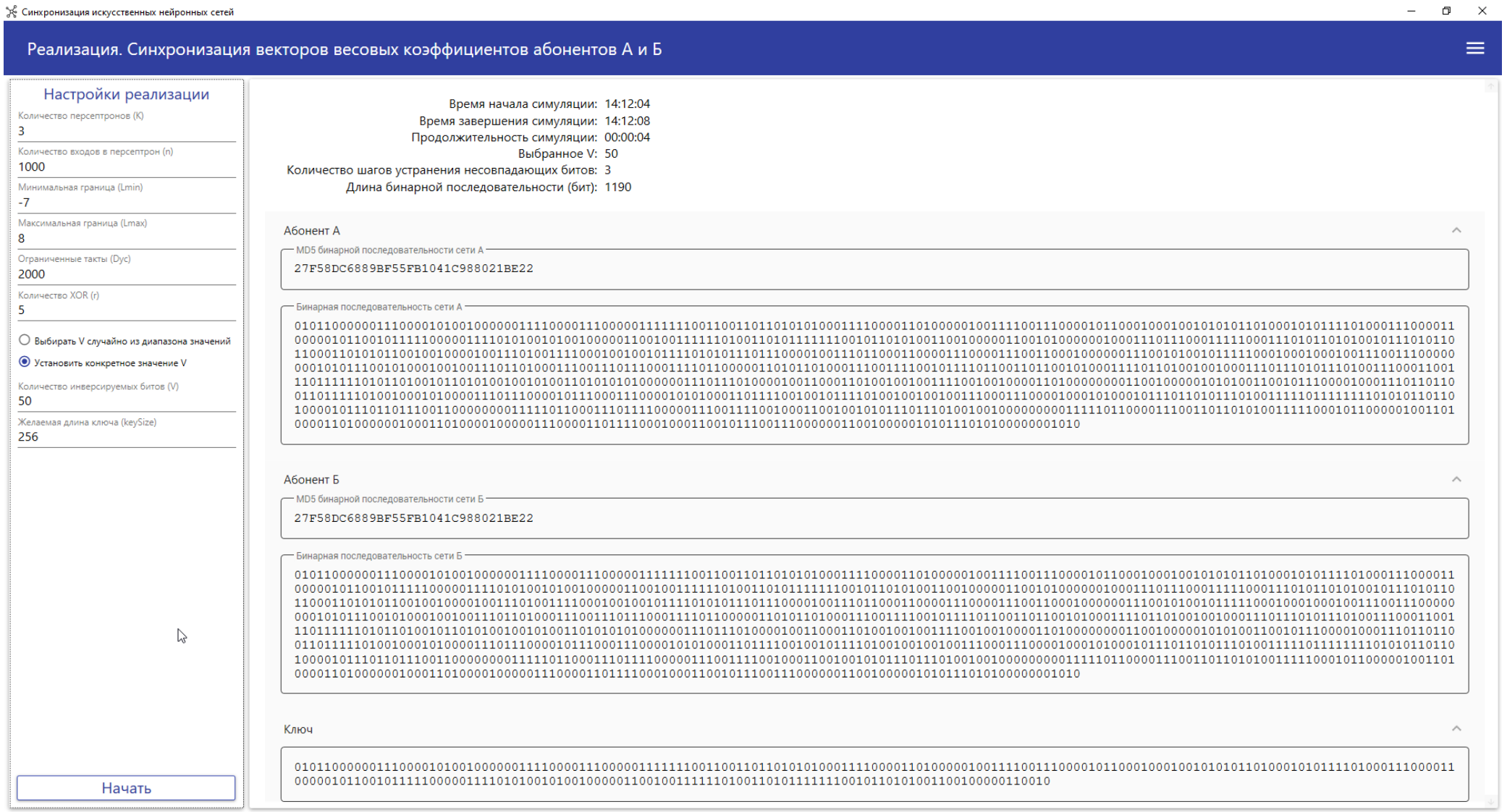
Оценка качества общего секрета, сформированного с помощью синхронизируемых искусственных нейронных сетей

М.Л.Радюкевич, М.А.Казловский
Государственное предприятие «НИИ ТЗИ»
г.Минск, Республика Беларусь

Комбинированный метод с секретной модификацией

1 шаг	Задание входных параметров ИНС: *n* - количество входов каждого персептрона; *K* - количество персептронов; *±L* - интервал возможных значений весовых коэффициентов персептронов; *r* - количество строк для функции свертки; *dyc* - количество тактов синхронизации; *V* - количество инвертируемых бит.
2 шаг	Синхронизация ИНС абонентов *A* и *B* до достижения заданного на 1 шаге количества тактов синхронизации *(dyc)*. Повторение шага 2 заданное количество раз *(r)*.
3 шаг	Выполнение функции свертки (сложение по модулю 2) *r* бинарных последовательностей (БП), полученных на шаге 2
4 шаг	Внесение некоторых изменений в БП абонентами *A* и *B*, инвертировав случайным образом независимо друг от друга *V* бит
5 шаг	Устранение несовпадений путем вычисления «четности» каждой пары битов в БП абонентов *A* и *B*

Общий секрет



Последовательности, используемые для оценки

Комбинированный метод с секретной модификацией с постоянными параметрами

$$L_1 = -7, L_2 = 8,\ K = 3, n = 1000, dyc = 2000$$

(1) – V = 25, r = 5;

(2) – V = 50, r = 2;

(3) – V = 50, r = 5;

(4) – V = 75, r = 5;

(5) – 25 ≤ V ≥ 75, r = 5.

(6) – последовательность псевдослучайных чисел, полученная с помощью алгоритма генерации псевдослучайных чисел в режиме HMAC (СТБ 34.101.47-2017, пункт 6.3)

(7) – последовательность случайных чисел, полученная с помощью физического датчика случайных чисел «Ключ-ВС»

Результаты оценки энтропии по методу NIST SP 800-90B

№	Тест проверки независимости наблюдений (p-value)	Тест проверки одинаковой распределенности наблюдений (p-value)	Тест проверки максимальной повторяющейся подстроки Pr(X >= 1)	Тесты перестановок (кол-во раундов)	Минимальная энтропия
(1)	0,941522	0,947707	1,000000	105	7,959379
(2)	0,987454	0,724174	1,000000	89	7,955625
(3)	0,825671	0,568192	0,162773	943	7,959343
(4)	0,329841	0,208132	1,000000	3194	7,962526
(5)	0,814921	0,140662	1,000000	214	7,965644
(6)	0,825211	0,961217	1,000000	110	7,963794
(7)	0,748172	0,507601	1,000000	194	7,960608

Критерии оценки:

- p-value , Pr(X >= 1) должны быть больше порогового значения 0,001
- 10000 раундов для теста перестановок
- энтропия от 0 до 8.

Результаты статистического тестирования по методу NIST SP 800-22

Наименование теста	Frequency	Block Frequency	Cumulative Sums		Runs	Longest Run	Rank	FFT	Overlapping Template	Universal	Approximate Entropy	Serial		Linear Complexity
(1)	80 0,2278	80 0,4373	80 0,1626	80 0,3115	79 0,6631	80 0,1742	80 0,1223	80 0,0487	79 0,1223	79 0,1516	79 0,6371	79 0,7887	79 0,4606	79 0,6371
(2)	79 0,9643	80 0,1866	79 0,6371	79 0,7647	79 0,1626	80 0,9114	80 0,2133	79 0,2430	80 0,6371	80 0,6631	80 0,1516	79 0,4607	78 0,5852	80 0,5595
(3)	80 0,2757	78 0,8555	79 0,9536	80 0,2430	80 0,6890	80 0,4847	80 0,0414	79 0,6890	80 0,2757	79 0,0487	80 0,5092	80 0,7887	80 0,5091	80 0,0909
(4)	78 0,7647	79 0,3924	77 0,3924	78 0,4846	79 0,3504	79 0,7647	80 0,8120	80 0,5341	79 0,8942	80 0,8555	76 0,8942	79 0,6631	80 0,6371	80 0,7147
(5)	80 0,9114	80 0,1315	80 0,5852	80 0,6371	80 0,3115	78 0,5595	79 0,8343	78 0,4607	80 0,3925	78 0,5852	78 0,1996	79 0,7147	80 0,7147	78 0,3925
(6)	79 0,0781	80 0,5852	79 0,6890	79 0,2590	77 0,3306	79 0,9869	77 0,7147	80 0,4145	76 0,1412	80 0,9986	79 0,8555	79 0,0449	78 0,0138	79 0,5341
(7)	79 0,2133	79 0,8120	79 0,7146	80 0,7373	78 0,3306	79 0,8343	80 0,1742	80 0,6371	78 0,4607	80 0,9114	80 0,4607	79 0,0020	80 0,4847	78 0,5595

Заключение

Последовательности, генерируемые с помощью комбинированного метода с секретной модификацией, состоят из равновероятных, независимых и однородных случайных чисел

СПАСИБО ЗА ВНИМАНИЕ!

Радюкевич Марина Львовна

Начальник испытательной лаборатории по требованиям безопасности информации

Государственное предприятие «НИИ ТЗИ»

www.niitzi.by
тел.+375173028171,
моб.+375447265147 (Viber, Telegram)
e-mail: dml@niitzi.by