Нейронные сети в криптографии

**Нейрокриптография** — раздел криптографии, изучающий применение [стохастических](http://cryptowiki.net/index.php?title=%D0%A1%D1%82%D0%BE%D1%85%D0%B0%D1%81%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9) алгоритмов, в частности, [нейронных сетей](http://cryptowiki.net/index.php?title=%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), для шифрования и [криптоанализа](http://cryptowiki.net/index.php?title=%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7).

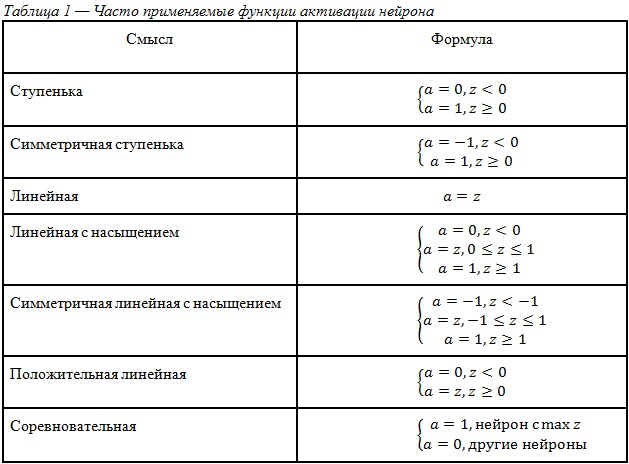
Искусственные нейронные сети

**Основные определения**

Искусственная нейронная сеть (ИНС) — [математическая модель](http://cryptowiki.net/index.php?title=%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C), а также её программная или аппаратная реализация, построенная по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма.

Искусственный нейрон — устройство, обеспечивающее вычисление функции: [](http://cryptowiki.net/index.php?title=File:Neuro1.jpg),где a — скалярный выход нейрона, W — весовая (1 × m) — матрица-строка, p — вектор-столбец входных сигналов, b — скаляр, называемый смещением, f — функция активации, скаляр: [](http://cryptowiki.net/index.php?title=File:Neuro2.jpg),где z — чистый вход (дискриминантная функция) нейрона.

В таблице 1 приведены часто используемые функции активации.

[](http://cryptowiki.net/index.php?title=File:Neuro3.jpg)

Число входов нейрона определяется семантикой решаемой проблемы. Если, например, стоит задача определения лётная сегодня погода или нет, то входами нейрона представляется целесообразно сделать скорость ветра, температуру воздуха и влажность. Таким образом входов у нейрона, решающего данную проблему, будет три. Системы с одним нейроном имеют значительную область применения, поскольку вычислять линейные функции вектора данных требуется во многих приложениях. Среди них кодирование, декодирование, фильтрация (отделение сигнала от шума), выделение контуров на изображениях, статистическая обработка. Линейные функции применяются также в простейших задачах классификации для двух классов. Если классифицируемых типов объектов больше двух, то одного нейрона будет недостаточно.

Слой нейронов — это множество нейронов, которое имеет один общий входной вектор. Слой нейронов включает весовую матрицу, сумматоры, вектор смещений b, блоки, реализующие функции активации, выходной вектор a. Каждый элемент входного вектора p соединён с каждым нейроном через весовую матрицу W размерности (n × m), где n — число нейронов в слое. Как правило, нейронная сеть является многослойной. Существуют входной и выходной слои. Слои нейронов, расположенные между ними, называются скрытыми слоями нейронной сети. Искусственные нейронные сети делятся на сети прямого распространения и рекуррентные нейронные сети. Многослойной нейронной сетью прямого распространения называется сеть, включающая набор слоёв нейронов, для которых выход каждого предыдущего слоя служит входом для последующего. Рекуррентная нейронная сеть — это сеть с обратной связью, т.е. некоторые из выходов нейронной сети снова подаются на её входы.

**История создания и развития ИНС**

Впервые понятие искусственной нейронной сети было упомянуто в 1940-х годах в работах [МакКаллога](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D0%BA-%D0%9A%D0%B0%D0%BB%D0%BB%D0%BE%D0%BA,_%D0%A3%D0%BE%D1%80%D1%80%D0%B5%D0%BD) и Питтса[[1]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8" \l "McCuPi90" \o "Список литературы к разделу Нейронные сети в криптографии), в которых описываются основные возможности сетей из искусственных нейронов. На практике ИНС впервые применили в 1950-х годах, и связано это событие было с изобретением персептрона Френком [Розенблаттом](https://ru.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D0%B5%D0%BD%D0%B1%D0%BB%D0%B0%D1%82%D1%82,_%D0%A4%D1%80%D1%8D%D0%BD%D0%BA). Приблизительно в то же время Видров и Хофф предложили другой обучающий алгоритм для настройки адаптивных линейных нейронных сетей. В научных трудах [Минского](https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BD%D1%81%D0%BA%D0%B8%D0%B9,_%D0%9C%D0%B0%D1%80%D0%B2%D0%B8%D0%BD_%D0%9B%D0%B8) и Пайперта было выявлено, что сети Розенблатта и Видрова имеют ограничения, которые сужают их область действия. Кроме того, отрасль, занимающаяся исследованиями нейронных сетей, значительно замедлилась в развитии в виду того, что на тот момент не существовало электронных вычислительных машин, вычислительных ресурсов которых было бы достаточно для работы с искусственными нейронными сетями. Примерно на 10 лет исследования в данной области практически прекратились. К 80-м годам прошлого века мощные на тот момент персональные компьютеры и рабочие станции стали более доступны, что породило новую волну исследований.

По существу, многослойная ИНС представляет собой вычислительную среду параллельного действия с адаптацией на параметрическом, алгоритмическом и структурном уровне управляемых процессов. Существующие в настоящее время микропроцессорные средства могут реализовать функции нейронных сетей при создании для них соответствующего программного обеспечения, но всё же более перспективным считается применение нейрочипов, архитектура которых специально ориентирована на выполнение соответствующих операций[[2]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#G05).

Искусственные нейронные сети используются повсеместно. Число их приложений, вкладываемые средства в их разработку, а также интерес к ним постоянно растут. Они используются в системах прогнозирования трафика на дорогах, в системах распознавания образов (в том числе лиц людей, например), существуют даже модели систем управления вертолетами на базе ИНС. Спектр задач, решаемых с использованием ИНС велик: классификация объектов, аппроксимация функции по конечному набору её значений, оптимизация, построение отношений на множестве объектов, смысловой поиск информации и ассоциативная память, управление динамическими системами и пр.

**Применение искусственных нейронных сетей для решения задач ИБ**

Искусственные нейронные сети благодаря своей архитектуре в действительности представляют собой эффективный способ параллельной обработки данных. Данное свойство ИНС позволяет в перспективе применять их для широкого круга задач, однако часто сложность реализации такой системы сводит на нет её практическую применимость. Но несмотря на данный факт ИНС весьма широко применяются для защиты информации, как в рамках научно-исследовательских проектов, так и в рамках коммерческих продуктов.

Существуют решения, построенные на базе искусственных нейронных сетей, позволяющие обеспечивать доступность данных[[3]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#C.D0.BB.D0.98.D1.80.D0.9A.D0.BE.D0.91.D0.B509).

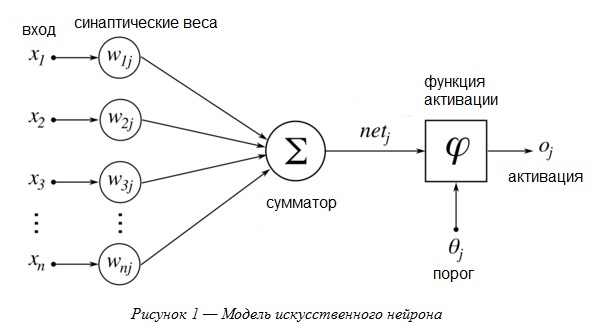
Системы цифровых водяных знаков, построенные с использованием искусственных нейронных сетей, позволяют обеспечивать защиту авторского права[[4]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#BaSi08).

Архитектура искусственных нейронных сетей позволяет эффективно выполнять работы по распознаванию образов и классификации множества объектов по какому-либо признаку. Кроме того, благодаря правильно спроектированным алгоритмам обучения нейронные сети могут достигать крайне высоких показателей точности. Приведенные выше преимущества позволяют эффективно использовать искусственные нейронные сети в системах биологической аутентификации.

В частности, существует ряд работ, посвященных распознаванию подписи человека с использованием искусственных нейронных сетей[[5]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#TrReMcCa08), распознаванию лица человека[[6]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#HeBaKa99). В России существует стандарт [ГОСТ Р 52633-2006](http://csd.faculty.ifmo.ru/files/52633-2006.pdf), определяющий требования к средствам высоконадёжной биометрической аутентификации. При биометрической аутентификации в соответствии с данным стандартом используется многослойная нейронная сеть. Недавно была опубликована статья Григория Маршалко[[7]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8" \l "Ma14" \o "Список литературы к разделу Нейронные сети в криптографии) , посвященная анализу данного стандарта.

Построение функции хэширования с использованием ИНС

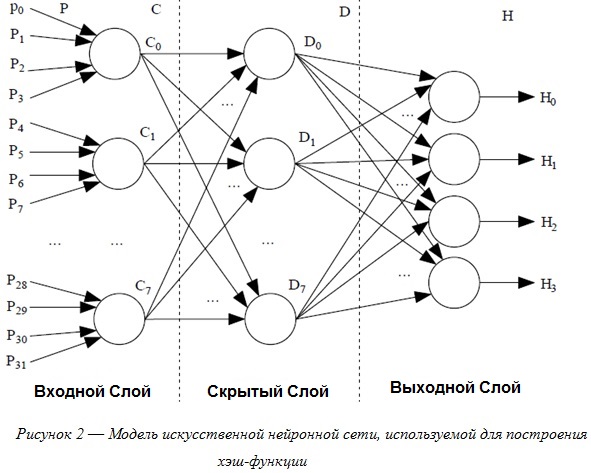
Сама модель искусственных нейронных сетей хорошо подходит для построения хэш-функций на её основе. Искусственный нейрон является базовым блоком при построении ИНС. Рассмотрим модель искусственного нейрона, представленную на Рисунке 1.

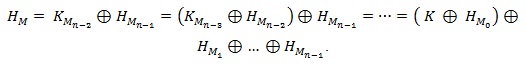
[](http://cryptowiki.net/index.php?title=File:Neuro4.jpg)

У представленного на рисунке нейрона n входов, n весовых характеристик по одной на каждый вход, смещение, которое подаётся на вход функции активации и одно выходное значение. Таким образом, зная входной вектор вычислить выходное значение легко, однако задача получения входного вектора нейрона по известному выходному значению представляется трудноразрешимой. На основании этих рассуждений можно сделать вывод о том, что искусственные нейронные сети обладают свойством однонаправленности[[8]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8" \l "T14" \o "Список литературы к разделу Нейронные сети в криптографии).

**Анализ существующих алгоритмов хэширования, использующих ИНС**

Существует ряд научных работ, посвященных созданию алгоритмов [хэширования](http://cryptowiki.net/index.php?title=%D0%A5%D1%8D%D1%88%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), использующих ИНС. Используемая в них ИНС изображена на рисунке 2[[9]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#LiSuWa07).

[](http://cryptowiki.net/index.php?title=File:Neuro5.jpg)

Используется трехслойная нейронная сеть прямого распространения и хаотическое отображение. Как правило в качестве хаотического отображения применяется некоторое количество итераций кусочно-линейной функции с контролирующим параметром. Хаотичность отображения при этом определяется значением параметра. Исследования показывают[[10]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#LiSuWa05), что при правильном выборе количества итераций хаотического отображения выходное значение функции будет сильно отличаться при незначительных изменениях во входных параметрах. В приведенных работах в скрытом слое нейронов хаотическое отображение не итерируется, для того, чтобы сократить количество операций, требуемых для вычисления функции [хэширования](http://cryptowiki.net/index.php?title=%D0%A5%D1%8D%D1%88%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), а на входном и выходном слоях нейронной сети производится T (T ≥ 50) итераций. На основе описанной выше искусственной нейронной сети и генератора ключей строится алгоритм [хэширования](http://cryptowiki.net/index.php?title=%D0%A5%D1%8D%D1%88%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Генератор ключей преобразует ключ пользователя в набор весовых характеристик, смещений и управляющих параметров, для каждого слоя. Алгоритм переводит данные произвольной длины в 128-битное значение хэш-функции. Для этого данные сначала добиваются до кратности блоку длиной 1024 бита, который и подается на вход нейронной сети, по следующему алгоритму: в последний некратный блок дописываем одну единицу и остальные нули. После этого каждый блок подаётся на вход нейронной сети. Результат вычисляется по формуле: [](http://cryptowiki.net/index.php?title=File:Neuro6.jpg)

**Достоинства и недостатки алгоритмов хэширования, использующих ИНС**

Исследования показывают[[9]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#LiSuWa07), что построенный алгоритм [хэширования](http://cryptowiki.net/index.php?title=%D0%A5%D1%8D%D1%88%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) с использованием искусственной нейронной сети обладает свойством односторонности, высокой чувствительности выходного значения к входным данным и ключу пользователя. Кроме того, описанный алгоритм защищен от атак «дней рождения» и атак «встреча по середине». В приведенных примерах все слои искусственной нейронной сети и генератор ключей реализованы с помощью операций сложения/вычитания и умножения/деления. Модель искусственной нейронной сети позволяет проводить эти вычисления параллельно, что позволит улучшить временные показатели приведенных алгоритмов. При использовании параллельных вычислений число операций у приведенного алгоритма, построенного на базе искусственной нейронной сети, становится меньше, чем у таких алгоритмов, как MD5 и SHA-1[[10]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#LiSuWa05).

Однако описанная схема имеет и ряд недостатков. Прежде всего это лишнее усложнение модели, т.к. для корректного функционирования хэш-функции требуется ключ. Как правило, функции хэширования работают без ключа, в случае же с алгоритмом, описанным выше, ключ требуется для генерации параметров нейронной сети. Иными словами, статическое задание параметров искусственной нейронной сети нарушит требование однонаправленности преобразования. Кроме того, как видно из архитектуры представленной выше нейронной сети — для корректной проверки полученного значения требуется синхронизация ключей. То есть если пользователь захочет проверить значение функции хэширования для некоторых данных — ему потребуется знать ключ, использованный при вычислении этого значения, т.к. из разных ключей будут генерироваться различные наборы характеристик нейронной сети. Для синхронизации ключей используются древовидные машины чётности, которые в свою очередь также являются разновидностью нейронных сетей[[10]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#LiSuWa05).

Шифрование

**Анализ существующих алгоритмов шифрования на основе ИНС на примере AES**

Также модель искусственной нейронной сети подходит для задач шифрования.

Задача шифрования будет рассмотрена на примере алгоритма AES. AES (Advanced Encryption Standard) является итеративным блочным шифром, который был выбран NIST в качестве международного стандарта и замены DES. В настоящее время является наиболее широко распространенным блочный шифром. Rijndael является итеративным блочным шифром, шифрование или расшифрование блока данных осуществляется c помощью раундовой функции. Три стандартные версии AES называются AES-128, AES-192 и AES-256 и отличаются друг от друга длиной ключа (128, 192, и 256 бит) и количеством раундов (10, 12, и 14) Их безопасность была тщательно исследована АНБ. Тем не менее, в последнее время появились некоторые виды атак, которые, как было доказано, достаточно эффективно применяются к AES. Чтобы противостоять этим атакам, можно сделать некоторые изменения, внедрив нелинейную нейронную сеть в AES[[11]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#AmMa11).

Нейронные сети используются для классификации и аппроксимации функций/выделения задач, которые устойчивы к некоторым неточностям, для которых имеется много доступных данных для обучения, но к которым не могут быть применены жесткие правила. Автор статьи попытался реализовать Rijndael-криптосистему с помощью ИНС. Эта криптосистема имеет менее сложное строение, чем AES и не линейна в эксплуатации. Нелинейной должна быть нейронная сеть с обратной связью, что позволило бы выполнить шифрование/расшифрование открытого текста/зашифрованного текста с высокой производительностью и очень низким уровнем ошибок. Идея автора состояла в том, чтобы разработать такую нелинейную ИНС. Нелинейность необходима для уменьшения вероятности взлома алгоритма. Уменьшение вероятности взлома достигается с помощью нелинейной функции активации, также свойство нелинейной аппроксимации сети является полезным для практического применения.

Многослойный [персептрон](http://cryptowiki.net/index.php?title=%D0%9F%D0%B5%D1%80%D1%81%D0%B5%D0%BF%D1%82%D1%80%D0%BE%D0%BD) (MLP) является наиболее популярным видом ИНС прямого распространения, его свойством является способность эмулировать любое соотношение входов/выходов. MLP отвечает здесь за частоту обновления, так как он обновляет веса после того, как весь блок обучающих данных представлен полностью. Блочная адаптация является более надежной с того момента, когда шаг обучения усреднен по всем обучающим шаблонам.

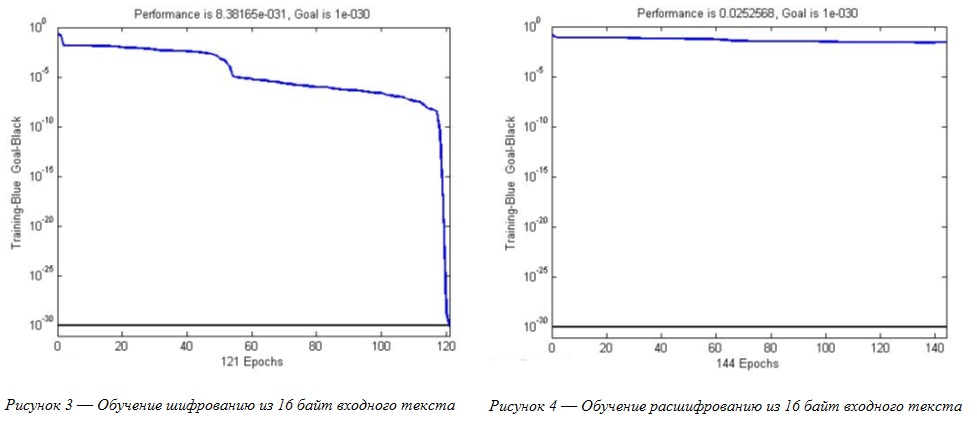
MLP имеет следующие параметры. Для процесса шифрования, могут быть использованы следующие настройки:

* входной вектор, являющийся открытым текстом;
* выходной — зашифрованный текст из алгоритма AES;
* первоначальные веса будут ключом шифрования;
* нелинейная функция активации каждого нейрона будет (log-сигмойда), что дает выходные значения между (0 — 1).

Для процесса расшифровки, могут быть использованы следующие параметры:

* входным вектором является шифртекст;
* выходные значения — открытый текст;
* Первоначальные веса будут ключом для расшифровки;
* нелинейная функция каждого нейрона будет (сигмовидной), что дает выход между (0 — 1).

Вход и выход можно масштабировать, чтобы иметь возможность совмещаться с функцией активации. В фазе обучения, Rijndael-алгоритм производит зашифрованный текст из определенного входного текста. ИНС принимает входной текст в качестве входного и выходного текста в качестве цели, и самообучается для достижения такого же выходного текста. Модель структуры ИНС называется "последовательно-параллельная модель", где алгоритм Rijndael влияет на динамическое поведение нейронной модели. Фаза операций будет многослойной ИНС прямого распространения с конечными весами, используемыми для получения выходного сигнала шифрования/расшифрования. На этом этапе будет продолжаться производство открытого текста/зашифрованного текста до тех пор, пока новый ключ не начнет использоваться в системе, тогда ИНС необходимо будет переобучиться на новый ключ. В шифровании и расшифровании, в качестве нелинейной функции активации для каждого нейрона был использован гиперболический тангенс. Свойство сигмоиды производит выходные значения в диапазоне (от -1 до +1). Данные, используемые в AES находятся в диапазоне (0 — 255). Таким образом, чтобы ИНС была совместима с данными AES (текстом, зашифрованным текстом, ключом шифрования) на этапе функции активации, есть необходимость преобразовать данные в диапазон (0 — 1). Это достигается путем использования коэффициента масштабирования (1/256) таким образом, чтобы стать совместимым с выходом функции активации. Коэффициент может быть использован на выходе каждого нейрона повторно для преобразования выходного диапазона обратно в (0 — 255). Для простоты автор использовал только версией AES, имеющей 128-битный ключ. AES использует блок данных длиной 128 бит для шифрования/расшифрования. Таким образом, ИНС будет использовать данные в форме байт, так что и вход, и выход будет размером 16 байт. ИНС должен иметь по крайней мере один скрытый слой в 16 нейронов для достижения размера входного ключа длины 16 байт. Для обучения ИНС имеем топологию (16 — 16 — 16 — 1). Она принимает вектор из 16 байт в качестве входных данных и производит вектор из 16 байт как обученный текст. Веса каждого слоя являются ключом (16 байт) вектор. В этой ИНС шифрование не будет производить нужный текст, потому что минимальный градиент будет достигнут без достижения целевой производительности. Рисунок 3 и 4 отражают обучение процессов шифрования и дешифрования на основе 16-ти байт входного текста.

[](http://cryptowiki.net/index.php?title=File:Neuro7.jpg)

Тесты показывают, что выходные тексты на нейро-AES в шифровании и расшифровании не идентичны выходным текстам шифрования и расшифрования AES. Одним из основных способов решений этой проблемы является сокращение входных и целевых векторов ИНС. Это решение будет иметь тенденцию к сокращению времени подготовки и достижению целевой производительности. Идея сокращения заключается в создании более чем одной параллельной операции ИНС. Каждая операция ИНС будет работать с частью входных и выходных векторов.

На данный момент опробованы несколько топологий ИНС и обнаружено, что ИНС с топологией (4 — 16 — 16 — 1) является лучшим выбором. Нейро-криптосистема состоит из 4 слоев, работающих параллельно. Каждый из слоев ИНС принимает входной вектор длиной 4 байта. Топология желаемого ИНС в процессе расшифрования/шифрования выглядит следующим образом.

Слой 1 с 4 нейронами, где каждый нейрон получает один байт из входного вектора (открытый текст/зашифрованный текст).

Слой 2 с 16 нейронами, где каждый нейрон суммирует вес всех 8 нейронов в 1-м слое.

Слой 3 с 16 нейронами, где каждый нейрон суммирует вес всех 8 нейронов во 2-м слое.

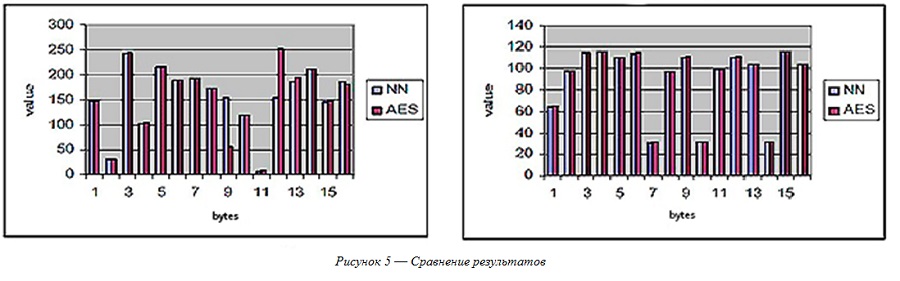
Слой 4 (выходной слой) с 1 нейроном, который суммирует вес всех 8 нейронов в третьем слое.

Начальные веса ИНС являются ключами для процесса расшифрования/шифрования. Таким образом, ключ длиной 16 байт из ИНС был взят следующим образом: 4x1 матрица в качестве начального веса от входа к слою 1. 16x4 матрица (представляет 16 байт из ключа и повторяется 4 раза) в качестве начальных весов от слоя 1 к слою 2. 16x16 матрица (представляет те же 16 байт в слое 1, но повторяется 16 раз) в качестве начального веса от слоя 2 к слою 3. 1x16 матрица (представляет то же самое в слое 1 от входа, но в транспонированном виде), в качестве первоначального веса от слоя 3 до выходного слоя.

Уравнение выхода этого ИНС следующее[[11]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#AmMa11): [](http://cryptowiki.net/index.php?title=File:Neuro8.jpg) ,где output — открытый текст/зашифрованный текст (в соответствии со способом), w — симметричный ключ. Тангенциальные сигмоиды передаточных функций в скрытых слоях сжимают бесконечный входной диапазон в конечный выходной диапазон.

**Достоинства и недостатки алгоритмов шифрования на основе ИНС на примере AES**

Выбранная НС была обучена с различными начальными весами (ключами), чтобы проверить правильность предложенной криптосистемы. Оценки проводились путем сравнения нейро-AES с AES[[11]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#AmMa11), как показано на рисунке 5, где показано шифрование и расшифрование с различными ключами. Из рисунка 5 видно, что существуют некоторые различия в битах между криптосистемой AES и нейро-AES и количество ошибочных битов уменьшается после нескольких итераций, где НС уже была обучена на всех данных, которые могут быть использованы в этой криптосистеме.

[](http://cryptowiki.net/index.php?title=File:Neuro9.jpg)

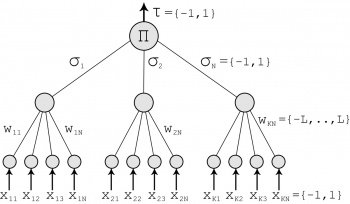
Из результатов сравнения можно утверждать, что построенная криптосистема на основе ИНС может быть использована вместо алгоритма шифрования AES и данная криптосистема будет более устойчива к известным атакам на алгоритм AES[[11]](http://cryptowiki.net/index.php?title=%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B8%D1%82%D0%B5%D1%80%D0%B0%D1%82%D1%83%D1%80%D1%8B_%D0%BA_%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%83_%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8#AmMa11), так как она основана на нелинейной функции активации. Но не исключается возможность использовать иную топологию сети, позволяющую шифровать и расшифровывать блоки данных большей длины, а также использовать ключ больших размеров. Но главный недостаток алгоритма на нейронной сети состоит в том, что после обучения нейронной сети не исключены небольшие ошибочные отклонения значений от значений шифрования или расшифрования алгоритмом AES, что означает, что в шифрованном и расшифрованном тексте могут появится искажения. Также к недостаткам можно отнести усложнение алгоритма относительно простого шифрования алгоритмом AES и необходимость в создании и поддержании более сложной системы на этапе внедрения.

Протокол обмена ключами

Для обмена ключами между двумя абонентами наиболее часто используется [алгоритм Диффи-Хеллмана](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0). Его более безопасная замена основана на синхронизации двух древовидных машин четности (TPM, tree parity machines). Синхронизация этих машин похожа на синхронизацию двух хаотических осцилляторов в теории хаотических связей.

**TPM**

TPM — это особый вид многоуровневой нейронной сети прямого распространения.

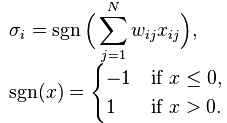
[](http://cryptowiki.net/index.php?title=File:Neuro14.jpg)

[](http://cryptowiki.net/index.php?title=File:Neuro14.jpg)

TPM

Она состоит из одного выходного нейрона, *K* скрытых нейронов и *K*×*N* входных нейронов. Входные нейроны принимают двоичные значения:[](http://cryptowiki.net/index.php?title=File:Neuro10.jpg)

Веса между входными и скрытыми нейронами принимают значения:[](http://cryptowiki.net/index.php?title=File:Neuro11.jpg)

Значение каждого скрытого нейрона есть сумма произведений входного значения и весового коэффициента:[](http://cryptowiki.net/index.php?title=File:Neuro12.jpg)

Значение выходного нейрона есть произведение всех скрытых нейронов:[](http://cryptowiki.net/index.php?title=File:Neuro13.jpg)

Выходное значение также двоичное.

**Протокол**

У каждого абонента (А или Б) есть своя TPM. Их синхронизация происходит следующим образом:

1. Задаём случайные значения весовых коэффициентов
2. Выполняем следующие шаги, пока не наступит синхронизация
   1. Генерируем случайный входной вектор X
   2. Вычисляем значения скрытых нейронов
   3. Вычисляем значение выходного нейрона
   4. Сравниваем выходы двух TPM:
      1. Выходы разные: переход к п.2.1
      2. Выходы одинаковые: применяем выбранное правило к весовым коэффициентам

После полной синхронизации (веса wij обоих TPM одинаковые), А и Б могут использовать веса в качестве ключа.

Этот метод известен как двунаправленное обучение.

Для обновления весовых коэффициентов могут использоваться следующие правила:

* Правило Хебба:

[](http://cryptowiki.net/index.php?title=File:Neuro15.jpg)

* Анти-правило Хебба:

[](http://cryptowiki.net/index.php?title=File:Neuro16.jpg)

* Случайное блуждание:

[](http://cryptowiki.net/index.php?title=File:Neuro17.jpg)

**Виды атак**

* Метод грубой силы
* Обучение собственной TPM
* Другие атаки