МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра математичекого моделирования и анализа данных

Отчёт
о прохождении производственной практики
для специальности
1-31 81 12«Прикладной компьютерный анализ данных»

магистранта 2года обучения
Деркача Максима Юрьевича

Руководитель практики от кафедры
чл.-корр. НАН Беларуси,

доктор физ.-мат. наук, профессор

Харин Юрий Семенович

Руководитель практики от организации Пьянов Владислав Сергеевич

Минск, 2019

1 *

Оглавлен1ие * 2

2 Введение **2**

3 Перечень задач **3**

4 Входные данные и математические модели **4**
4.1 Входные данные 4
4.2 Математическая модель однослойной сети 4
4.3 Математическая модель многослойной сети 5

5 Построение нейронных сетей **6**
5.1 Построение однослойной сети 6
5.2 Построение многослойной сети 6

6 Результаты компьютерных экспериментов и их анализ **7**
6.1 Выбор алгоритма оптимизации для однослойной сети 7
6.2 Выбор алгоритма оптимизации для многослойной сети 7
6.3 Зависимость точности построения модели от количества входных нейронов . 8
6.4 Проведение компьютерных экспериментов на контрольных данных 11

7 Заключение **12**

8 * **13**

2 Введение

Проблема защиты информации затрагивает практически все сферы деятельности человека. Среди способов защиты информации важнейшим считается криптографический [1].

Нейронная криптография - это раздел криптографии, посвященный анализу применения стохастических алгоритмов, особенно алгоритмов искусственных нейронных сетей, для использования в шифровании и криптоанализе.[2] Существуют решения, построенные на основе искусственных нейронных сетей, позволяющие обеспечить доступность данных [3].

Архитектура искусственных нейронных сетей позволяет эффективно проводить работы по распознаванию образов и классификации множества объектов по любым признакам. Кроме того, благодаря хорошо продуманному алгоритму обученные нейронные сети могут достигать чрезвычайно высоких уровней точности.

Основной целью практики было построить нейронную сеть для апроксимации двоичной (дискретной) функции и провести анализ полученных результатов.

3 Перечень задач

1. Построить генератор двоичных функций на основе полинома Жегалкина.
2. Построить однослойную нейронную сеть для апроксимации двоичной(дискретной) функции.
3. Провести компьютерные эксперименты с однослойной нейронной сетью для апроксимации тестовой двойчной функции и криптографического примитива. Провести анализ проведенного эксперимента.
4. Построить многослойнную нейронную сеть для апроксимации двоичной(дискретной) функции.
5. Провести компьютерные эксперименты с многослойнной нейронной сетью для апроксимации тестовой двойчной функции и криптографического примитива. Провести анализ проведенного эксперимента.

4 Входные данные и математические модели

4.1 Входные данные

Для проведение компьютерных экспериментов был построен генератор двоичных функций:

$$G_n = \{n, [a_i]\}, \tag{1}$$

где n - количество переменных булевой функции,
$[a_i]$ - вектор коэффициентов полинома Жегалкина, соответствующего генерируемой булевой функции.

Для контрольного теста использовались выборки A_1, A_2, A_3.

$$A_i^{(n)} = \{X_1^{(i)}, ..., X_n^{(i)}\} \subseteq V^{20}, V \in \{0, 1\}, \tag{2}$$

где $n \leq n_+ = 2^{20} \approx 10^6, i = 1, 2, 3, A_i$ - классифицированная выборка.

$$B_i = \{Y_1^{(i)}, ..., Y_n^{(i)}\}, \tag{3}$$

где $Y_i^{(j)} \in V$ - номер класса, к которому относится вектор $X_j^{(i)}$, $j = 1, ..., n$.

$$Y_i^{(j)} = E(X_j^{(i)}), \tag{4}$$

где E - некоторый криптографический примитив.

4.2 Математическая модель однослойной сети

Пусть $X \in R^n$ -множество объектов; Y - множество допустимых ответов. Положим, что $X = (x^0, x^1, ..., x^n) \in \{-1\} \times X$, где $x^j = f_j(x), j \geq 1$ - признаковое описание, а $x_0 = -1$ - дополнительный константный признак; $Y = \{0, 1\}$. И задана обучающая выборка $\{(x_i; y_i)\}_{i=1}^{(l)}$. Тогда

$$y = f(u), u = \sum_{i=1}^{n} w_i x_i + w_0 x_0, \tag{5}$$

где w_i - веса входов,
$f(u)$ - передаточная функция(функция активации).

Тогда построение однослойной сети сводится к задачи поиска вектора, доставляющего минимум функционалу

$$Q(w) -> min_w, \tag{6}$$

где $Q(w)$ - некоторая функция потерь (например, квадратичная функция потерь $Q(w) = \sum_{i=1}^{n}(f_i(x_i) - y_i)^2$).

4.3 Математическая модель многослойной сети

Пусть $X \in R^n$ -множество объектов; Y - множество допустимых ответов. Положим, что $X = (x^0, x^1, ..., x^n) \in \{-1\} \times X$, где $x^j = f_j(x), j \geq 1$ - признаковое описание, а $x_0 = -1$ - дополнительный константный признак; $Y = \{0, 1\}$. И задана обучающая выборка $\{(x_i; y_i)\}_{i=1}^{(l)}$. Тогда

$$y = f(u), u = \sum_{i=1}^{n} w_i x_i + w_0 x_0, \tag{7}$$

где w_i - веса входов,
$f(u)$ - передаточная функция(функция активации).

Тогда построение однослойной сети сводится к задачи поиска вектора, доставляющего минимум функционалу

$$Q(w) -> min_w, \tag{8}$$

где $Q(w)$ - некоторая функция потерь (например, квадратичная функция потерь $Q(w) = \sum_{i=1}^{n}(f_i(x_i) - y_i)^2$).

5 Построение нейронных сетей

5.1 Построение однослойной сети

Для построения однослойной сети для апроксимации двоичной функции использовались следующие параметры:

1. функция активации: $f(u) = \frac{1}{(1+exp(-u))}$- сигмоидальная функция;
2. количество итераций обучения: 1000;
3. скорость обучения: 0.001.

5.2 Построение многослойной сети

Для построения многослойной сети для апроксимации двоичной функции использовались следующие параметры:

1. функция активации: $f(u) = \frac{1}{(1+exp(-u))}$- сигмоидальная передаточная функция;
2. скорость обучения: 0.001;
3. количество скрытых слоев варировалась от 2 до 20.
4. количество входных нейронов для скрытых слоев: были проведены эксперименты для двух случаев: 1) константное количество входных нейронов для всех скрытых слоев; 2) количество входных нейронов рассчитывалось по следующей формуле: $N_{in} = \sum_{i=1}^{k} C_n^i$, где k - номер слоя, n - количество нейронов на первом слое.

6 Результаты компьютерных экспериментов и их анализ

6.1 Выбор алгоритма оптимизации для однослойной сети

Для выбора алгоритма оптимизации был проведен компьютерный эксперимент при следующих параметрах:

1. входные данные были полученный при помощи генератора двоичных функций при $n = 6$;
2. в качестве функции активации использовалась $f(u) = \frac{1}{(1+exp(-u))}$- сигмоидальная функция;
3. количество итераций обучения: 1000;
4. скорость обучения: 0.001.

Optimizer	**Accuracy**	**Loss**
Adam	0.6123	0.6512
Proximal	0.4902	3.4120
Adagard	0.5122	2.8922
ProximalAdarad	0.5232	1.3524
Gradient	0.5102	3.4129

Из полученных результатов, очевидно что в качетсве алгоритма оптимизации следует использовать алгоритм Адама. В последующих вычислениях будем пользоваться данным алгоритмом.

6.2 Выбор алгоритма оптимизации для многослойной сети

Для выбора алгоритма оптимизации был проведен компьютерный эксперимент при следующих параметрах:

1. входные данные были полученный при помощи генератора двоичных функций при $n = 6$;
2. эксперимент был проведен для следующего количества скрытых слоев: 2, 4;
3. в качестве функции активации использовалась $f(u) = \frac{1}{(1+exp(-u))}$- сигмоидальная функция;
4. количество итераций обучения: 1000;
5. скорость обучения: 0.001.

Из полученных результатов, очевидно что в качетсве алгоритма оптимизации следует использовать алгоритм Адама. В последующих вычислениях будем пользоваться данным алгоритмом.

Optimizer	Accuracy (4 HL)	Loss (4 HL)	Accuracy (2 HL)	Loss (2 HL)
Adam	0.9456	0.1259	0.7980	0.4344
Proximal	0.5902	1.4120	0.6310	0.5819
Adagard	0.5747	1.8922	0.4951	3.1123
ProximalAdarad	0.5932	1.3524	0.5427	2.1299
Gradient	0.5902	1.4129	0.6873	0.4925

6.3 Зависимость точности построения модели от количества входных нейронов

Были проведены эксперимента для многослойной модели, в которой количество нейронов в скрытых слоях выбиралось следующим образом:

1. $N_{in} = n$, n - количество нейронов на первом слое.

2. $N_{in} = \sum_{i=1}^{k} C_n^i$, где k - номер слоя, n - количество нейронов на первом слое.

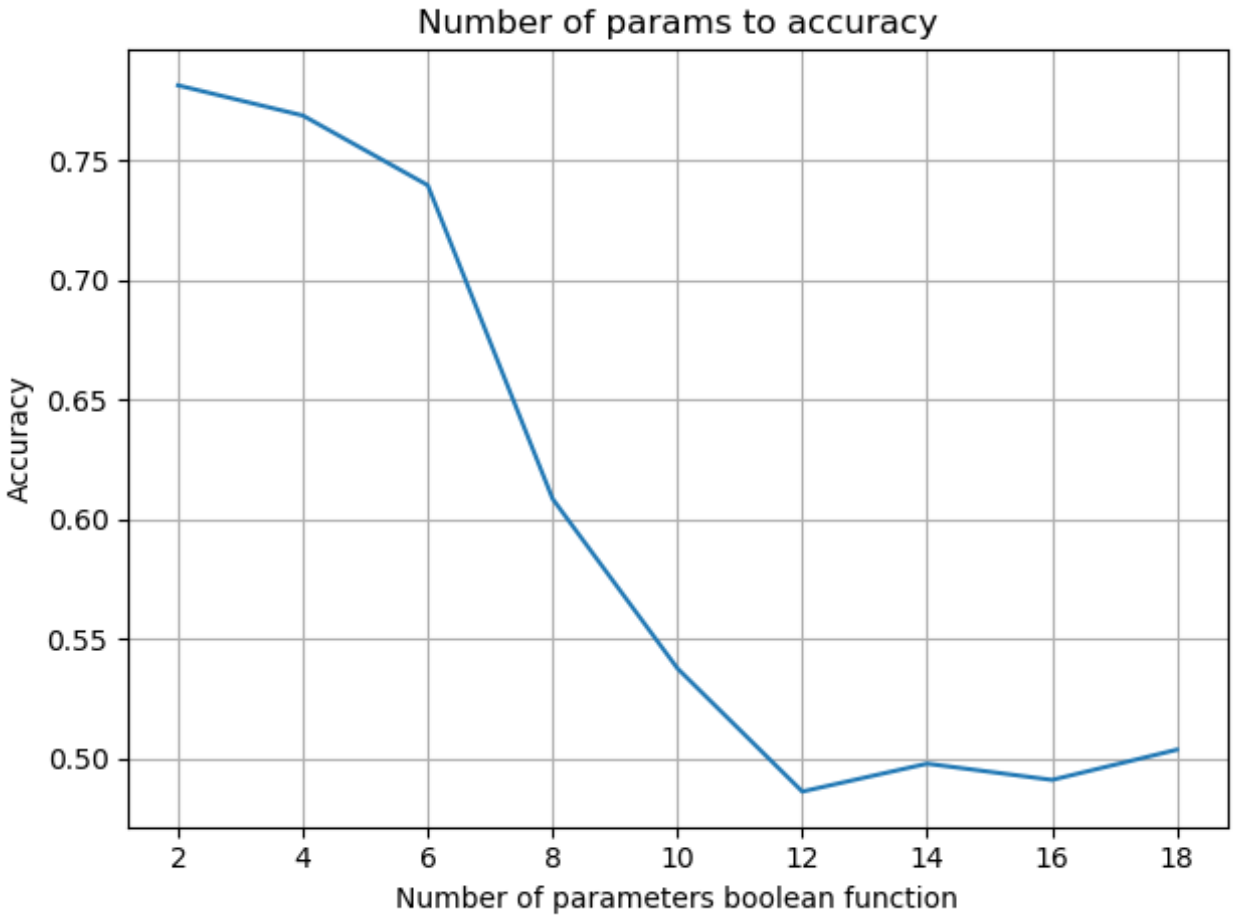

Рис. 1: График зависимости точности построенной модели от количества входных нейронов при $N_{in} = n$.

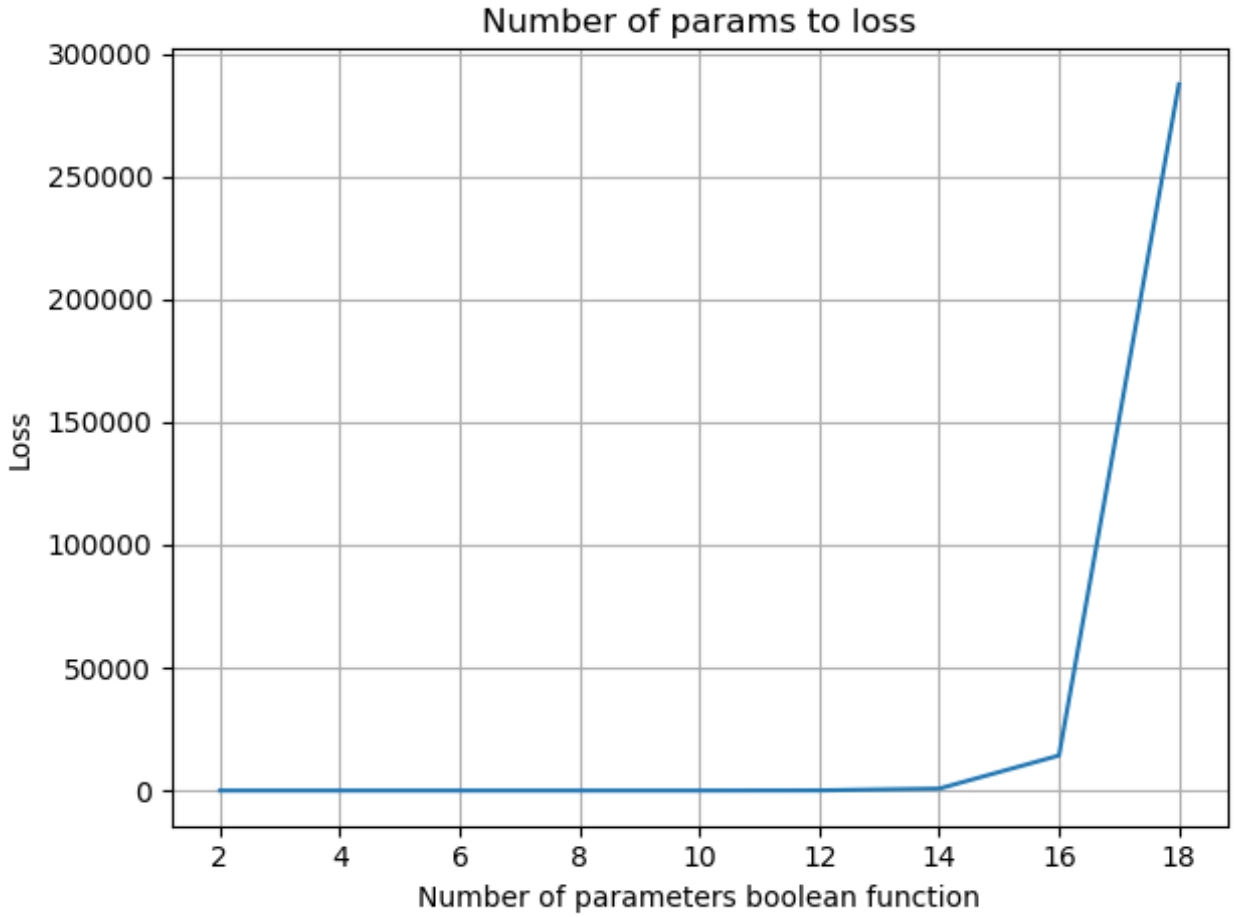

Рис. 2: График зависимости значений потерь от количества входных нейронов при $N_{in} = n$.

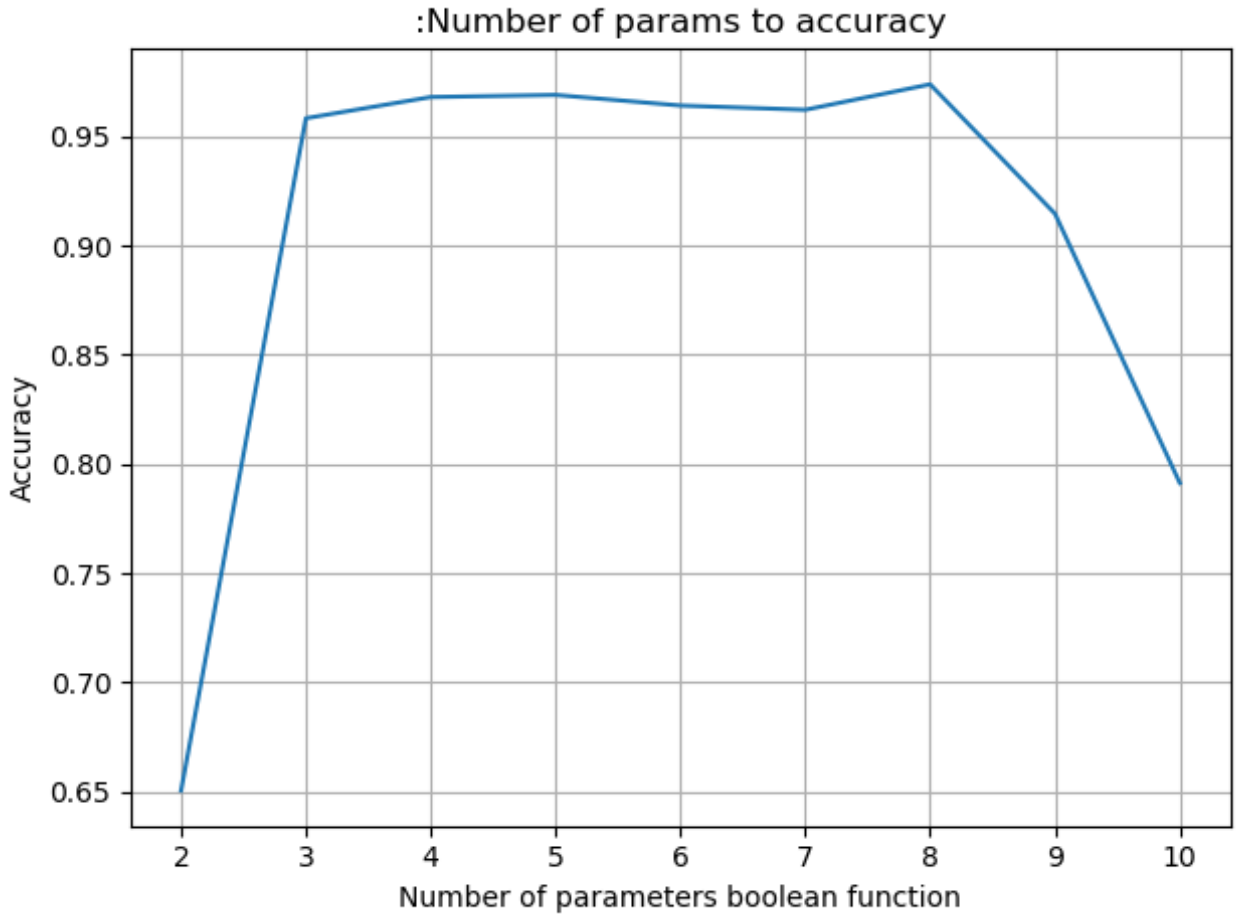

Рис. 3: График зависимости точности построенной модели от количества входных нейронов при $N_{in} = \sum_{i=1}^{k} C_n^i$.

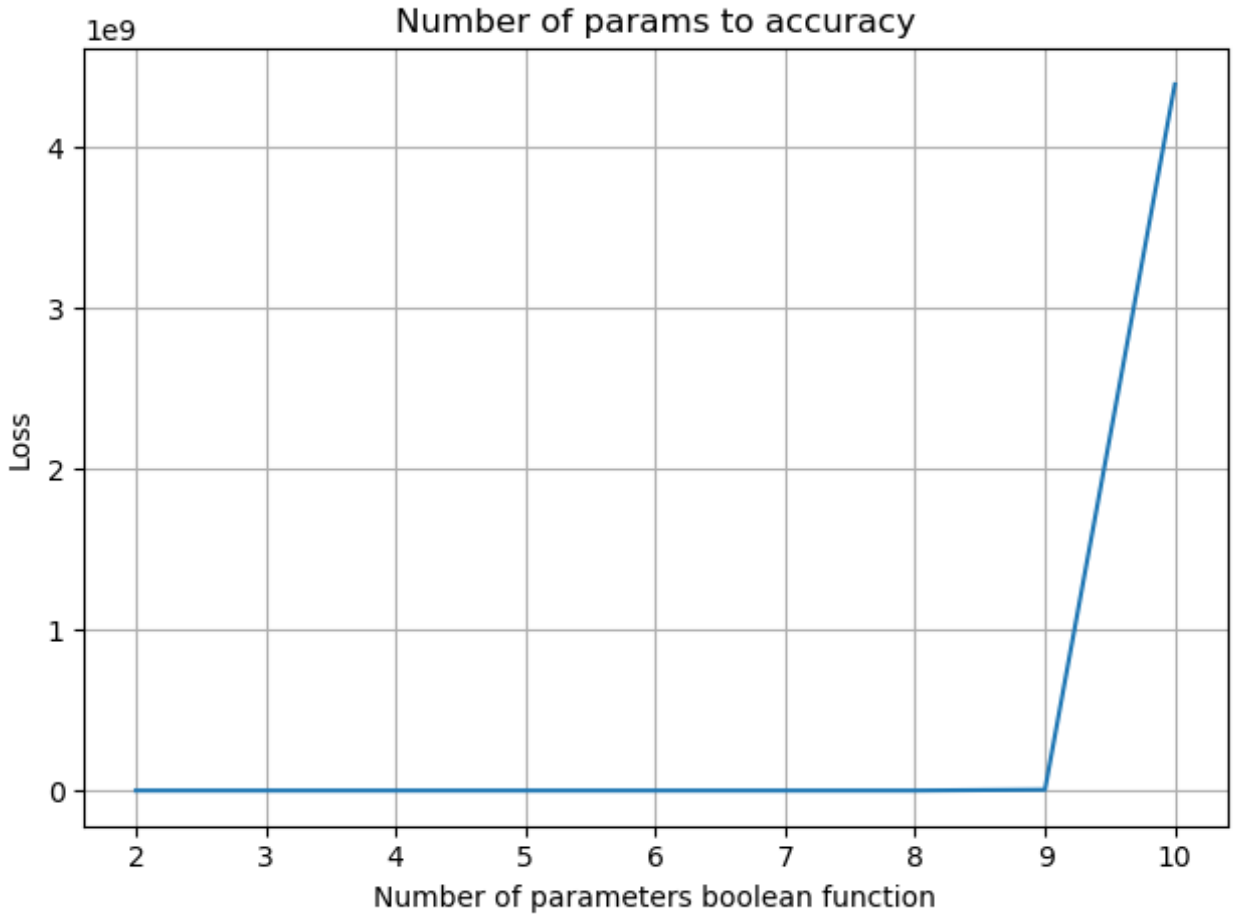

Рис. 4: График зависимости значений потерь от количества входных нейронов при $N_{in} = \sum_{i=1}^{k} C_n^i$.

Из полученных результатов, очевидно что следует использовать второй метод выбора количества нейронов на скрытых слоях. В дальнейшем будем использовать, данный метод.

6.4 Проведение компьютерных экспериментов на контрольных данных

Были проведены эксперимента для выборок A_1, A_2 и A_3.

7 Заключение

В данной работе построены однослойная и многослойная нейронные сети для апроксимации бинарных функций. Для данных нейронных сетей были проведены компьютерные эксперименты и их последующий анализ. Были проведены различные эксперименты над нашей моделью, чтобы определить лучшую структуру и параметры.

8 *

Литература

1. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. — 2003. — Минск.
2. Neural networks in cryptography [Электрон. ресурс]. — 2015. — *http : //cryptowiki.net/index.php?title = Neural_networks_in_cryptography*.
3. Pattanayak S., Ludwig S.A. Encryption based on Neural Cryptography. — 2017.
4. Kinzel F., Kanter I. Neural Cryptography. — 2002.