УДК 621.391

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ КРИПТОАНАЛИЗА ШИФРА «ГРАФИЧЕСКИЕ МАТРИЦЫ»

Алексеев А.П., Назаренко П.А., Орлов В.В.

В статье рассматривается возможность применения искусственной нейронной сети для криптоанализа шифра «Графические матрицы».

Ключевые слова: криптография, криптоанализ, искусственная нейронная сеть, суммирование по модулю два (гаммирование), метод перестановок, шифр «Графические матрицы».

Постановка задачи

Основная идея шифра «Графические матрицы» (ГМ) состоит в том, что символы открытого текста представляют в виде матриц черных и белых точек (пикселей), которые описывают с помощью двоичной системы счисления. В процессе шифрования графические матрицы трансформируют по сложному закону, определяемому секретным ключом [1]. При шифровании используют операции перестановок столбцов, строк, циклического сдвига, логического сложения с другой матрицей, сети Фейстеля и т.п.

Простейший пример зашифрования символа показан на рис. 1. Матрица исходного символа «Ч» (рис. 1а) трансформирована путем циклического сдвига строк (рис. 1б) и циклического сдвига столбцов (рис. 1в). На рис. 2 показан пример зашифрования путем логического сложения по правилу Исключающее ИЛИ (шифр гаммирования) исходной матрицы а) с матрицей б), в результате которого получена матрица в). Особенностью шифра ГМ является то, что вид символа открытого текста постоянно изменяется (даже в одном сеансе связи). Этот шифр можно отнести к шифрам многоалфавитной замены. Сказанное иллюстрирует рис. 3, на котором показан возможный вид одного и того же символа.

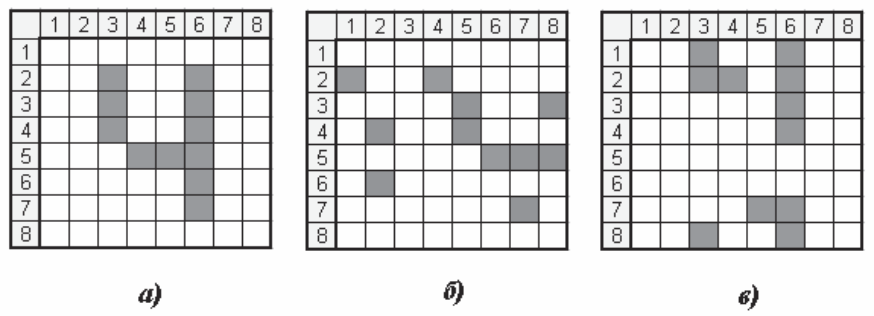

Рис. 1. Трансформация символа «Ч» с помощью операций циклического сдвига строк и столбцов

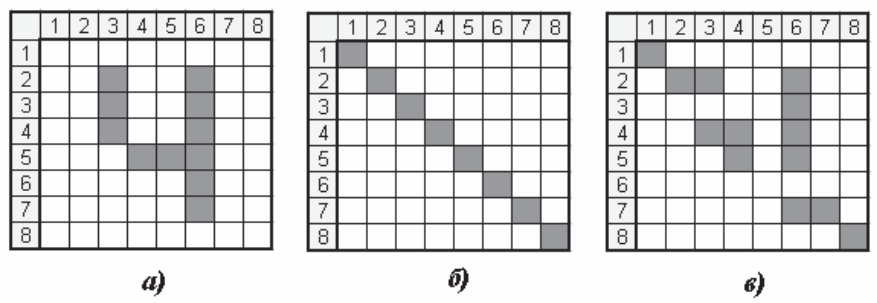

Рис. 2. Трансформация символа «Ч» с помощью логической операции «Исключающее ИЛИ»

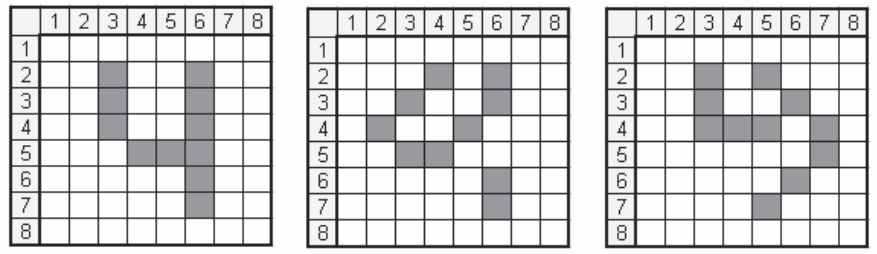

Рис. 3. Пример многоалфавитной замены символа «Ч»

Последовательность выполняемых при шифровании преобразований иллюстрирует рис. 4. Процесс шифрования состоит из двух этапов: предыскажения графической матрицы путем добавления аддитивного белого гауссовского шума и криптографического преобразования зашумленной матрицы:

$$M_i = f_1\left(T_i, K_1\right) = T_i + N_i, \qquad (1)$$

где M_i – предыскаженная матрица (результат первого шага шифрования); $f_1\left(X, K\right)$ – функция преобразования матрицы X на ключе K (первый шаг преобразований); T_i – i-ая матрица символа алфавита открытого текста; K_1 – «подключ» (далее без кавычек) – часть общего ключа $K = \left(K_1, K_2\right)$, используемый на первом шаге преобразования; N_i – матрица шума.

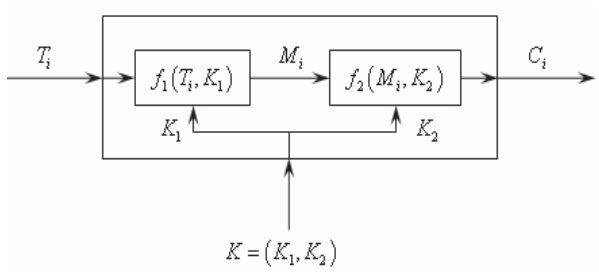

Рис. 4. Схема шифра «Графические матрицы»

Окончательное шифрование происходит в соответствии с выражением (2):

$$C_i = f_2\left(M_i, K_2\right) = f_2\left(T_i + N_i, K_2\right), \qquad (2)$$

где C_i – матрица шифртекста; $f_2\left(X, K\right)$ – функция преобразования второго шага матрицы X на ключе K (второй шаг преобразований); K_2 – подключ общего ключа $K = \left(K_1, K_2\right)$, используемый на втором шаге преобразования.

Вносимая при кодировании с помощью графических матриц избыточность определяется по формуле (3).

$$\chi = \left(1 - \frac{H\left(O\right)}{\log_2 N}\right) \cdot 100\%, \qquad (3)$$

где $H\left(O\right)$ – энтропия источника открытого текста; N – объем алфавита шифртекста.

При энтропии источника открытого текста $H\left(O\right) = 8$ бит (8-битные символы с равной вероятностью появления и объеме алфавита шифртекста $N = 2^{64}$ (для матриц 8×8), избыточность составляет $\chi = 87{,}5\%$.

При таком объеме вносимой избыточности представляет интерес исследование возможности использования искусственной нейронной сети (ИНС) для криптоанализа указанного шифра.

Методика исследований

Были исследованы два метода шифрования ГМ: шифрование матриц методами гаммирования и перестановок. Эти два метода шифрования ГМ являются аналогами классических методов замены и перестановок. Однако в классическом методе перестановок переставляются символы, а в шифре «Графические матрицы» переставляются пиксели матрицы. Это же можно сказать и о методе замены.

Методика оценки криптостойкости заключалась в следующем. Исследовалась способность нейронной сети правильно восстановить символы открытого текста, которые были искажены (трансформированы) в процессе шифрования и нанесения шума на матрицу. При этом восстановление символа в процессе распознавания нужно понимать, скорее, как предсказание наиболее вероятного вида символа. Окончательный выбор одного символа из нескольких символов с близкими вероятностями распознавания в процессе криптоанализа должен происходить с помощью цепей Маркова [2].

В процессе исследований предстояло ответить на вопрос о том, из какого состояния хаотического расположения пикселей еще возможно правильное распознавание символа. Для получения количественных оценок были использованы три варианта трансформации символа открытого текста: один заключался в том, что на исходную графическую матрицу наносился белый шум и исследовалась способность ИНС правильно распознать исходный символ. Заметим, что шум наносился в тех местах матрицы, где отсутствовало изображение самого символа.

Этот вариант можно считать особым случаем метода гаммирования, в котором единицы на матрицах гаммы и открытого текста не пересекаются. Второй вариант трансформации сводился к тому, что исходный графический символ демонтировался (пиксели отделялись от изображения символа и переносились в другие точки матрицы, не занятые самим символом). Таким образом имитировался метод перестановок. Третий вариант искажения символа использовался для исследования метода гаммирования (пиксели меняли цвет в зависимости от значения гаммы). Реализация ИНС была осуществлена с помощью матема-

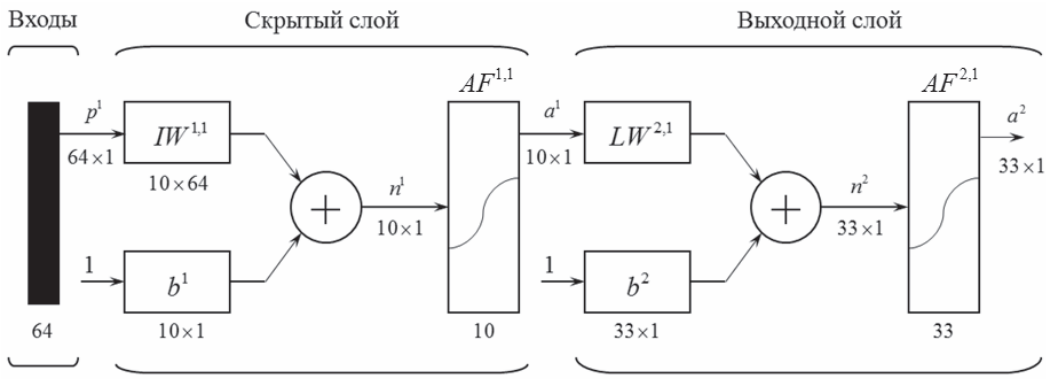

Рис. 5. Структура искусственной нейронной сети

тической системы MATLAB [3]. Для реализации распознавания символов использовалась ИНС со структурой двухслойного перцептрона [4].

Число входов совпадало с количеством элементов (пикселей) графической матрицы и для матрицы 8×8 пикселей составляло 64. Скрытый слой содержал 10 сигмоидальных нейронов. Количество нейронов в выходном слое совпадало с числом классов, то есть символов алфавита открытого текста, и равнялось 33. Функция активации нейронов выходного слоя – логистическая. Структура применявшейся ИНС показана на рис. 5.

В соответствии со структурой ИНС на вход первого слоя подавались 64-разрядные векторы-столбцы p^1. Каждый из входных векторов-столбцов умножался на вектор-строку входной матрицы весов $IW^{1,1}$. Размерность последней зависел от числа нейронов в слое и размера входных векторов. В рассматриваемой сети размерность входной матрицы весов составляла 10×64. Взвешенные значения входов суммировались со скалярными значениями смещений первого слоя b^1. В результате формировались значения входов функции активации первого слоя n^1. Вычисленные значения активационных функций $AF^{1,1}$ нейронов первого слоя формировали векторы выхода a^1. Выходной слой имел аналогичную структуру. Отличием являлось то, что выходной слой содержал 33 нейрона вместо 10 во входном слое, а также то, что размерность векторов входа совпадала с размерностью векторов выхода и составляла 10 элементов по числу нейронов первого слоя.

Для обучения на вход ИНС подавались незашумленные графические матрицы в виде символов русского алфавита. Обучающая функция реализована на основе метода градиентного спуска с моментами и с адаптивным обучением. Максимальное число циклов обучения было ограничено на уровне 5000. Для оценки функционирования сети была выбрана функция SSE (суммарная квадратичная ошибка), определяющая сумму квадратов ошибок обучения. Критерием окончания обучения была установлена величина отклонения от эталона равная 0,1.

Результаты исследований

При исследовании матриц, искаженных аддитивным белым гауссовским шумом, для каждого символа алфавита зашумление осуществлялось от 1 точки до полного заполнения матрицы с шагом в одну точку. При этом для каждого числа точек шума создавалось 10 различных вариантов матриц. Результаты распознавания матриц были усреднены по всем символам. Аппроксимированная зависимость процента успешных распознаваний от процента зашумления матрицы представлена на рис. 6.

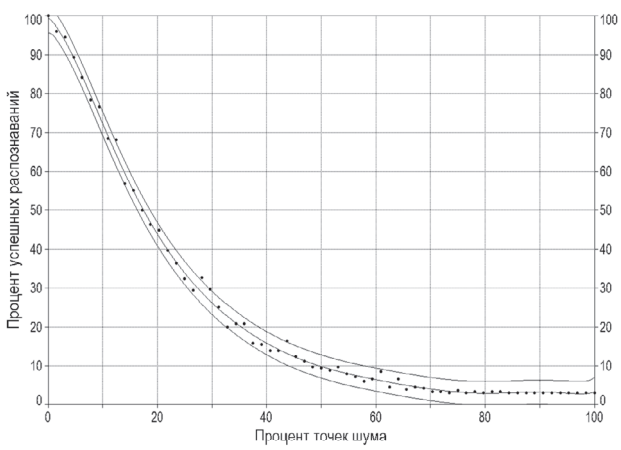

Рис. 6. Зависимость успешных распознаваний символов от степени зашумления

Из приведенного графика видно, что при наличии в матрице 18% пикселей шума вероятность правильного распознавания символа составит 0,5. При 60% шуме правильное распознавание становится практически невозможным. Вместе с тем при выполнении условий реализации шифра, когда в среднем четверть точек матрицы заполнена шумом, вероятность успешного распознавания матрицы составила 32,42%.

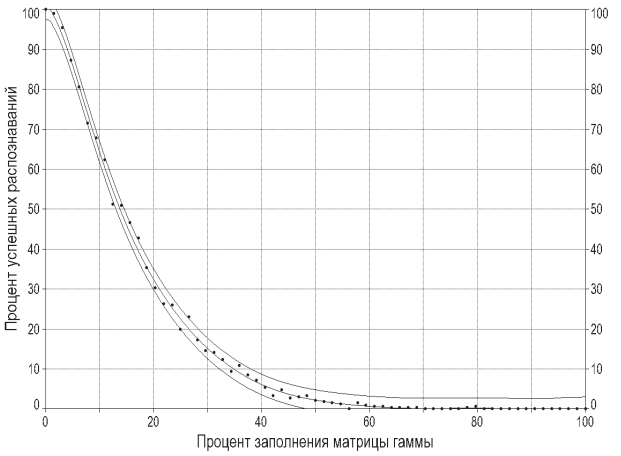

Рис. 7. Зависимость процента успешных распознаваний символов, искаженных операцией гаммирования, от степени заполнения матрицы гаммы

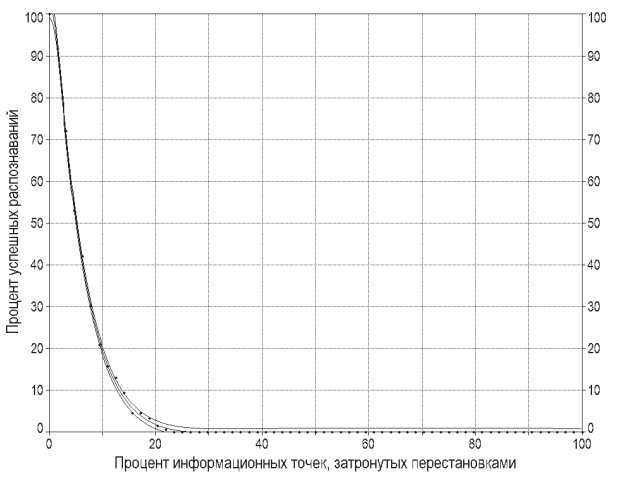

Рис. 8. Зависимость успешных распознаваний символов, искаженных перестановками, от процента черных точек матрицы, затронутых перестановками

При исследовании матриц, искаженных гаммированием, для каждого символа алфавита формировалась матрица гаммы, содержащая от 1 черной точки шума до полного заполнения с шагом в одну точку. Для каждого числа черных точек создавалось 10 различных вариантов матриц гаммы. Затем путем сложения чистых (неискаженных) матриц с матрицами гаммы по правилу «Исключающее ИЛИ» формировались наборы тестовых матриц. Результаты распознавания матриц были усреднены по всем символам. Аппроксимированная зависимость процента успешных распознаваний от процента заполнения матрицы гаммы черными точками представлена на рис. 7-8.

Графики рис. 7-8 говорят о том, что при типичной ситуации, когда в результате применения криптопреобразования в среднем половина точек меняет свое значение, ИНС не может правильно распознать матрицу.

Выводы

Искусственные нейронные сети могут быть успешно использованы для криптоанализа шифра «Графические матрицы» в тех случаях, когда анализируемая комбинация пикселей незначительно отличается от эталона (5…10%). Преобразование символов методом перестановок пикселей сложнее распознать, чем нанесение шума на матрицу – то есть метод перестановок более криптостоек по сравнению с методом гаммирования. Применение ИНС для атаки на метод перестановок не дает положительного эффекта (нет успешных распознаваний матриц). Сложнее распознать символ искаженный гаммированием, чем символ, искаженный белым шумом, когда шум не попадает на изображение символов.

Литература

1. Алексеев А.П., Орлов В.В. Способ стеганографического сокрытия информации. Патент РФ 2374770. Опубл. 27.11.2009.
2. Кельберт М. Я., Сухов Ю. М. Вероятность и статистика в примерах и задачах. Том II. Марковские цепи как отправная точка теории случайных процессов и их приложения. М.: МЦНМО, 2009. – 295 с.
3. Медведев В.С., Потемкин В.Г. Нейронные сети. MATLAB 6. М: «Диалог-МИФИ», 2002. – 496 с.
4. Хайкин С. Нейронные сети. Полный курс. М.: «Вильямс», 2006.– 1104 с.

USING NEURAL NETWORKS FOR CRYPTANALYSIS OF CIPHER «GRAPHICS ARRAY»

Orlov V.V., Alekseev A.P., Nazarenko P.A.

This article discusses the possibility of using neural networks for cryptanalytic cipher «Graphical matrix».

Keywords: *cryptography, cryptanalysis, artificiality neural networks, summation on the module two, method of shifts, code "Graphic matrixes".*

Алексеев Александр Петрович, к.т.н., доцент Кафедры «Информатика и вычислительная техника» Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. (8-846) 262-97-46; 228-00-59. E-mail: apa@bk.ru

Назаренко Петр Александрович, к.т.н., доцент Кафедры «Информационные системы и технологии» ПГУТИ. Тел. (8-846) 925-39-92; 228-00-21. E-mail: saod@yandex.ru

Орлов Владимир Владимирович, ведущий инженер-программист ЗАО «СБКК» (г. Самара). Тел. (8-846) 245-21-26. E-mail: crypter@list.ru

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 658.3

МЕТОДЫ ПРИНЯТИЯ РЕШЕНИЙ ПРИ УПРАВЛЕНИИ ПЕРСОНАЛОМ КРУПНОЙ ОРГАНИЗАЦИИ

Бузуев А.И., Яговкин Н.Г.

В статье представлен новый подход к совершенствованию методов принятия решений при управлении персоналом крупной организации, позволяющих обосновать структуру и провести оптимизацию должностных обязанностей персонала, а также управлять подготовкой и проводить комплексную оценку его компетентности.

Ключевые слова: методы принятия решений, граф, должностные обязанности, персонал, ранжирование, целевая функция, когнитивные карты.

Введение

В настоящее время в связи с укрупнением и децентрализацией систем управления организациями, переносом центра тяжести на микроуровень, внедрением новых технологий заметно возросло число и усложнился процесс принятия кадровых решений при формировании эффективной организационной системы, многие из которых затруднительно решить традиционными методами (экспертным путем или «волевым» решением должностного лица).

К таким решениям относятся обоснование структуры должностных обязанностей персонала; управление подготовкой и переподготовкой работников в условиях динамически меняющихся целей и структуры организации; комплексная оценка компетентности персонала в структурных подразделениях, позволяющая оценить ее соответствие поставленным задачам.

Существующие информационные системы, используемые для управления персоналом, относятся к классу синтезирующих и не решают поставленные задачи. Они, как правило, предусмотрены для учета кадрового состава, планирования и регулирования оплаты труда, табельного учета в подразделениях и расчета оплаты труда, удержания налогов, платежей, расчета пособий, отпускных и т.п.

Принятие кадровых решений заметно усложняется необходимостью анализа большого числа факторов: экономических, социальных, правовых, национальных и др. В этих условиях эти кадровые решения предполагают выполнение многовариантных расчетов, обоснование критериев оценки альтернатив и их приоритетов, определение действий в условиях риска и неопределенности, поэтому необходимо использовать методы принятия решений [1-2; 6].

Разработка метода принятия решений по совершенствованию организационной системы крупной организации

Метод принятия решений по совершенствованию организационной системы строится на основе проблемно-целевой структуры организации, формирование которой позволяет произвести де-