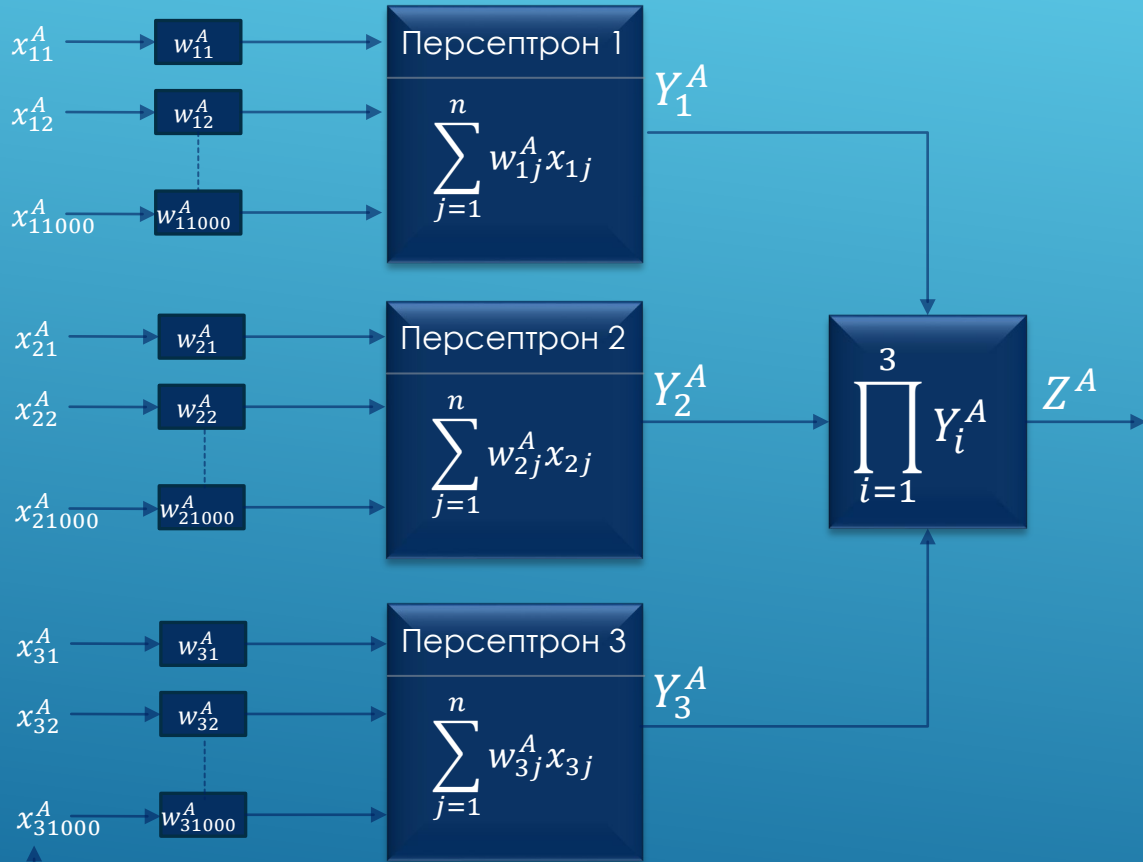


АНАЛИЗ СТОЙКОСТИ
КОМБИНИРОВАННОГО МЕТОДА
ФОРМИРОВАНИЯ
КРИПТОГРАФИЧЕСКОГО КЛЮЧА
С СЕКРЕТНОЙ МОДИФИКАЦИЕЙ
РЕЗУЛЬТАТОВ СИНХРОНИЗАЦИИ
ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

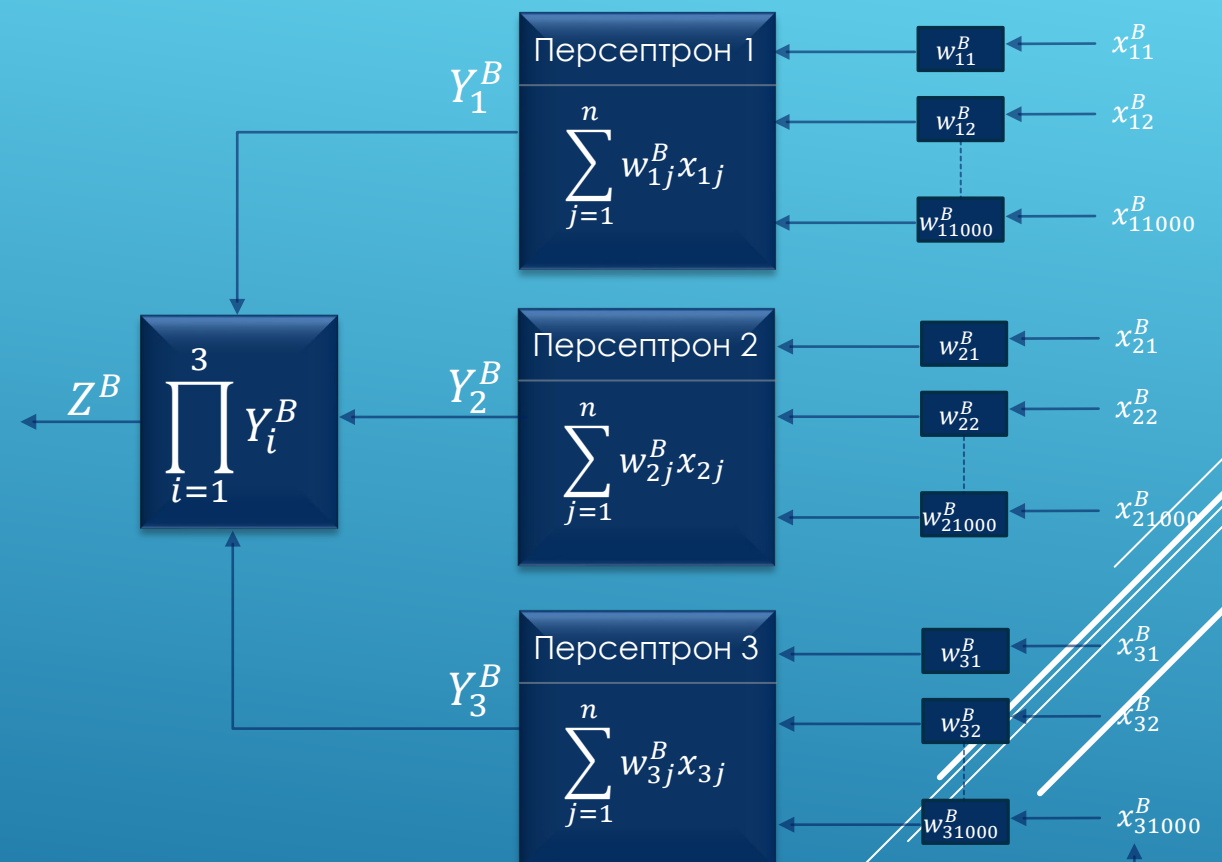
Радюкевич М. Л.

Синхронизация ИНС

Сеть А

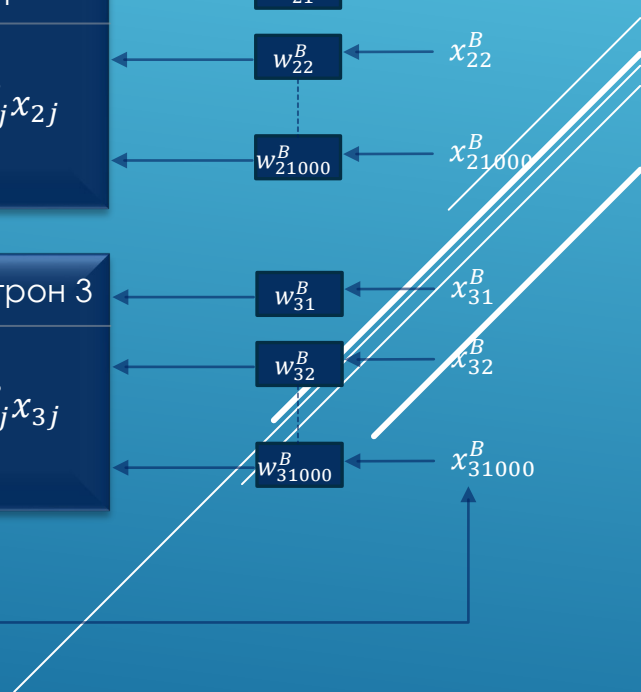


Сеть В



Генератор X

$$x_{ij} \in [-1; 1]$$

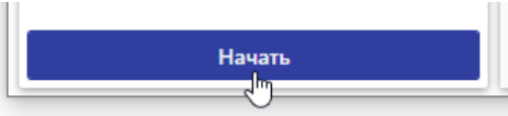
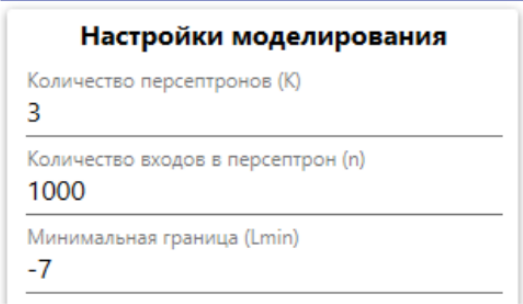
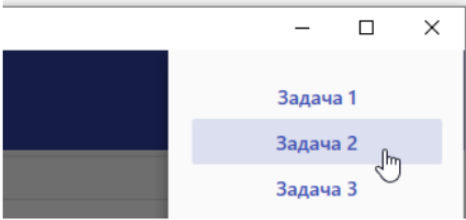
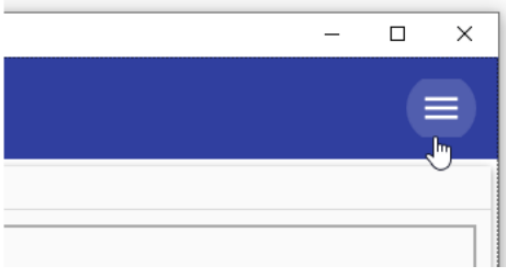


Программная модель

Синхронизация искусственных нейронных сетей

Добро пожаловать в программную модель
для статического моделирования процессов синхронизации ИНС

1. Откройте меню программы
2. Выберите интересующую задачу
3. Задайте настройки моделирования
4. Запустите моделирование



Настройки моделирования	
Количество персептронов (K)	3
Количество входов в персептрон (n)	1000
Минимальная граница (Lmin)	-7

Обоснование параметров СИНС

Синхронизация искусственных нейронных сетей

Задача 3. Вероятность синхронизации сетей А с В и А с Е при изменении параметров n , K , L

Настройки моделирования

- Количество персептронов (K): 3
- Количество входов в персептрон (n): 1000
- Минимальная граница (L_{min}): -7
- Максимальная граница (L_{max}): 8
- Разрешенные такты (d): 5000
- Количество синхронизаций: 100000
- Шаг графика: 100

График Таблица

	d	P_{ab}	P_{ae}
	1800	0,112	0,001
	1900	0,181	0,004
	2000	0,278	0,005
	2100	0,376	0,01
	2200	0,488	0,017
	2300	0,594	0,027
	2400	0,678	0,035
	2500	0,757	0,045
	2600	0,803	0,056
	2700	0,849	0,06
	2800	0,885	0,063
	2900	0,916	0,065
	3000	0,945	0,069
	3100	0,96	0,071
	3200	0,975	0,076
	3300	0,983	0,076
	3400	0,986	0,076
	3500	0,993	0,076
	3600	0,994	0,077
	3700	0,997	0,077
	3800	0,998	0,078
	3900	1	0,078

Начать

Обоснование параметров СИНС

Переход на несимметричный интервал

Синхронизация искусственных нейронных сетей

Задача 4. Влияние несимметричности интервала значений параметра L на вероятностные характеристики дерева ч

Настройки моделирования

Количество персептронов (K)
3

Количество входов в персептрон (n)
1000

Автоматическая подстановка n

Минимальная граница (Lmin)
-8

Максимальная граница (Lmax)
8

Разрешенные такты (d)
3000

Количество синхронизаций
100000

Таблица

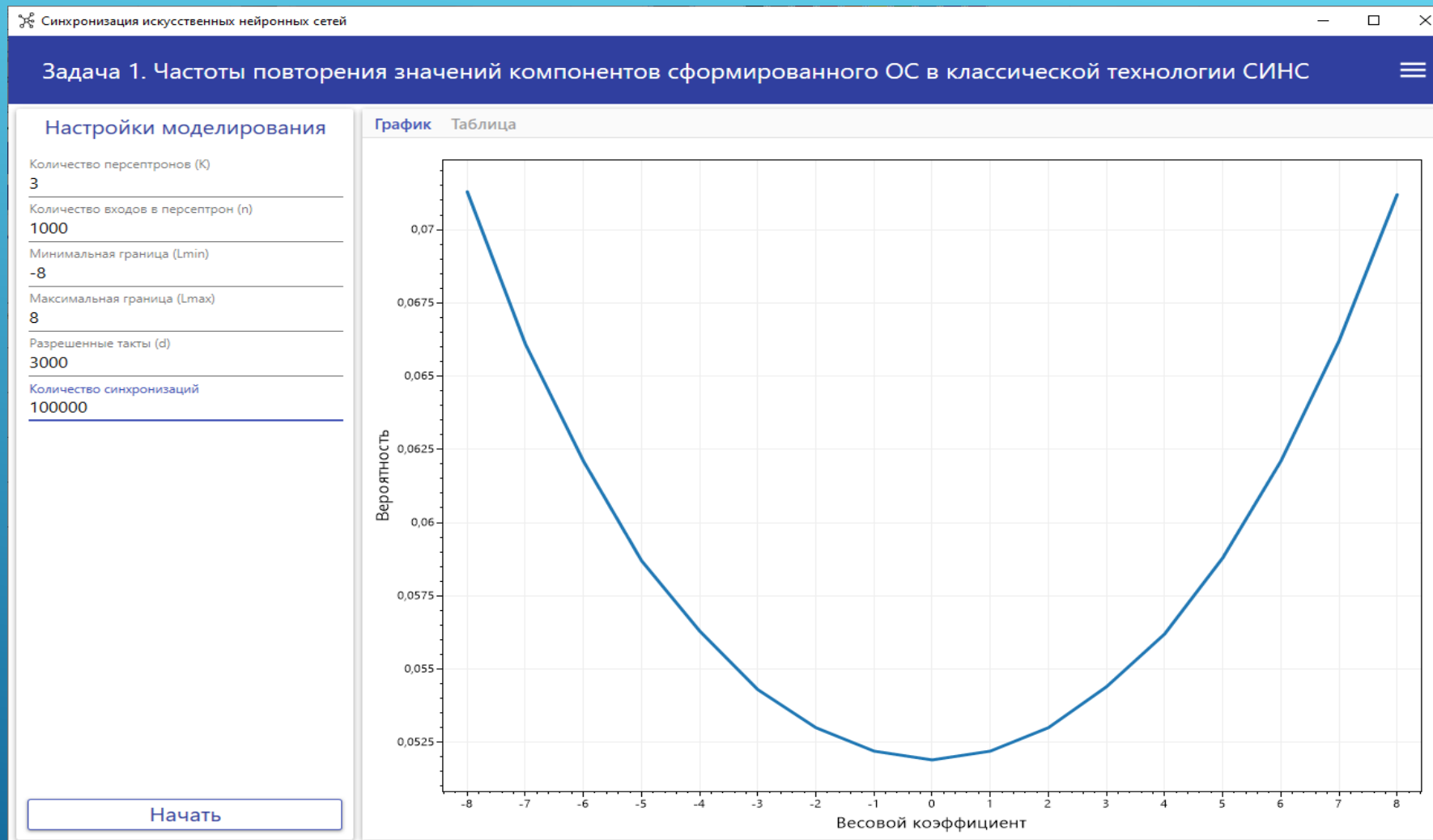
n	Pсим	Pасим
10	0,5092	0,5101
100	0,5034	0,5036
1000	0,5012	0,5011

Начать

$w_{ij(10)}$	0	1	0
$w_{ij(2)}$	0000	0001	0

-6	-7	-8
110	1111	?

Недостатки классических СИНС



Метод усиления секретности

Синхронизация искусственных нейронных сетей

Задача 6. Частоты повторения значений компонентов сформированного ОС после усиления секретности

Настройки моделирования

Количество персептронов (K)

3

Количество входов в персептрон (n)

1000

Минимальная граница (Lmin)

-7

Максимальная граница (Lmax)

8

Количество сетей для XOR (R)

10

Разрешенные такты (d)

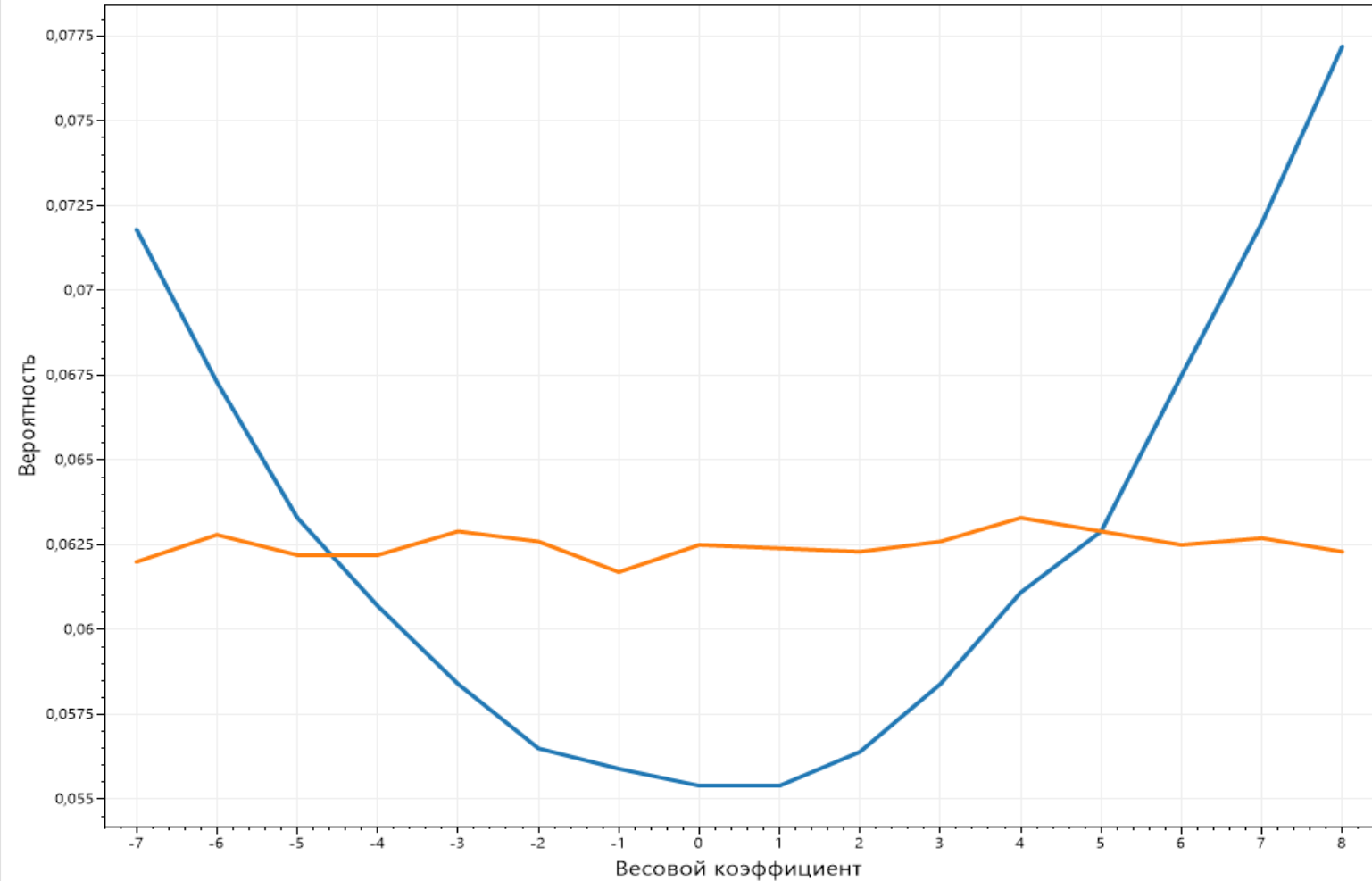
3500

Количество синхронизаций

100000

Начать

График Таблица



Комбинированный метод

1 этап

формирование частично совпадающих бинарных последовательностей с помощью синхронизируемых искусственных нейронных сетей

2 этап

устранение несовпадающих битов путем открытого сравнения четностей пар битов

Комбинированный метод

Синхронизация искусственных нейронных сетей

Задача 7. Ослабление корреляции бинарных последовательностей A и E после усиления секретности

Настройки моделирования


Количество персептронов (K)
3

Количество входов в персептрон (n)
1000

Минимальная граница (Lmin)
-7

Максимальная граница (Lmax)
8

Количество XOR (r)
5

Ограниченные такты (Duc) 
3000

Автоматическая подстановка Duc

Количество синхронизаций
100000

Таблица

d	Paб	Paе	Paбcalc	Paercalc	Naб	Naе	Naбр	Naер
500	0	0	0	0	0,6305	0,6111	0,5069	0,504
1000	0	0	0	0	0,7439	0,6589	0,5456	0,5155
1500	0,005	0	3,125E-12	0	0,8911	0,6763	0,6733	0,5194
2000	0,327	0,008	0,003739	3,277E-11	0,9741	0,6574	0,8785	0,5132
2500	0,775	0,045	0,2796	1,845E-07	0,996	0,6557	0,9759	0,5098
3000	0,946	0,053	0,7576	4,182E-07	0,9994	0,6455	0,9958	0,5088

Начать

Комбинированный метод с секретной модификацией

Синхронизация искусственных нейронных сетей

Задача 9. Корреляция векторов А, Б и Е поэтапно

Настройки симуляции

Количество персептронов (K)
3

Количество входов в персептрон (n)
1000

Минимальная граница (Lmin)
-7

Максимальная граница (Lmax)
8

Ограниченные такты (Dус)
2000

Количество XOR (r)
5

Установить конкретное значение V
 Выбирать V случайно из диапазона значений

Количество инверсируемых битов (V)
50

Количество симуляций
100000

Начать

Этап 1: XOR-синхронизация сетей

Корреляция векторов А и Б: 0.8748
Корреляция векторов А и Е: 0.5141

Этап 2: Инвертирование битов

Выбранное V: 50
Корреляция векторов А и Б: 0.8685
Корреляция векторов А и Е: 0.5139

Этап 3: Устранение несовпадающих битов

Количество шагов устранения: 4
Корреляция векторов А и Б: 1
Корреляция векторов А и Е: 0.5029
Длина бинарной последовательности (бит): 906

Стойкость к атакам

Вероятность атаки
«полного перебора»
составляет
 $2,3 * 10^{-3612}$

Вероятность атаки
«отложенного перебора»
составляет
 $4,54 * 10^{-150}$

Формирование общего ключа

Синхронизация искусственных нейронных сетей

Реализация. Синхронизация векторов весовых коэффициентов абонентов А и Б

Настройки реализации

Количество персептронов (К)
3

Количество входов в персептрон (n)
1000

Минимальная граница (Lmin)
-7

Максимальная граница (Lmax)
8

Ограниченные такты (Dус)
2000

Количество XOR (r)
5

Выбирать V случайно из диапазона значений

Установить конкретное значение V

Количество инверсируемых битов (V)
50

Желаемая длина ключа (keySize)
256

Время начала симуляции: 14:12:04
Время завершения симуляции: 14:12:08
Продолжительность симуляции: 00:00:04
Выбранное V: 50
Количество шагов устранения несовпадающих битов: 3
Длина бинарной последовательности (бит): 1190

Абонент А

MD5 бинарной последовательности сети А
27F58DC6889BF55FB1041C988021BE22

Бинарная последовательность сети А

```
01011000000111000010100100000011110000111000001111110011001101101010100011110000110100000100111100111000010110001000100101010110100010101111010001110000110000010110010111100000111010100101001000001000111011100011110001110101101010010111010110  
00000101100101111000001111010100101001000001100100111111010011010111111001011010100110010000011001010000001000111011100011110001110101101010010111010110  
110001101010110010010000100111010011110001001001011110101110110000100111011000110000111000110001000100111100010001000100110011100000  
0001010111001010001001001110110100011100111011000111010100001101011010001110011110010111011001101001111011010010001111011010010001110111010111010011100011001  
11011111010110100101101010010010100110101010100000111011101000010011000110100100100111100100100001101000000011001000001010100110010111000010001110110110  
011011111010010000101000011101110000101110001110000101010001101110010010111101001001001110001110000100010100010111011010111010011110111111101010110110  
100001011101101110011000000001111011000111011100000111001111001000110010010101110111010010010000000011110110000111001101101010011110001011000001001101  
00001101000000100011010000100000111000011011110001000110010111001110000001100100000101011101010000001010
```

Абонент Б

MD5 бинарной последовательности сети Б
27F58DC6889BF55FB1041C988021BE22

Бинарная последовательность сети Б

```
0101100000011100001010010000001111000011100000111111001100110110101010001111000011010000010011110011100001011000100010010101011010001010111101000111000011  
00000101100101111000001111010100101001000001100100111110100110101111110010110101001100100000110010100000010001110111000111100011110101101010010111010110  
110001101010110010010000100111010011110001001001011110101011101100001001110100011000011100011000101011111000100010001001110011100001000110011100000  
00010101110010100010010011101101000111001110110001110110000011010101000111001110010111011001001000111011010010010001110110100100100011101110101110100111000111001  
11011111010110100101101010010100101001010010000001110110100001001100011010010010011110010010000011001000001010100110010111000010001110110110  
01101111101001000010100001110111000010111000111000010101000101111001001011110100100100101110101011101001111101101001111101101101001111101010110110  
1000010111011011100110000000011110110001110111100001110011110010001100100101011101110100100100000000111101100001110011011010100111110001011000001001101  
000011010000001000110100001000001110000110111100010001100101110011100000011001000001010111010100000001010
```

Ключ

```
0101100000011100001010010000001111000011100000111111001100110110101010001111000011010000010011110011100001011000100010010101011010001010111101000111000011  
000001011001011110000011110101001010010000011001001111110100110101111110010110101001100100000110010
```

Начать

ЗАКЛЮЧЕНИЕ

Криптостойкость

Быстродействие

Простота реализации

СПАСИБО ЗА ВНИМАНИЕ!

Радюкевич Марина Львовна

Государственное предприятие «НИИ ТЗИ»

Начальник испытательной лаборатории по требованиям
безопасности информации

тел.+375 17 294-01-71

факс +375 17 285-31-86