УДК 004.032.26

А. Ю. Степанова[1], С. В. Клименко[1], О. О. Слипченко[1],
Н. С. Михайлов[2]

[1]Днепропетровский национальный университет имени Олеся Гончара
[2]Государственное предприятие «Конструкторское бюро «Южное»

ИСЛЕДОВАНИЕ КРИПТОСТОЙКОСТИ СИСТЕМ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

Рассматрены вопросы использования нейронных сетей для криптографической защиты информации. Исследованы вопросы криптостойкости и основные причины ненадежности криптосистем. Рассмотрены вопросы применения нейрокомпьютерной сети к криптоанализу. Проведен анализ работы нейрокомпьютерной сети на основе разработанного программного обеспечения.

Ключевые слова: *криптография; шифрование; алгоритм; нейронная сеть*.

Розглянуто питання використання нейронних мереж для криптографічного захисту інформації. Досліджено питання крипостійкості та основні причини ненадійності криптосистем. Розглянуто питання застосування нейрокомп'ютерної мережі в криптоаналізі. Проведено аналіз роботи нейрокомп'ютерної мережі на основі розробленого програмного забезпечення.

Ключові слова: *криптографія; шифрування; алгоритм; нейронна мережа.*

The article deals with the use of neural networks for cryptographic protection of information. Questions of cryptostability and the main reasons for the unreliability of cryptosystems are investigated. Questions of application of a neurocomputer network to cryptanalysis are considered. The analysis of the operation of the neurocomputer network is based on the developed software.

Keywords: *cryptography; encryption; algorithm; neural network.*

Введение. Последнее время характеризуется резким увеличением числа открытых работ по всем вопросам криптологии, а криптоанализ становится одной из наиболее активно развивающихся областей исследований. Многие криптосистемы, стойкость которых не вызывала особых сомнений, оказались успешно раскрытыми.

При этом разработан большой арсенал математических методов, представляющих прямой интерес для криптоаналитика. В начале 70-х

годов была известна только классическая одноключевая криптография, но число открытых работ по этой тематике было весьма скромным. Отсутствие интереса к ней можно объяснить целым рядом причин. Во-первых, не ощущалось острой потребности в криптосистемах коммерческого назначения. Во-вторых, большой объем закрытых исследований по криптографии обескураживал многих ученых, которым, естественно, хотелось получить новые результаты. Но самым важным фактором являлось то, что криптоанализ как научная дисциплина фактически по-прежнему представлял собой большой набор разрозненных «трюков», не объединенных стройной математической концепцией.

Ближе к концу XX века ситуация радикально изменилась. Во-первых, с развитием сетей связи и повсеместным применением ЭВМ необходимость в криптографической защите данных стала осознаваться все более широкими слоями общества. Во-вторых, изобретение Диффи и Хелманном криптографии с открытым ключом создало благоприятную почву для удовлетворения коммерческих потребностей в секретности, устранив такой существенный недостаток классической криптографии, как сложность распространения ключей. По существу, это изобретение открыло качественно новую неисследованную область, которая к тому же обещала возможность широкого внедрения новых результатов быстро развивающейся теории вычислительной сложности для разработки конкретных систем с простым математическим описанием. Ожидалось, что стойкость таких систем будет надежно опираться на неразрешимость в реальном времени многих хорошо известных задач и что, может быть, со временем удастся доказать принципиальную нераскрываемость некоторых криптосистем.

Но надежды на достижение доказуемой стойкости посредством сведения задач криптографии к хорошо известным математическим задачам не оправдалась, а, скорее, наоборот. Именно то обстоятельство, что любую задачу отыскания способа раскрытия некоторой конкретной криптосистемы можно переформулировать как привлекательную математическую задачу, при решении которой удается использовать многие методы той же теории сложности, теории чисел и алгебры, привело к раскрытию многих криптосистем. На сегодняшний день классическая лента однократного использования остается единственной, безусловно, стойкой системой шифрования.

Идеальное доказательство стойкости некоторой криптосистемы с открытым ключом могло бы состоять в доказательстве того факта, что любой алгоритм раскрытия этой системы, обладающий

непренебрежимо малой вероятностью ее раскрытия, связан с неприемлемо большим объемом вычислений. И хотя ни одна из известных систем с открытым ключом не удовлетворяет этому сильному критерию стойкости, ситуацию не следует рассматривать как абсолютно безнадежную.

Анализ публикаций и постановка задачи. На сегодняшний день разработано много систем, в отношении которых доказано, что их стойкость эквивалентна сложности решения некоторых важных задач, которые почти всеми рассматриваются как крайне сложные, таких, например, как известная задача разложения целых чисел. Многие из раскрытых криптосистем были получены в результате ослабления этих предположительно стойких систем с целью достижения большого быстродействия. Кроме того, результаты широких исследований, проводившихся с начала XXI столетия как в самой криптографии, так и в общей теории вычислительной сложности, позволяют современному криптоаналитику гораздо глубже понять, что же делает его системы нестойкими.

Проведение криптоанализа для давно существующих и недавно появившихся криптоалгоритмов очень актуально, так как вовремя можно сказать, что данный криптоалгоритм нестоек, и усовершенствовать его или заменить новым. Для того чтобы выявлять нестойкие криптоалгоритмы, необходимо все время совершенствовать уже известные методы криптоанализа и находить новые.

Нейронным сетям, как таковым, посвящено довольно много публикаций, в которых рассмотрены их различные типы и архитектуры [1–4]. Целью данной статьи является рассмотрение применения нейронных сетей для криптографических систем защиты информации, а также их применение в криптоанализе.

Надежность криптосистем. В современном программном обеспечении криптоалгоритмы широко применяются не только для задач шифрования данных, но и для аутентификации и проверки целостности. На сегодняшний день существуют хорошо известные и апробированные криптоалгоритмы (как с симметричными, так и несимметричными ключами), криптостойкость которых либо доказана математически, либо основана на необходимости решения математически сложной задачи (факторизации, дискретного логарифмирования и т.п.). Таким образом, они не могут быть вскрыты иначе, чем полным перебором или решением указанной задачи.

С другой стороны, в компьютерном и околокомпьютерном мире все время появляется информация об ошибках или «дырах» в той или иной программе (в том числе применяющей криптоалгоритмы), или о том,

что она была взломана (cracked). Это создает недоверие как к конкретным программам, так и к возможности вообще защитить что-либо криптографическими методами не только от спецслужб, но и от простых хакеров.

Причины ненадежности можно отобразить на схеме, приведенной на рис. 1.

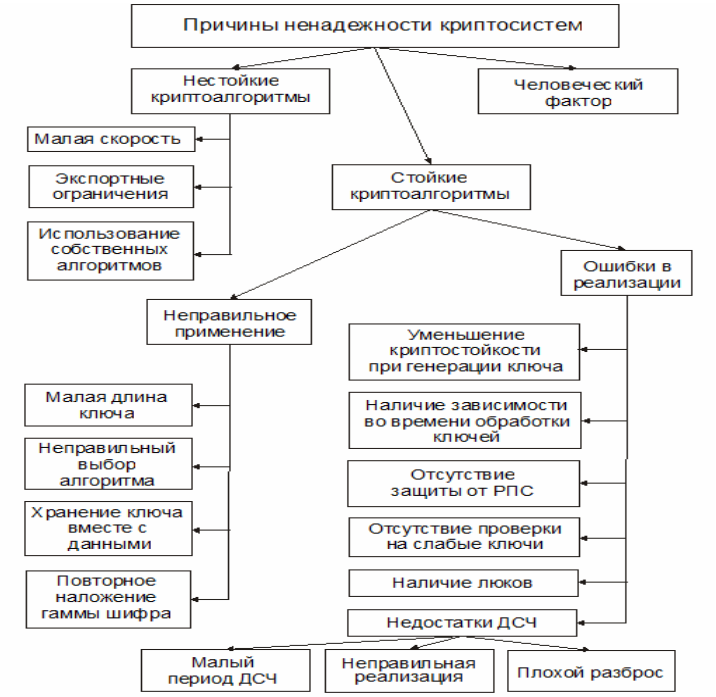

Рисунок 1 – Причины ненадежности криптосистем

Поэтому знание истории атак и «дыр» в криптосистемах, а также понимание причин, по которым они имели место, является одним из необходимых условий разработки защищенных систем. Перспективным направлением исследований в этой области является анализ успешно проведенных атак или выявленных уязвимостей в криптосистемах с целью их обобщения, классификации и выявления причин и закономерностей их появления и существования.

По аналогии с таксономией причин нарушения безопасности вычислительной среды, выделим следующие причины ненадежности криптографических программ:

1. Невозможность применения стойких криптоалгоритмов;
2. Ошибки в реализации криптоалгоритмов;
3. Неправильное применение криптоалгоритмов;
4. Человеческий фактор.

Структура системы анализа криптографических алгоритмов. Система анализа криптографических алгоритмов состоит из двух подсистем: подсистемы криптографической защиты информации с использованием представителей различных классов шифров и подсистемы криптоанализа [5]. Схема системы анализа криптографических алгоритмов представлена на рис. 2.

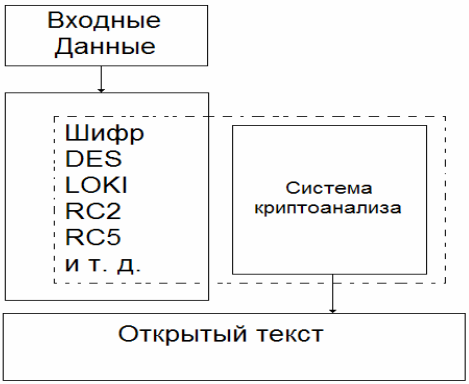

Рисунок 2 – Схема системы криптоанализа

Применение нейрокомпьютерной сети к криптоанализу. При решении задачи криптоанализа выбран вариант в котором на этапе обучения имеются следующие входные данные: открытый текст, ключ, алгоритм шифрования, закрытый текст.

На этапе криптоанализа имеется только закрытый текст. На этапе распознавания происходит выделение из криптотекста знакомых системе образцов и представление их одним нейроном или нейронным ансамблем на следующих уровнях. Как при обучении, так и при распознавании входные векторы являются нечеткими, т. е. имеется небольшой разброс векторов, принадлежащих к одному классу. В связи с этим нейросеть, осуществляющая эту операцию, должна обладать определенной способностью к статистическому усреднению. Напротив, может оказаться, что группа векторов находится в непосредственной близости друг к другу, но все они представляют разные классы. Тогда нейросеть должна определять тонкие различия

между векторами. Ещё одно требование к нейросети низкого уровня обработки сигнала — обучение без учителя, т. е. способность самостоятельно разделять входные сигналы на классы.

Большое количество нейросетевых алгоритмов выполняют функцию разделения входного криптотекста на классы, известно 3 математических модели этого разделения:

1. Разделение входных данных гиперплоскостями (простой персептрон).

Применение этого алгоритма оправданно только для задач, обладающих высокой линейностью. Например, можно построить нейросеть, разбивающую точки (0,0) и (1,1) на два класса для двумерного сигнала, но невозможно решить задачу по разбиению точек (0,0), (1,1) – первый класс, и (0,1), (1,0) – второй. Это широко известный пример, приведенный на рис. 3, неспособности простого персептрона решить задачу «исключающее или».

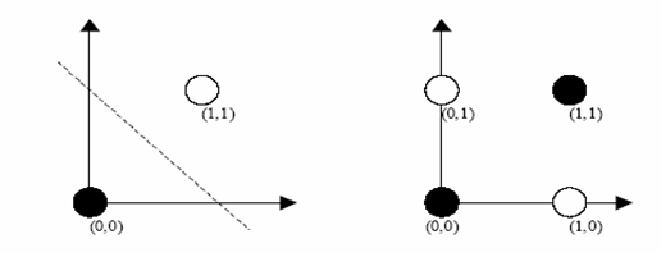

Рисунок 3 – Теорема Минского

2. Разделение входных данных гиперповерхностями (многослойные персептроны).

При последовательном соединении слоев, подобных простому персептрону, появляется возможность комбинировать гиперплоскости и получать гиперповерхности довольно сложной формы, в том числе и замкнутые. Такая нейросеть в принципе при достаточном числе нейронов способна разделять сигналы на классы практически любой сложности. Но применение таких нейросетей ограничено сложностью их обучения. Разработан мощный алгоритм, называемый «алгоритмом обратного распространения ошибки», но и он требует значительного времени обучения и не гарантирует минимального значения ошибки (опасность попадания в локальные минимумы).

3. Поиск наибольшего соответствия (наименьшего углового или линейного состояния). При нормализованных векторах входа все векторы располагаются на поверхности гиперсферы.

Существует модель нейросети, отвечающая этим требованиям —

это сеть встречного распространения. В оригинале она представляет собой объединение двух хорошо известных алгоритмов: самоорганизующейся карты Кохонена и слоя Гроссберга. В процессе обучения входные векторы ассоциируются с соответствующими выходными векторами. Когда сеть обучена, приложение входного вектора приводит к требуемому выходному вектору. Обобщающая способность сети позволяет получать правильный выход даже при приложении входного вектора, который является неполным или слегка неверным.

Схематически сеть встречного распространения изображена на рис. 4.

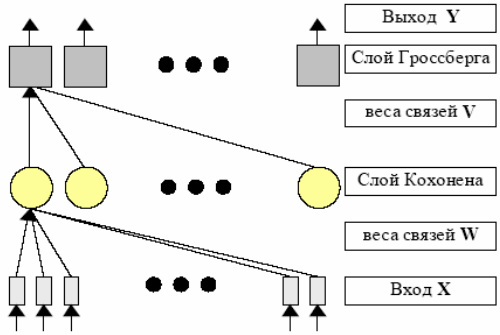

Рисунок 4 – Сеть встречного распространения

Распространение данных в такой сети происходит следующим образом: входной вектор нормируется на 1,0 и подается на вход, который распределяет его дальше через матрицу весов W. Каждый нейрон в слое Кохонена вычисляет сумму на своем входе и в зависимости от состояния окружающих нейронов этого слоя становится активным или неактивным (уровни 1,0 и 0,0). Нейроны этого слоя функционируют по принципу конкуренции, т. е. в результате определенного количества итераций активным остается один нейрон или небольшая группа, «пузырек активности». Этот механизм называется латеральным торможением и подробно рассмотрен во многих источниках. Так как отработка этого механизма требует значительных вычислительных ресурсов, в данной модели он заменен нахождением нейрона с максимальной активностью и присвоением ему активности 1,0, а всем остальным нейронам 0,0. Таким образом, срабатывает нейрон, для которого вектор входа ближе всего к вектору весов связей.

Если сеть находится в режиме обучения, то для выигравшего нейрона происходит коррекция весов матрицы связи по формуле (1):

$$W_н = W_с + \alpha\left(X - W_с\right) \quad (1)$$

где $W_н$ – новое значение веса, $W_с$ – старое значение, α – скорость обучения, X – величина входа. Геометрически это правило иллюстрирует рис. 5.

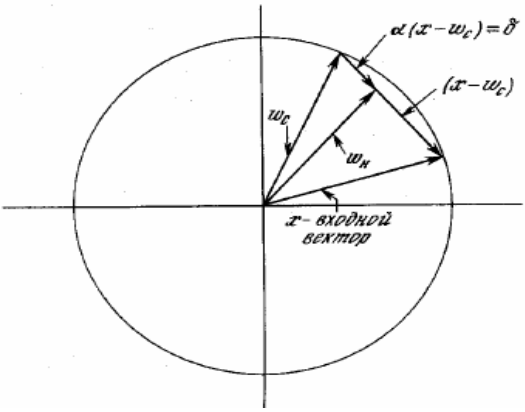

Рисунок 5 – Коррекция весов нейрона Кохонена

Так как входной вектор x нормирован, т. е. расположен на гиперсфере единичного радиуса в пространстве весов, то при коррекции весов по этому правилу происходит поворот вектора весов в сторону закрытого текста. Постепенное уменьшение скорости поворота α позволяет произвести статистическое усреднение входных векторов, на которые реагирует данный нейрон. Главной проблемой при коррекции весов нейрона Кохонена является выбор начальных значений весов. Так как в конце обучения векторы весов будут располагаться на единичной окружности, то в начале их также желательно нормировать на 1,0. В рассматриваемой модели векторы весов выбираются случайным образом на окружности единичного радиуса.

Проблема: если весовой вектор окажется далеко от области входа, он никогда не даст наилучшего соответствия, всегда будет иметь нулевой выход, следовательно, не будет корректироваться и окажется бесполезным. Оставшихся же нейронов может не хватить для разделения входного пространства на классы. Для решения этой проблемы предлагается много алгоритмов, здесь же применяется

правило «желания работать»: если какой-либо нейрон долго не находится в активном состоянии, он повышает веса связей до тех пор, пока не станет активным и не начнет подвергаться обучению. Этот метод позволяет также решить проблему тонкой классификации: если образуется группа входных данных, расположенных близко друг к другу, с этой группой ассоциируется и большое число нейронов Кохонена, которые разбивают её на классы. Правило «желания работать» записывается в следующей форме, показанной в формуле (2)

$$W_н = W_с + W_с \beta(1 - a) \quad (2)$$

где $W_н$ – новое значение веса, $W_с$ – старое значение, β – скорость модификации, a – активность нейрона.

Чем меньше активность нейрона, тем больше увеличиваются веса связей. Далее сигнал через матрицу весов V поступает на слой Гроссберга, где слой срабатывает по старому методу.

Алгоритм обучения:

Входные данные: обучающая выборка (набор входных векторов); выходные данные: скорректированные связи

1. Предъявить сети входной вектор.
2. Выполнять итерации до установления стабильного состояния.
3. Для всех узлов сети выполнить коррекцию связей согласно разделению входных данных гиперповерхностями или поиску наибольшего соответствия.
4. Повторять пункты 1–3 для каждого входного вектора.

Анализ работы нейрокомпьютерной сети. С использованием **р**азработанного на основе алгоритма программного обеспечения проанализированы различные виды криптографических алгоритмов, а именно: DES, RSA, RC2, с различными длинами ключа: 16, 24, 56. Также варьировалось количество зашифрованных символов.

Анализ 16-битного ключа показывает, что криптостойкость выбранных алгоритмов различна и минимальна для DES, что подтверждается и другими методами криптоанализа.

Алгоритм DES был изначально ориентирован на аппаратную реализацию и в программном исполнении работает очень медленно. При увеличении обучающей выборки время анализа DES возросло вдвое, тогда как для RC2 и RSA практически не изменилось.

Увеличение размера ключа положительным образом влияет на криптостойкость, что и подтвердил проведенный анализ 24-битного ключа.

Криптостойкость с увеличением размера ключа резко возрастает.

Причем DES приблизился по криптостойкости к RC2, тогда как для RC5 стойкость возросла в гораздо большей степени [6].

Выводы. В статье рассмотрены основные причины ненадежности криптосистем. Проведенный криптоанализ шифров DES, RC2 и RC5 показал, что шифр RC5 является наиболее стойким по сравнению с другими рассмотренными шифрами. Следовательно, алгоритм RC5 более предпочтительно использовать при шифровании для защиты данных. Также из анализа видно, что увеличение длины ключа существенно увеличивает криптостойкость шифров. Разработанное программное обеспечение системы криптоанализа показало большую эффективность, чем использование классических методов криптоанализа.

Библиографические ссылки

1. Хайкин С. Нейронные сети. Полный курс. Москва: Вильямс, 2016. 1104 с.
2. Каллан Р. Нейронные сети. Краткий справочник. Москва: Вильямс, 2017. 288 с.
3. Галушкин А. Нейрокомпьютеры: учебное пособие. Астрахань: АльянС, 2014. 528 с.
4. Латыпова Р. Нейронные сети. Дюссельдорф: Lambert Academic Publishing, 2012. 64 с.
5. Шнайер Б. Прикладная криптография. Москва: Вильямс, 2016. 1024 с.
6. Тадеусевич Р., Боровик Б., Гончаж Т., Леппер Б. Элементарное введение в технологию нейронных сетей с примерами программ. Москва: Телеком, 2011. 408 с.

Надійшла до редколегії 11.07.2017