Литература

1. Скрягин Л.Н. Как пароход погубил город: Очерки о катастрофах на реках, озерах и в портах. М.: Транспорт, 1990. 272 с.

2. Что произошло в Тяньцзине: цифры, факты и версии. URL: https:// news.tut. by/world/460274.html (дата обращения: 23.11.2018).

3. Пожар на заводе BASF. URL: https://www.youtube.com.watch?v=kZHvuN7 JnrA (дата обращения: 20.11.2018).

4. Тайна взрыва линкора «Императрица Мария». URL: http://history-paradox.ru/ linkor_im.php (дата обращения: 23.11.2018).

5. Черкашин Н. Как погиб линкор «Новороссийск» // Информационно-аналитическое интернет-издание фонда исторической перспективы «Столетие». 2015. 27 окт.

6. Об утверждении свода правил СНиП 2.07.01-89* «Градостроительство. Планировка и застройка городских и сельских поселений: приказ Минрегиона России от 28 дек. 2010 г. № 820 // ЭЛЕКТРОННЫЙ ФОНД правовой и нормативно-технической документации. URL: http://www.docs.cntd.ru (дата обращения: 08.11.2018).

НЕЙРОННЫЕ СЕТИ И ЗАЩИТА ИНФОРМАЦИИ

А.Ю. Лабинский, кандидат технических наук, доцент;
А.П. Толстов, кандидат юридических наук.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрены возможности использования нейронных сетей для защиты информации. Приведены основные особенности нейронных сетей и возможности нейрокриптографического подхода для кодирования информации.

Ключевые слова: искусственные нейронные сети, хэш-функция, кодирование информации, моделирование

SYNTHETIC NEURAL NETWORKS AND INFORMATION PROTECTION

A.Yu. Labinskiy; A.P. Tolstov.
Saint-Petersburg university of State fire service of EMERCOM of Russia

This article presents the special feature for information protection. Presents the possibility of the synthetic neural networks for information encode and development the neural networks encoding system.

Keywords: synthetic neural networks, hashing function, information encode, simulation

Деятельность органов управления МЧС России происходит в сложной обстановке воздействия различных факторов. При этом особую важность приобретают вопросы защиты информации. Современный подход к решению вопросов защиты информации заключается в использовании современных направлений компьютерного моделирования, одним из которых является использование фрактальной концепции [1]. Другим перспективным направлением компьютерного моделирования является моделирование с помощью искусственных нейронных сетей [2].

Криптология [3], разделяющаяся на два направления – криптографию и криптоанализ, занимается защитой информации с помощью различных преобразований. Криптография использует математические методы поиска и преобразования информации. Криптоанализ

использует различные математические методы расшифровывания информации без знания ключей.

Современная криптография включает в себя четыре крупных раздела [3]:

– симметричные криптосистемы;

– криптосистемы с открытым ключом;

– системы электронной подписи;

– управление ключами.

Любая защищенная связь для защиты информации использует криптографические методы, в том числе методы симметричного и асимметричного шифрования (с открытым ключом), а также односторонние хэш-функции.

Шифрование является процессом преобразования информации, в котором исходный текст, называющийся также открытом текстом, заменяется шифрованным текстом. Процесс шифрования с использованием криптосистемы представлен на рис. 1.

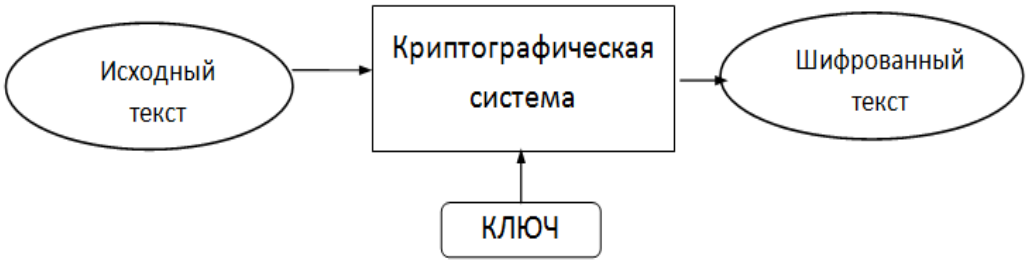

Рис. 1. **Процесс шифрования**

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

В криптографических системах с открытым ключом используются два ключа – открытый и закрытый, которые математически связаны друг с другом. На входе в криптографическую систему исходный текст шифруется с помощью открытого ключа, доступного всем пользователям. На выходе из криптографической системы информация расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

В качестве хэш-функций используются функции, которые можно легко рассчитать. При этом обратное восстановление таких функций требует больших усилий. В качестве примера можно привести функции возведения в степень и логарифма. Использование хэш-функций обычно сочетается с технологией асимметричного шифрования.

Асимметричные системы для преобразования ключей, которые могут использоваться в целях необратимости процесса шифрования даже для отправителя сообщения, включают в себя так называемые необратимые или односторонние функции (безопасные хэш-функции), у которых при заданном значении x относительно просто вычислить значение f(x), однако при использовании уравнения y=f(x) нет простого пути для вычисления значения x. Хэш-функции создают дайджест (хэш-код, «отпечаток») шифруемого текста (данных), который используется для подтверждения истинности исходной информации.

В криптографической системе входящее сообщение пропускается через математическую хэш-функцию, в результате чего на выходе из криптографической системы получается некоторая последовательность битов. Этот процесс преобразования информации практически невозможно восстановить.

Основой методов шифрования с помощью хэш-функции является применение к значению ключа одностороннего (безопасного) математического преобразования, в результате чего получаются соответствующие шифрованные значения.

Основные результаты использования хэш-функций [3]:

– вероятность подбора ключа уменьшается;

– распределение значения свертки в структурах данных становится более равномерным;

– становится возможной генерация последовательностей псевдослучайных чисел, которые можно использовать в имитационном моделировании.

Рассмотрим некоторые известные алгоритмы хэширования.

Алгоритм MD5 (Message Digest), разработанный в 1991 г., для сообщения произвольной длины создает дайджест длиной 128 бит. Сообщение разбивается на блоки длиной 512 бит (16 слов по 32 бита). Каждый блок обрабатывается с помощью четырех логических функций, используемых в процессе 64 циклов обработки:

– $F1(X, Y, Z)=(X \wedge Y) \vee ((\neg X) \wedge Z)$;
– $F2(X, Y, Z)=(X \wedge Z) \vee (Y \wedge (\neg Z))$;
– $F3(X, Y, Z)=X \oplus Y \oplus Z$;
– $F4(X, Y, Z)=Y \oplus (X \wedge (\neg Z))$.

Здесь побитовые операции $\wedge$ – И, $\vee$ – ИЛИ, $\neg$ – НЕ, $\oplus$ – XOR (исключающее ИЛИ), X, Y, Z – шестнадцатеричные коды 32-битовых слов (16*32=512).

Алгоритм SHA-1 (Secure Hash Algorithm), разработанный в 1993 г, для сообщения произвольной длины создает дайджест длиной 160 бит. Сообщение разбивается на блоки длиной 512 бит. Каждый блок обрабатывается в течение 80 циклов с помощью трех логических функций.

Наиболее известным алгоритмом симметричного шифрования является DES (Data Encryption Standard), разработанный фирмой IBM в 1977 г. Шифруемая информация разбивается на блоки 64 бит, длина ключа 56 бит. В настоящее время используется улучшенная версия этого алгоритма – DES3 (Triple DES), в которой производится троекратное выполнение алгоритма DES. В качестве ключа шифрования используется хэш ключа, вычисленный по алгоритму хэширования MD5 (длина хэша ключа 128 бит). В соответствии с алгоритмом шифрования DES каждый бит зашифрованных данных является функцией от всех битов исходных данных и всех битов ключа. Окно вывода консольной программы шифрования, созданной на языке C# с использованием алгоритма DES3, представлено на рис. 2.

Рис. 2. **Окно вывода консольной программы шифрования**

На языке программирования C# шифрование осуществляется с использованием пространства имен System.Security.Cryptography.

Протокол обмена ключами

Алгоритм Диффи-Хеллмана часто используется для обмена ключами между двумя абонентами. Для моделирования данного алгоритма обычно используется многоуровневая нейронная сеть прямого распространения [4], схема которой представлена на рис. 3.

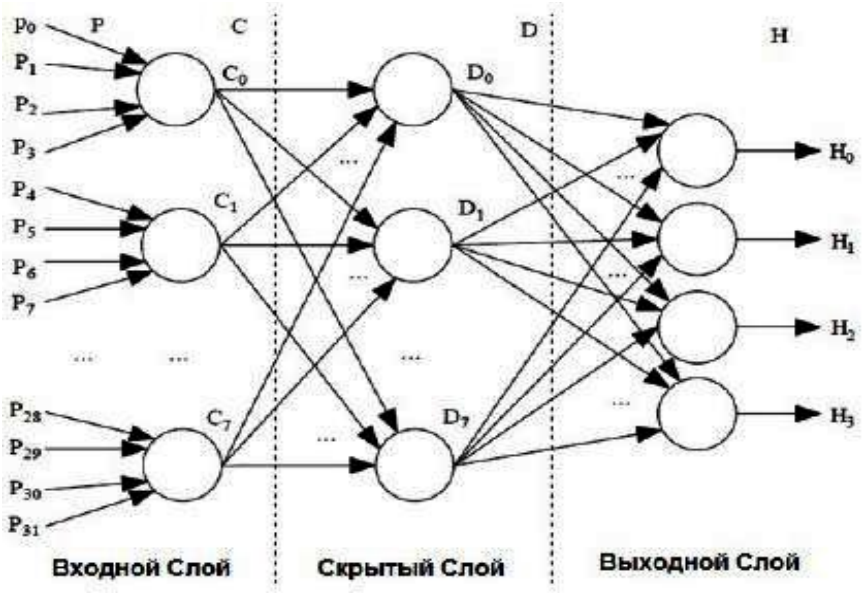

Рис. 3. **Схема многоуровневой нейронной сети прямого распространения**

Порядок работы (протокол) обмена ключами следующий. У каждого абонента (А или Б) есть своя многоуровневая нейронная сеть прямого распространения. Синхронизация нейронных сетей происходит с использованием следующего алгоритма [4]:

1. Задаются случайные значения весовых коэффициентов нейронной сети.
2. Выполняются шаги, предшествующие синхронизации:
2.1. На вход нейронов входного слоя подается случайный вектор X.
2.2. Вычисляются значения на выходе нейронов скрытого слоя.
2.3. Вычисляются значения на выходе нейронов выходного слоя.
2.4. Сравниваются выходные значения двух нейронных сетей.
3. Если выходные значения разные, то происходит переход к п. 2.1.
4. Если выходные значения одинаковые, то выбранное правило применяется к весовым коэффициентам нейронной сети.

После полной синхронизации нейронных сетей (значения весовых коэффициентов обоих сетей одинаковые), абоненты А и Б могут использовать значения весовых коэффициентов в качестве ключа. Этот метод известен как двунаправленное обучение нейронной сети [4].

Моделирование криптографической системы

При обмене ключами между абонентами сети возможен перехват ключа злоумышленником, что грозит последующей расшифровкой зашифрованного сообщения. Использование абонентами в составе криптографической системы двух синхронизированных искусственных нейронных сетей позволяет использовать в качестве ключа весовые коэффициенты сети W_{ij}, что повышает криптографическую стойкость криптосистемы. В данной работе моделирование процесса обмена ключами производилось с использованием аппроксимации значений ключа с помощью искусственной нейронной сети без скрытого слоя

(однонаправленная сеть без обратных связей), содержащей по 24 нейрона в каждом слое. Обучение сети происходило по алгоритму обратного распространения ошибки. Подробное описание указанной нейронной сети, включая алгоритм обучения, представлено в работе [5]. Зависимость числа итераций от размера ключа представлена на диаграмме (рис. 4).

Рис. 4.

Размер ключа менялся от 8 до 24 бит. С увеличением размера ключа объем вычислений (число итераций) процесса аппроксимации увеличивался (рис. 3).

Имея ключ, можно приступать к процессу шифрования/дешифрования, осуществляемому криптографической системой. В данной работе криптографическая система была реализована в виде программы для ЭВМ, интерфейс которой представлен на рис. 5.

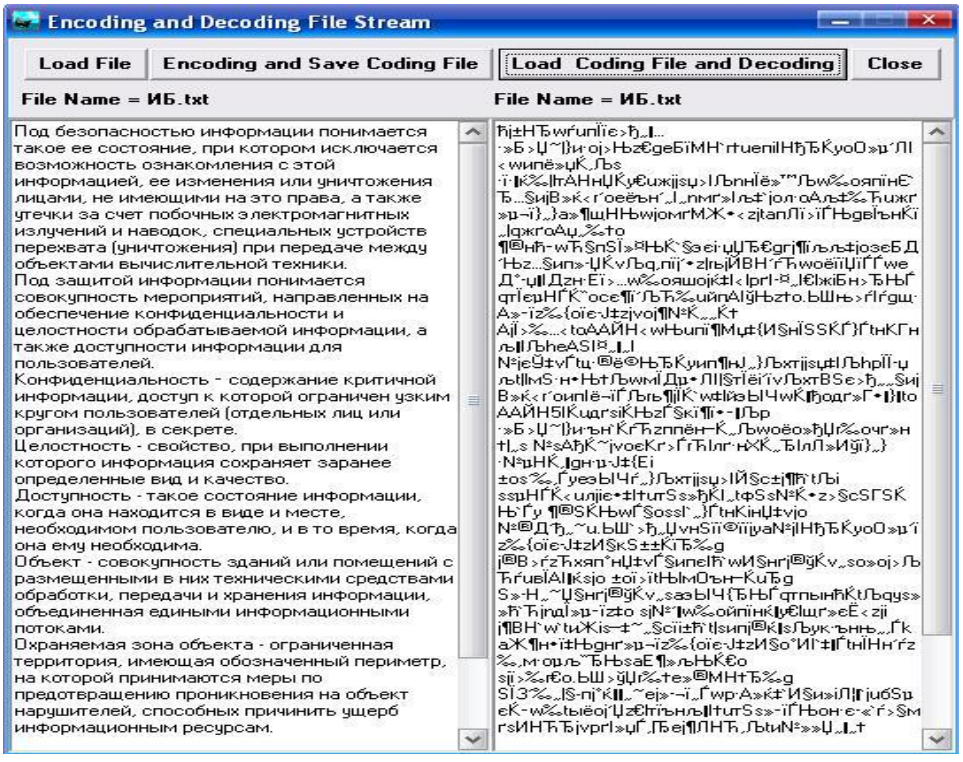

Рис. 5. **Программа, реализующая криптографическую систему**

В левом окне программы представлен исходный текст, а в правом окне – зашифрованный текст. В данной программе обмен данными, находящимися на внешнем носителе, осуществляется с помощью потоков, что обеспечивает высокую скорость передачи данных в процессе шифрования и дешифрования.

Программа содержит поточный класс, кодирующий и декодирующий исходный файловый поток. Поточный класс имеет два метода чтения и записи информации, а также свойство, хранящее ключ шифрования. В данной программе для демонстрации процесса шифрования текста используется упрощенный механизм шифрования, при котором значение ключа при шифровании добавляется в каждый байт исходного текста, а при расшифровке вычитается из каждого байта зашифрованного текста.

Нейросетевой подход к защите информации позволяет осуществлять процесс обмена ключами, обладающий необходимой криптографической стойкостью. Однако использование искусственных нейронных сетей требует достаточно большого объема вычислений и должно быть оптимизировано.

Литература

1. Лабинский А.Ю., Ильин А.В. Фракталы и защита информации. СПб.: Природные и техногенные риски (физико-математические и прикладные аспекты). 2016. № 1 (17). С. 82–86.

2. Червяков Н.А., Евдокимов А.Б., Галушкин А.П. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: Физматлит, 2012.

3. Бабаш А.В., Баранова Е.К. Криптографическое методы защиты информации. М.: Кронус, 2016.

4. Гридин В.Н., Солодовников В.И., Евдокимов И.А. Нейросетевой алгоритм симметричного шифрования // Информационные технологии. 2015. Т. 21. № 4.

5. Лабинский А.Ю., Уткин О.В. К вопросу аппроксимации функции нейронной сетью // Природные и техногенные риски (физико-математические и прикладные аспекты). 2016. № 1 (17). С. 5–11.

АНАЛИЗ ЭКОЛОГИЧЕСКОГО УЩЕРБА ОТ НЕФТЯНЫХ РАЗЛИВОВ

В.Д. Захматов, доктор технических наук, профессор;
В.А. Онов, кандидат технических наук, доцент.
Санкт-Петербургский университет ГПС МЧС России.
Н.В. Щербак, кандидат технических наук.
ООО «ЗОЛА», Санкт-Петербург

Проведен системный анализ разливов нефти с целью обоснования направления исследований по созданию новой аварийно-спасательной универсальной техники, размещенной на одном морском или сухопутном транспортном средстве. Эта техническая система предназначена для тушения пожаров и предотвращения крупных, аварийных разливов нефти или ликвидации локальных разливов нефти.

Ключевые слова: разливы нефти, аварийные локальные, катастрофические разливы, пожар – причина разлива, локализация и ликвидация разливов, гавани, открытое море, побережье

ANALYSIS OF ENVIRONMENTAL DAMAGE FROM OIL SPILLS

V.D. Zachmatov; V.A. Onov. Saint-Petersburg university of State fire service of EMERCOM of Russia.
N.V. Shcherbak. LLC «ZOLA», Saint-Petersburg

The system analysis of oil spills is carried out in order to substantiate the direction of research on the creation of a new emergency and rescue universal equipment placed on one sea