого символа (класса) с учетом частотного анализа α. В результате получается вектор числа областей $\gamma(m_1...m_t)$, где t — число различных символов (классов); m_i — число областей для i-го класса.

2. Случайным образом формируются области, соответствующие каждому символу в зависимости от векторов $\gamma(m_1...m_t)$. Число областей для каждого символа будет различным. Область задается в виде обучающей выборки — набора близко лежащих

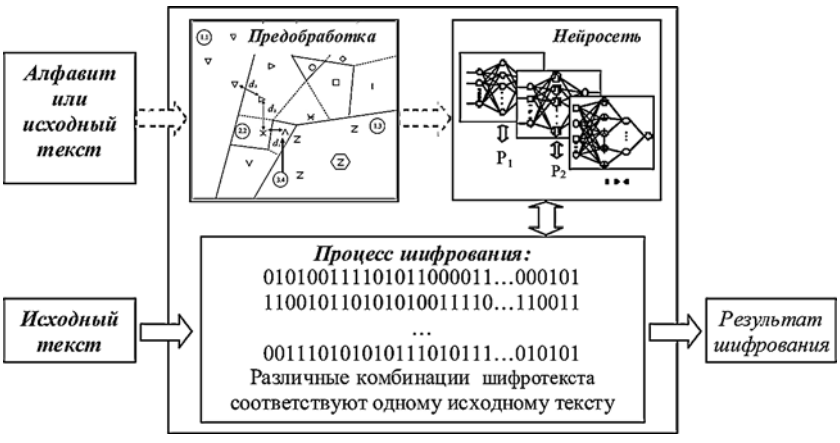

Рис. 1. Блок шифрования: предобработка, формирование нейросети, основной этап

векторов с указанием их класса. При этом вновь сгенерированные вектора сравниваются с уже полученными, что гарантирует принадлежность каждого вектора к единственному классу.

В качестве примера рассмотрим следующее шифруемое сообщение: *"jerome k. jerome. three men in a boat (to say nothing of the dog). there were four of us — george, and william samuel harris, and myself, and montmorency."*. Несложно заметить, что частотность появления символов неравномерна. Так, пробел встречается 28 раз, "*e*" — 17 раз, а символы *k*, *b*, *c*, (,), — всего по одному разу. Основные статистические показатели шифруемого текста приведены в таблице.

Статистика шифруемого текста

Общее число символов в сообщении M	154
Размер алфавита A	27
Среднее значение частоты появления символа $F_{average}$	0,037
Минимальное значение частоты появления символа F_{min}	0,0065
Максимальное значение частоты появления символа F_{max}	0,1818

На рис. 2 (см. третью сторону обложки) приведено сравнение частотности символов во входной последовательности и распределение точек в пространстве шифрования по соответствующим классам входной последовательности.

Из рисунка видно, что графики очень близки. Данная особенность гарантирует равномерное распределение символов входной последовательности по области шифрования, что делает затруднительным применение к алгоритму методов частотного криптоанализа.

Построение нейронной сети. После предобработки данных и формирования обучающего множества строится нейронная сеть. Прежде всего выбирается нейросетевая парадигма. Затем формируется структура сети, задаются значения весовых коэффициентов, проводится обучение.

Построение различных типов нейросетей имеет свои индивидуальные особенности, но преследует единую цель: научиться распознавать и классифицировать искаженный код из областей, сформированных на предварительном этапе. Фактически создается ключ шифрования, который в данном случае будет представлять собой информацию о выбранном типе нейросети и значениях ее структурных характеристик: число нейронов в каждом слое, весовые коэффициенты слоев $W1$ и $W2$.

Процесс обучения определяется внутренним представлением данных выбранной сети [1]. Так, для многослойного персептрона характерно разбиение пространства входных данных посредством гиперплоскостей или поверхностей. Правила классификации входного значения содержатся в весовых коэффициентах, функциях активации и связях между нейронами, но обычно их структура слишком сложна. Таким образом, как правило, не представляется возможным отделить влияние определенного признака на целевое значение, потому что этот эффект может быть опосредован значениями других параметров. В связи с этим особенностью использования нейронных сетей данного типа применительно к задаче шифрования является необходимость отдельно хранить информацию об областях допустимых искажений кода. Также потребуется обучение сети решению задачи классификации, что для данного типа сети может занять довольно продолжительное время.

Нейросети, использующие радиальные базисные функции в нейронах промежуточного слоя, основаны на разбиении пространства окружностями или в общем случае гиперсферами (групповое представление) [1]. С точки зрения задачи аппроксимации скрытые элементы RBF-сети формируют совокупность функций (локальной поддержки), которые образуют базисную систему для представления входных примеров в построенном на ней пространстве. Вследствие чего такие сети, в отличие от многослойного персептрона, не умеют экстраполировать свои выводы за область известных данных. При удалении от обучающего множества значение функции отклика быстро спадает до нуля, таким образом RBF-нейроны действуют в достаточно малой области входного пространства, и чем шире пространство (число входов и расстояние между ними), тем больше требуется нейронов.

При построении RBF-сети для задачи шифрования в качестве центров скрытых радиально-базисных элементов могут быть выбраны центры областей допустимых искажений кода. В этом случае необходимо подобрать ширину функции активации. Другим вариантом может служить соотнесение некоторого множества RBF-нейронов каждому шифруемому символу, что позволяет задавать довольно сложные области искажений, в том числе несвязанные. Число элементов в каждом множестве необходимо задавать с учетом частотного анализа исходного алфавита и стремиться к равномерному распределению кодов символов в пространстве шифрования.

Поиск значений весовых коэффициентов линейного выходного слоя может как осуществляться с помощью алгоритмов обучения RBF-сети, так и задаваться пользователем. В частности, пользователь

может указать, какому символу (группе символов) исходного алфавита соответствует RBF-нейрон. Для этого значение весового коэффициента, связывающего скрытый радиально-базисный элемент с соответствующим нейроном выходного слоя, задается равным 1, а значения всех остальных весовых коэффициентов равными 0.

Основной этап алгоритма шифрования. Основной этап заключается в формировании шифротекста, который может быть распознан используемой нейронной сетью. На вход модуля шифрования подается исходное сообщение. Далее последовательно выполняется такой набор действий.

1. Из исходного текста выделяется очередной символ или группа символов используемого алфавита, т. е. определяется класс.

2. Для найденного класса случайным образом выбирается эталонный вектор, который характеризует определенный кластер (область), соответствующий данному классу. Для нейронных сетей, использующих RBF-нейроны, эталонный вектор может быть взят из матрицы $W1$, тогда как для персептрона необходимо отдельно хранить информацию об областях допустимых искажений кода.

3. Для данного кластера случайным образом выбирается вектор $p = (x_1 ... x_r)$ (где x_i — значение i-й координаты вектора, а r — размерность области определения), для которого результат работы сети $net(p)$ соответствует исходному классу. Тем самым мы получаем случайный вектор, принадлежащий выбранному кластеру и классу.

4. Полученный шифр $p = (x_1 ... x_r)$ сохраняется, а алгоритм переходит к следующему символу. Диаграмма потоков данных модуля шифрования представлена на рис. 3.

Результатом работы будет набор векторов $p_1(x_1 ... x_r) ... p_K(x_1 ... x_r)$, который соответствует полученному зашифрованному тексту, где K — число символов или групп символов в исходном сообщении. Полученная последовательность не является числовыми кодами символов, поэтому прочитать ее, не имея ключа, не представляется возможным. Данный алгоритм позволяет шифровать одни и те же символы или группы символов различными кодовыми последовательностями, причем находиться они могут в несвязанных областях.

Алгоритм дешифрования

Алгоритм дешифрования заключается в распознавании полученного шифротекста. Ключ дешифрования является составным ключом, включающим топологию сети и ее основные характеристики, в частности матрицы весовых коэффициентов $W1$ и $W2$. На вход алгоритма поступает зашифрованное сообщение, из которого выделяется очередной вектор пространства, в котором осуществлялось шифрование. Полученный вектор подается на вход сети, где происходит прямое прохождение сигнала и его классификация, т. е. определяется класс и выбирается соответствующий символ исходного алфавита.

Диаграмма потока данных модуля дешифрования представлена на рис. 4.

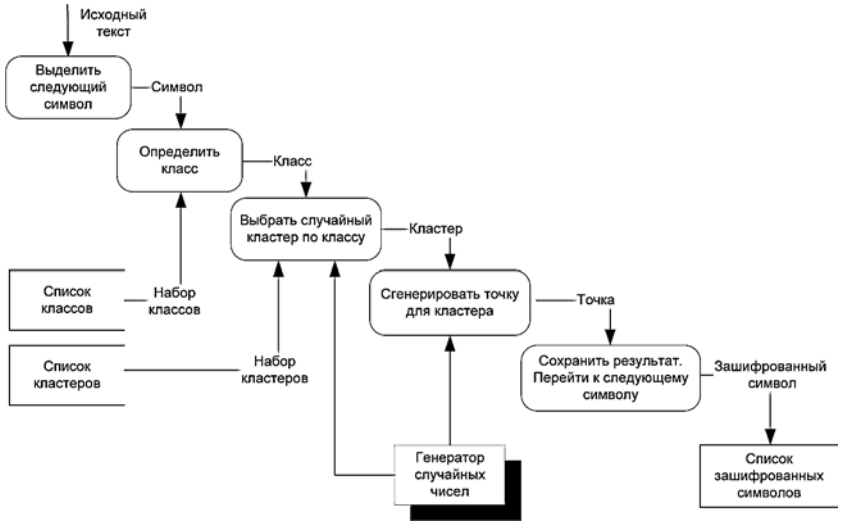

Рис. 3. Диаграмма потоков данных модуля шифрования

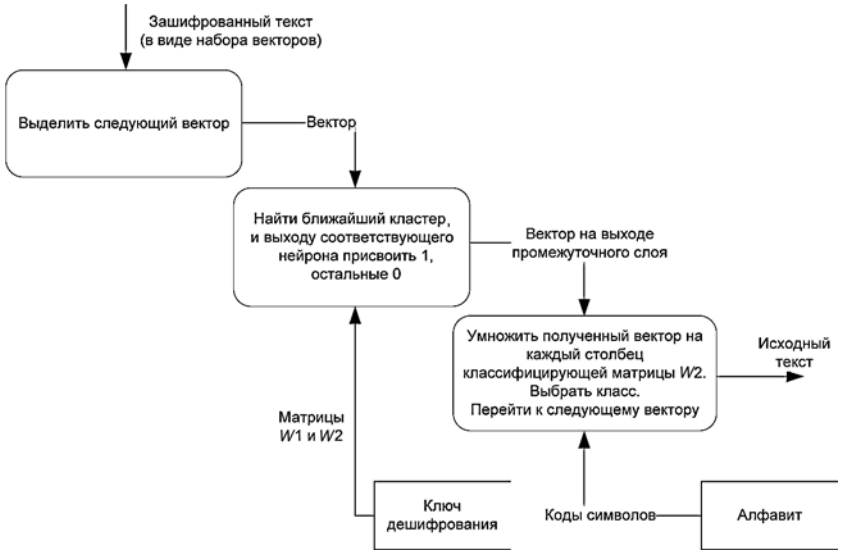

Рис. 4. Диаграмма потока данных модуля дешифрования

Полученный текст сохраняется, а алгоритм переходит к следующему элементу зашифрованного сообщения.

Анализ алгоритма и ключей шифрования

Предложенный алгоритм шифрования с использованием нейронных сетей основывается на генерации случайных чисел. Ключом шифрования и дешифрования является сама нейросеть, а именно выбранная парадигма и ее структурные характеристики. Эти значения, с одной стороны, зависят от нейронной сети, а с другой стороны, определяются представлением кода — его длиной, числом одновременно кодируемых символов и т. п. При использовании для обучения истинно случайных чисел и достаточно большой области обучения (пространства, в котором осуществляется шифрование) вероятность получения одинаковых топологий сети крайне мала. Все полученные топологии являются равноправными, т. е. и ключи шифрования являются равноправными. Невозможно установить простые зависимости между ключами, используемыми в процессе шифрования.

При формировании обучающего множества сначала составляется вектор классов $C = C_1 \ldots C_c$, где C_i — i-й класс, характеризующий символ или группу символов, c — общее число классов. Затем формируется вектор кластеров $K = (x_1 \ldots x_s)_1 \ldots (x_1 \ldots x_s)_k$, где k — число кластеров, $k \geqslant c$; $(x_1 \ldots x_s)_i$ — координаты i-го кластера; s — размерность пространства, в котором осуществляется шифрование. Матрица $W1$ имеет размер $s \times k$. Для сетей, использующих RBF-нейроны, матрица состоит из элементов, характеризующих координаты кластеров. Для многослойного персептрона k характеризует не число кластеров, а число нейронов промежуточного слоя, достаточное для разделения кластеров. В свою очередь, матрица $W2$ имеет размер $k \times c$. Так как для сохранения целостности задачи требуется передавать в качестве ключа шифрования всю топологию сети, то размер ключа вычисляется по формуле

$$N = s \cdot k \cdot b + k \cdot c \cdot b,$$

где b — число бит, необходимое для хранения значения весового коэффициента.

Из приведенной формулы видно, что размер ключа прямо пропорционален числу используемых кластеров и размерности пространства, в котором осуществляется шифрование. Данное обстоятельство может быть использовано пользователем для улучшения криптостойкости алгоритма, так как размер ключа связан с количеством вычислений, требуемых для подбора ключей, соотношением $N_{\text{операций}} = 2^N$.

Однако, используя особенности различных нейросетевых парадигм, в приведенную формулу могут быть внесены некоторые изменения. Например, для сетей, использующих RBF-нейроны, в частности для сети LVQ, другим вариантом подсчета требуемого объема памяти для матрицы $W2$ является указание класса для текущего кластера в виде пары [номер кластера, номер класса], так как все остальные веса равны 0, то их можно не учитывать. Тогда для второго слоя достаточно k пар или $2 \cdot k \cdot b'$ бит, где b' бит необходимо для хранения номера нейрона. В этом случае $N = s \cdot k \cdot b + 2 \cdot k \cdot b'$.

Для сетей класса многослойный персептрон нет необходимости использовать в выходном слое число нейронов, равное числу классов, а можно воспользоваться кодированием номера класса с помощью бинарного вектора. В этом случае число нейронов в выходном слое будет равно значению $c' = \log_2 c$, округленному до большего целого. Кроме того, для данного типа нейросетей число нейронов промежуточного слоя k' не характеризует число кластеров, а должно быть достаточным для разделения имеющихся кластеров в пространстве шифрования. Для двумерной плоскости его можно оценить исходя из числа прямых, которое необходимо для разбиения плоскости на k областей.

Если рассматривать тестовое шифруемое сообщение из предварительного этапа, то размер алфавита и число классов $c = 27$. Число кластеров не может быть меньше 27, так как каждому классу должен соответствовать хотя бы один кластер. Размерность пространства шифрования равна 2. На рис. 5 (см. третью сторону обложки) представлены графики с оценочными значениями количества бит, необходимого для хранения значений весовых коэффициентов, для следующих вариантов нейросетей:

- НС1 — многослойный персептрон, у которого число нейронов выходного слоя равно c, число нейронов промежуточного слоя меняется от 7 до 10 в зависимости от числа кластеров, для хранения весового коэффициента используется 64 бита;
- НС2 — многослойный персептрон, аналогичный НС1, но у которого число нейронов выходного слоя закодировано с помощью бинарного вектора и равно 5;
- НС3 — нейросеть с RBF-нейронами промежуточного слоя, где для хранения весовых коэффициентов используется по 16 бит;
- НС4 — нейросеть, аналогичная НС3, но для хранения весовых коэффициентов промежуточного слоя (кластеров) используется 64 бита.

Размер ключа зависит от размерности пространства, в котором осуществляется шифрование, и от числа классов, характеризующих символ или группу символов. Однако необходимо учитывать тот факт, что с ростом размерности пространства s также увеличивается и длина получаемого шифротекста,

что нежелательно, поэтому данный параметр стоит использовать крайне осторожно. Увеличение длины получаемого шифротекста может быть компенсировано с помощью введения дополнительных классов, которые будут включать не единичные символы, а часто встречающиеся в тексте цепочки символов, но это потребует дополнительных вычислительных затрат на предварительном этапе в процессе построения сети.

Заключение

В статье рассмотрены принципы применения нейронных сетей для криптографической защиты информации. В основу предлагаемого подхода положена способность ряда нейронных сетей к восстановлению искаженных сигналов и распознаванию объектов, имеющих характеристики, отличные от эталонных. Рассмотрены особенности применения многослойного персептрона и сетей, использующих радиальные базисные функции в нейронах промежуточного слоя. Предложены алгоритмы шифрования, дешифрования и предобработки данных. Алгоритм шифрования основан на генерации различных вариантов искаженного кода, который может распознать или восстановить используемая сеть. Ключ шифрования и дешифрования включает информацию о выбранном шаблоне нейросети и ее структурных характеристиках (число нейронов в слое, весовые коэффициенты, функции активации, пороговые значения и т. д.). Показана зависимость ключа от числа используемых кластеров и размерности пространства шифрования. Данный подход может быть использован для решения задач защиты информации, хранящейся на электронных носителях и передаваемой по различным каналам связи, как на персональном, так и на корпоративном уровне.

Список литературы

1. **Ежов А., Шумский С.** Нейрокомпьютинг и его применение в экономике и бизнесе. М.: МИФИ, 1998. 224 с.
2. **Медведев В. С., Потемкин В. Г.** Нейронные сети. MATLAB 6. М.: Диалог МИФИ, 2002. 496 с.
3. **Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.** Основы криптографии. М.: Гелиос АРВ, 2005. 480 с.
4. **Гридин В. Н., Солодовников В. И., Евдокимов И. А.** Применение нейросетевого подхода на основе LVQ-сети для шифрования текстовой информации // Системы высокой доступности. 2011. Т. 7, № 1. С. 65—68.
5. **Евдокимов И. А., Гридин В. Н., Солодовников В. И., Солодовников И. В.** Предобработка данных с учетом заданных значений отдельных признаков // Информационные технологии и вычислительные системы. 2009. № 1. С. 14—17.

V. N. Griding, Prof., Doctor of Science, Director, **V. I. Solodovnikov,** Ph. D., Senior Researcher,
I. A. Evdokimov, Junior Researcher
Design information technologies Center Russian Academy of Sciences (DITC RAS)
Russia, Moscow region, Odintsovo, st. Marshal Biryuzova 7a, tel.: (495) 596-02-19, e-mail: info@ditc.ras.ru

Neural Network Algorithm for Symmetric Encryption

Data is a valuable resource, with access which is necessary to be strictly monitored and regulated. Even the partial loss of such data can have dire consequences for the owner. One of the most popular approaches, used to prevent the possible threat of unauthorized access, is the cryptographic protection or encryption.

The article investigates the possibility of using neural network methods for the cryptographic protection of information. The proposed approach is based on the ability of some neural networks for restoration of distorted signals and recognition of objects having characteristics different from the references. The features of using multilayer perceptron and networks with RBF-neurons in the intermediate layer were considered. Algorithms of encryption, decoding and data preprocessing were proposed. The basic idea of the encryption algorithm is to generate a distorted code that can be recognized or restored by the network. The encryption and decoding key includes information about the selected neural network template and its structural characteristics (the number of neurons in layer, weights, activation functions, threshold values, etc.). The encryption key dependences on number of used clusters and the dimension of encryption space were considered.

Keywords: *neural network, perceptron, RBF neural network, LVQ neural network paradigm, cryptographic protection, encryption, decoding*

References

1. **Ezhov A., Shumskij S.** *Nejrokompjuting i ego primenenie v ekonomike i biznese.* M.: MIFI, 1998. 224 p.
2. **Medvedev V. S., Potemkin V. G**. *Nejronnye seti. MATLAB 6.* M.: Dialog MIFI, 2002. 496 p.
3. **Alferov A. P., Zubov A. Ju., Kuzmin A. S., Cheremushkin A. V.** *Osnovy kriptografii.* M.: Gelios ARV, 2005. 480 p.
4. **Gridin V. N., Solodovnikov V. I., Evdokimov I. A.** Primenenie nejrosetevogo podhoda na osnove LVQ-seti dlja shifrovanija tekstovoj informacii. *Sistemy vysokoj dostupnosti.* 2011. V. 7, N. 1. P. 65—68.
5. **Evdokimov I. A., Gridin V. N., Solodovnikov V. I., Solodovnikov I. V.** Predobrabotka dannyh s uchetom zadannyh znachenij otdel'nyh priznakov. *Informatsionnye tehnologii i vychislitel'nye sistemy.* 2009. N. 1. P. 14—17.