Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.056.5

РАДЮКЕВИЧ
Марина Львовна

ФОРМИРОВАНИЕ ОБЩЕГО СЕКРЕТА С ПОМОЩЬЮ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ КРИПТОГРАФИЧЕСКИХ ПРИМЕНЕНИЙ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – методы и системы защиты информации,
информационная безопасность

Минск, 2022

Научная работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель	**Голиков Владимир Фёдорович,** доктор технических наук, профессор
Официальные оппоненты	**Урбанович Павел Павлович,** доктор технических наук, профессор кафедры информационных систем и технологий учреждения образования «Белорусский государственный технологический университет»
	Половеня Сергей Иванович, кандидат технических наук, доцент, заведующий кафедрой телекоммуникационных систем учреждения образования «Белорусская государственная академия связи»
Оппонирующая организация	Научно-исследовательское учреждение «Институт прикладных физических проблем имени А. Н. Севченко» Белорусского государственного университета

Защита состоится «12» октября 2023 г. в 10^{00} на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232, e-mail: dissovet@bsuir.by, тел. +375-17-293-89-89.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан «12» сентября 2023 г

Ученый секретарь
совета по защите диссертаций
кандидат технических наук, доцент О. В. Бойправ

ВВЕДЕНИЕ

В условиях стремительного развития информационных технологий особую значимость приобретает задача обеспечения конфиденциальности, целостности, подлинности, доступности и сохранности передаваемой информации. Утечка информации может повлечь за собой большие убытки как для компаний или государства, так и для частных лиц. Важную роль в защите информации играют криптографические методы.

В настоящее время разработано достаточно много как национальных алгоритмов криптографических преобразований, так и алгоритмов, имеющих международное признание и широкое применение. Криптостойкость систем, построенных на данных алгоритмах, базируется на секретности ключа, а не на секретности используемого преобразования. Поэтому правильно построенная система управления ключевой информацией имеет важное значение.

Появление мощных вычислительных технологий, развитие математических методов серьезно усложняют процессы распределения ключей и угрожают их безопасности. В связи с этим на сегодняшний день существует ряд работ, направленных на решение задач доставки ключевой информации абонентам сети с использованием других принципов. Одними из таких являются методы, использующие синхронизированные искусственные нейронные сети (СИНС).

Основная привлекательность данной технологии в случае ее использования в криптографических приложениях состоит в простоте реализации и исключении применения классических однонаправленных математических функций. Однако классическая технология СИНС не получила практического применения из-за недостаточной криптостойкости метода.

В настоящей работе ставится задача в более углубленном изучении технологии формирования общего секретного числа с помощью СИНС, известной под названием Synchronization of Neural Networks, оценке ее криптостойкости и разработке методов повышения конфиденциальности и быстродействия формируемого общего секрета (ФОС) по отношению к классической технологии СИНС.

В результате решение данной задачи позволит приблизить данную технологию к практическому применению.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с научными программами (проектами), темами

Тема диссертационной работы утверждена приказом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» от 31.12.2019 № 520-о.

Тема диссертации соответствует приоритетным направлениям научной, научно-технической и инновационной деятельности на 2021 – 2025 годы, утвержденным Указом Президента Республики Беларусь от 07.05.2020 № 156 (пункт 6 «Обеспечение безопасности человека, общества и государства: средства технической и криптографической защиты информации, криптология и кибербезопасность»).

Результаты диссертационных исследований применены в опытно-конструкторской работе шифр «Невод», выполняемой в рамках государственной научно-технической программы «Кибербезопасность» на 2021 – 2025 годы.

Цель, задачи, объект и предмет исследования

Цель: разработка методов и алгоритмов повышения конфиденциальности общего секрета для криптографических применений, формируемого с использованием СИНС. При этом в системе не должны использоваться процедуры, криптостойкость которых основывается на вычислительной сложности решения какой-либо математической задачи.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать технологию ФОС с помощью СИНС, известную под названием Synchronization of Neural Networks, и оценить ее криптостойкость;
- обосновать структуру и параметры СИНС, позволяющие формировать общий секрет по открытым каналам связи с наиболее высокой криптостойкостью в рамках классической технологии Synchronization of Neural Networks;
- разработать методы повышения конфиденциальности ФОС путем модификации алгоритма формирования и учета возможных моделей поведения криптоаналитика;
- разработать новый двухэтапный метод ФОС, использующий технологию СИНС на первом этапе как средство формирования частично совпадающих бинарных последовательностей (БП), с последующим устранением несовпадений.

Объектом исследования являются закономерности формирования ключевой информации с помощью СИНС. Предмет исследования – способы повышения конфиденциальности общего секрета у абонентов сети, формируемого с помощью СИНС.

Научная новизна

Решена важная научно-техническая задача, которая связана с повышением конфиденциальности общего секрета для криптографических применений, формируемого с использованием СИНС. Разработаны методы повышения конфиденциальности ФОС, которые обеспечивают существенное уменьшение корреляции между результатами синхронизации сетей

аутентифицированных абонентов и атакующей сетью, путем применения либо интеграции результатов многократно повторяемых синхронизаций, либо двухэтапной процедуры, включающей неполную синхронизацию искусственных нейронных сетей (ИНС) аутентифицированных абонентов на первом этапе и согласование этих последовательностей по методу согласования слабо совпадающих БП на втором этапе. Данные методы являются новыми. Их стойкость к возможным атакам обоснована теоретическими положениями и подтверждена статистическим моделированием.

Положения, выносимые на защиту

1. Обоснование структуры и значений параметров ИНС, позволяющих в рамках известной технологии Synchronization of Neural Networks формировать общий секрет с наиболее высокой конфиденциальностью, обмениваясь информацией по открытым каналам связи при ограниченном количестве тактов синхронизации.
2. Метод повышения конфиденциальности ФОС, базирующийся на существенном уменьшении корреляции между результатами синхронизации легальных сетей и атакующей сетью за счет применения интеграции результатов многократно повторяемых синхронизаций.
3. Комбинированный метод ФОС с помощью двухэтапной процедуры, включающий неполную синхронизацию ИНС аутентифицированных абонентов на первом этапе, обеспечивающую заданную степень совпадения формируемых случайных последовательностей, и согласование этих последовательностей по методу согласования слабо совпадающих БП на втором этапе, а также повышающий криптостойкость к известным атакам на несколько порядков и ускорение ФОС в два раза.
4. Комбинированный метод с секретной модификацией результатов синхронизации, заключающейся в секретном, независимом друг от друга изменении БП ИНС A и B, сформированных после первого этапа метода, и позволяющей при незначительном увеличении количества обменов информацией обеспечить криптостойкость по отношению к атаке отложенным перебором, соизмеримую с криптостойкостью случайной БП размером более 256 битов.

Личный вклад соискателя ученой степени в результаты диссертации с отграничением их от соавторов совместных исследований и публикаций

Содержание диссертационной работы отражает личный вклад автора, заключающийся в разработке методов, получении, интерпретации и анализе результатов исследований. Совместно с научным руководителем доктором технических наук, профессором Голиковым Владимиром Федоровичем определены структура, цели и задачи исследования, обобщены основные

научные результаты. Совместно с соавтором публикации студентом БНТУ Слепцовым А. П. осуществлялась подготовка и проведение исследований (моделирования), обсуждались полученные результаты. Результаты, полученные соавторами публикаций, в диссертацию не вошли.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях: VI Международная научно-техническая интернет-конференция «Информационные технологии в образовании, науке и производстве», БНТУ (Минск, 2018); XXIV научно-практическая конференция «Комплексная защита информации» (Витебск, 2019); III Белорусский ИКТ Саммит (Минск, 2019); XXV научно-практическая конференция «Комплексная защита информации» (Москва, 2020); XXVI научно-практическая конференция «Комплексная защита информации» (Минск, 2021); XXVII научно-практическая конференция «Комплексная защита информации» (Москва, 2022); 58-я научная конференция аспирантов, магистрантов и студентов БГУИР (Минск, 2022); XX Белорусско-российская научно-техническая конференция «Технические средства защиты информации», БГУИР (Минск, 2022).

Внедрение результатов диссертации подтверждено актом о практическом использовании результатов исследований и актом внедрения результатов исследования в учебный процесс.

Опубликованность результатов диссертации

По результатам выполненных исследований опубликовано 12 научных работ общим объемом 4,6 авторского листа. Из них 4 статьи объемом 2,3 авторского листа в рецензируемых научных журналах в соответствии с пунктом 19 Положения о присуждении ученых степеней и присвоении ученых званий, 6 публикаций в материалах и сборниках трудов научных конференций объемом 2,15 авторского листа, 2 тезиса докладов на научных конференциях объемом 0,15 авторского листа.

Структура и объем диссертации

Работа состоит из введения, общей характеристики работы, пяти глав, заключения, списка использованных источников, двух приложений. Список использованных источников включает библиографический список из 65 наименований и список публикаций соискателя ученой степени из 12 наименований. Общий объем – 116 страниц, в том числе 42 иллюстрации, 17 таблиц.

ОСНОВНАЯ ЧАСТЬ

В первой главе рассматривается современное состояние изучаемого вопроса. Технология СИНС представляется как метод открытого ФОС, не использующий классические односторонние функции, и претендует на роль альтернативного метода распределения ключевой информации. Несмотря на многочисленные научные публикации, посвященные СИНС, метод не нашел практического применения и всерьез не рассматривается классической криптографической наукой. Предположительно основной причиной этого являются вероятностный характер процессов успешного ФОС и его взлома злоумышленником, отсутствие строго математического доказательства безопасности используемой процедуры. В связи с этим в настоящей работе исследована безопасность метода, рассмотрены пути ее повышения, что в итоге позволяет приблизить данную технологию к практическому применению.

Суть данного метода следующая. Две нейронные сети, имеющие TPM - архитектуру (Tree Parity Machine, дерево машины четности) со случайными и секретными значениями весовых коэффициентов (ВК) синхронизируются общими случайными воздействиями, обмениваются выходными величинами, корректируют значения ВК своих сетей. Синхронизация продолжается до совпадения значений ВК обеих сетей. Эти значения и являются общим секретом. Процесс синхронизации наиболее часто рассматривается в терминах взаимного обучения ИНС.

Архитектура каждой сети состоит из K персептронов, принадлежащих внутреннему (скрытому) слою. Каждый из них имеет n входов, следовательно, вектор входных значений всей сети равен $K \times n$. В этой архитектуре приняты следующие обозначения: x_{ij} – j-й вход i-го персептрона, Y_i – выход i-го персептрона, где $i=1,2,\ldots,K$ и $j=1,2,\ldots,n$. Компоненты входного вектора X бинарные – $x_{ij}=\pm 1$. ВК персептронов равны w_{ij}. Выход всей архитектуры $Z^{A/B}$ – это произведение всех выходных величин внутренних персептронов. Индекс A/B означает, что операция касается обеих сетей A и B, а единичный индекс – одной сети соответственно. Внутри каждой сети корректируются веса только тех персептронов, выходная величина которых равна величине Z всей сети. Процесс коррекции идет по правилу Хебба

$$w_{ij}^{A/B} = \begin{cases} w_{ij}^{A/B} + Z^{A/B} \times x_{ij}, \text{если } Z^A = Z^B \text{ и } Z^{A/B} = Y_i^{A/B}, \\ w_{ij}^{A/B}, \text{ в противном случае.} \end{cases} \quad (1)$$

Кроме того, учитывается ограничение $w_{ij}^{A/B} \in [-L, L]$:

$$w_{ij}^{A/B} = \begin{cases} \pm L, \text{ если } \left|w_{ij}^{A/B}\right| > L, \\ w_{ij}^{A/B}, \text{ в противном случае,} \end{cases} \quad (2)$$

где L – целое положительное число.

Векторы ВК ИНС *A* и *B*:

$$w^A = w_{11}^A, w_{12}^A, \ldots w_{1n}^A, w_{21}^A, w_{22}^A, \ldots w_{2n}^A, \ldots w_{K1}^A, w_{K2}^A, \ldots w_{Kn}^A; \quad (3)$$

$$w^B = w_{11}^B, w_{12}^B, \ldots w_{1n}^B, w_{21}^B, w_{22}^B, \ldots w_{2n}^B, \ldots w_{K1}^B, w_{K2}^B, \ldots w_{Kn}^B, \quad (4)$$

в процессе синхронизации сближаются и на некотором шаге $t = t_C$ становятся равными $w^A(t_c) = w^B(t_c)$, где t = 1,2, … – номер такта. Условные траектории изменения этих векторов приведены на рисунке 1.

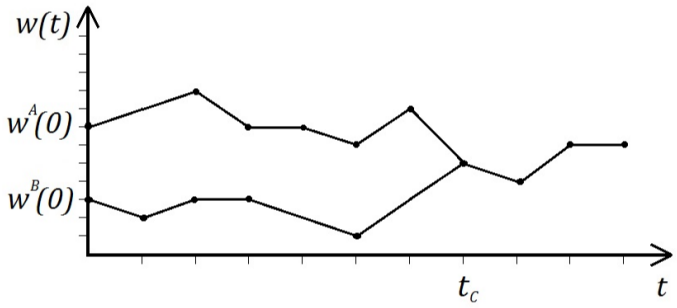

Рисунок 1 – Траектории движения векторов ВК при синхронизации сетей *A* и *B*

Величина t_c является случайной величиной, поэтому, если за выбранное количество тактов $t = d$ окажется, что $t_c \le d$, то процесс формирования является успешным. Так как значение t_c остается неизвестным абонентам в ходе синхронизации, то возникает вопрос о выборе значения величины *d*. С точки зрения безопасности и быстродействия формируемого секрета желательно *d* выбирать как можно меньшим числом. При этом число тактов обмена информацией между *A* и *B* будет минимальным, но уменьшается вероятность события $t_c \le d$. Величину *d* можно предварительно назначать по результатам моделирования и корректировать ее значение входе реальной синхронизации. Так как равенство $w^A(t_c) = w^B(t_c)$ стороны *A* и *B* не могут фиксировать по наблюдаемым несекретным параметрам, то они вынуждены обмениваться значениями некоторой функции $f(w^{A/B}(t))$, которая должна обладать следующими свойствами:

1) если $f(w^A(t)) = f(w^B(t))$, то $w^A(t) = w^B(t)$;

2) зная $f(w^{A/B}(t))$, вычисление $w^{A/B}(t)$ представляет собой задачу огромной вычислительной сложности;

3) зная $w^{A/B}(t)$, относительно легко вычисляется $f(w^{A/B}(t))$.

Этим условиям наиболее полно соответствуют функции, относящиеся к классу хэш-функций и широко используемые в криптографии.

Важной характеристикой технологии СИНС является скорость ФОС. Поскольку вычислительные операции при синхронизации сетей чрезвычайно просты, то очевидно, что быстродействие рассматриваемого алгоритма ФОС

следует оценивать количеством тактов (сеансов) обмена информацией по открытому каналу связи между абонентами *A* и *B*. В классической технологии СИНС в каждом такте обмена пересылается один бит информации, но количество таких тактов может составлять тысячи, десятки тысяч, сотни тысяч. С точки зрения технической реализации и криптостойкости целесообразно использовать минимально возможное число обменов. Поэтому при выборе структуры и параметров следует отдавать предпочтение структуре и значениям параметров сетей, обеспечивающих быструю синхронизацию.

Предложенная технология ФОС с момента опубликования первых работ исследовалась на криптостойкость. С позиции классической криптографии криптоаналитик, наблюдающий за процессом синхронизации, владеет всей информацией о структуре и параметрах ИНС, что и аутентифицированные абоненты *A* и *B*, и имеет возможность перехватывать всю информацию, пересылаемую по открытому каналу связи.

Известные атаки на технологию СИНС построены на создании некоторого вектора ВК $w^E(t)$, коррелированного с векторами $w^A(t)$, $w^B(t)$, и размерность которого совпадает с размерностями $w^A(t)$, $w^B(t)$. Для этого криптоаналитик *E* создает ИНС аналогичную ИНС *A* и синхронизирует ее с сетью *A*, которая синхронизируется с ИНС *B*.

Далее рассматриваются различные атаки. Показано, что одной из самых эффективных атак является геометрическая атака в сочетании с атакой отложенного перебора. Для этой атаки существующая технология СИНС не обладает достаточной криптостойкостью для практического применения в надежных криптосистемах.

Во второй главе анализируются потенциальные возможности классической технологии СИНС. В опубликованных работах по технологии СИНС приводятся результаты имитационного моделирования СИНС с различными параметрами. Их основной результат заключается в доказательстве и демонстрации того, что процесс синхронизации сетей *A* и *B* (двухстороннее обучение) имеет преимущество перед синхронизацией сетей *A* и *E* (одностороннее обучение), и этот факт позволяет рекомендовать рассматриваемую технологию для практического использования. Вместе с тем отсутствуют ответы на многие критичные вопросы, например:

1) какие значения *K, n, L* обеспечат требуемую вероятность успешного ФОС при допустимой вероятности успеха криптоаналитика и эквивалентной криптостойкости современных алгоритмов шифрования;

2) как выбрать число необходимых тактов синхронизации;

3) как убедиться в успехе синхронизации ИНС *A* и *B* и чем при этом они рискуют;

4) как преобразовать десятичную последовательность случайных чисел, полученную при синхронизации, в БП, сохранив при этом равномерность распределения.

Показано, что основными характеристиками, позволяющими оценивать успешность и безопасность ФОС, следует считать вероятность удачной

синхронизации сетей *A* и *B,* а также вероятность удачной попытки обучения сети *E* при выбранном значении *d*: $P_{AB} = P(t_{AB} \le d)$, $P_{AE} = P(t_{AE} \le d)$, где t_{AB} – номер такта, начиная с которого $w^A(t_{AB}) = w^B(t_{AB})$, t_{AE} – номер такта, начиная с которого $w^A(t_{AE}) = w^E(t_{AE})$.

Кроме вероятностей P_{AB} и P_{AE} для анализа процесса синхронизации будет полезно использовать показатель корреляционной зависимости между векторами w^A, w^B и w^E, w^A. Если сравнивать две последовательности десятичных чисел длиной $n \times K$, составляющих компоненты ВК двух векторов, то их схожесть можно оценить количеством совпадающих чисел в этих последовательностях n^c. Применительно к рассматриваемым векторам – n^c_{AB} и n^c_{AE}. Величина n^c является случайной и очевидно, что она может принимать значения от 0 (нет совпадающих чисел) до $n \times K$ (все числа совпадают). Механизм синхронизации двух ИНС изменяет величину корреляции векторов от нулевой (сравниваемые последовательности чисел статистически независимы) до полной (сравниваемые последовательности чисел идентичны). Таким образом, среднее значение $\overline{n^c}$ можно применять как упрощенную вероятностную характеристику корреляционной связи векторов. Иногда нагляднее использовать относительную величину $\overline{n^c} / n \times K$, изменяющуюся от 0 до 1. Для оценки корреляции между БП чисел предложено использовать $\overline{n^{cb}} / (n \times K \times l)$, где $\overline{n^{cb}}$ – среднее значение совпадающих битов. Этот индикатор изменяется от 0,5 при статистически независимых БП до 1 при идентичных БП. В таблице 1 показана динамика изменения $\overline{n^c}$ для ИНС *A* и *B* с параметрами $K = 3, n = 1000, L = 8$.

Таблица 1 – Динамика изменения $\overline{n^c_{AB}}$

d	0	100	200	400	800	1000	2000	3000	4000
$\overline{n^c_{AB}}$	175	283	356	492	806	1077	2809	2997	2999
$\overline{n^c} / n \times K$	0,058	0,094	0,118	0,164	0,268	0,359	0,936	0,999	0,999

Далее исследуется влияние параметров *n, K, L, d* на безопасность ФОС и быстродействие и обосновываются базовые значения этих параметров.

Кроме фактора безопасности формируемого секрета, необходимо учитывать и фактор допустимой продолжительности синхронизации. Очевидно, что в силу простоты программной реализации используемых ИНС, чисто вычислительные процедуры занимают незначительное время, однако результат вычислений на каждом такте синхронизации должен передаваться по каналу связи, т.е. число обменов информацией зависит от *d*. Вопрос о конкретном допустимом значении *d* зависит от технической реализации ИНС и канала связи, но тем не менее при любой реализации очевидно, что чем меньше будет число обменов информацией, тем выше быстродействие и надежность технологии.

Таким образом, установлено, что базовыми значениями параметров ИНС, обеспечивающими наиболее приемлемые вероятности успешного формирования общего секрета $P(t_{AB} \le d) = 0{,}994$ и его безопасности $P(t_{AE} \le d) = 0{,}045$, следует считать $n = 1000$, $K = 3$, $L = 8$, $d = 4000$.

Третья глава посвящена разработке метода повышения конфиденциальности криптографического ключа, сформированного с помощью СИНС. Повышение безопасности ФОС следует искать за счет снижения корреляции ВК векторов $w^E(t)$ и $w^A(t)$ при сохранении ее для ВК $w^A(t)$ и $w^B(t)$. Подобная постановка задачи в самом обобщенном виде в терминах информационно-вероятностного подхода изложена у Bennett C. H. и названа усилением секретности.

Применительно к нашей задаче исходная ситуация следующая. *A* и *B*, выбрав указанные ранее значения параметров своих ИНС, проводят r независимых друг от друга синхронизаций за d назначенных тактов. В результате получают r векторов ВК: абонент *A* имеет $w_1^A, w_2^A, w_3^A, ..., w_r^A$, абонент *B* – $w_1^B, w_2^B, w_3^B, ..., w_r^B$. Важным обстоятельством является то, что *A* и *B* не проводят проверку идентичности полученных векторов, т. е. проверка условия $w_i^A = w_i^B$, где $i = 1, 2, 3, ..., r$, исключается. Далее *A* преобразует каждый вектор w_i^A в БП (строку) S_i^A, где $S_i^A = \{0,1\}^b$, b – длина последовательности в битах. Аналогичное преобразование производит *B*: $w_i^B \to S_i^B$. Для реализации процедуры усиления секретности *A* и *B* полученные двоичные строки сжимают в итоговую строку заданного размера $\{S_1^A, S_2^A, ..., S_r^A,\}^{rb} \to \{K^A\}^b$, $\{S_1^B, S_2^B, ..., S_r^B,\}^{rb} \to \{K^B\}^b$.

После этого *A* и *B* проверяют идентичность сформированных строк K^A, K^B. В случае совпадения имеют общий секрет $K^{AB} = K^A = K^B$. При несовпадении сеанс формирования повторяется. При такой стратегии абонентов *A* и *B* криптоаналитик *E* вынужден выполнять те же операции, что *A* и *B,* и в итоге получает $\{S_1^E, S_2^E, ..., S_r^E,\}^{rb} \to \{K^E\}^b$ и может сравнить K^E с K^A. Реализуя перечисленные процедуры, *A* и *B* предполагают, что высокая на шаге $t = d$ корреляция между строками S_i^A и S_i^B сохранится и между K^A и K^B, а низкая корреляция между S_i^E и S_i^A еще более снизится между K^E и K^A. В таблице 2 приведены относительные средние значения числа совпадающих битов $\overline{n_{AB,r}^c} / (n \times K \times l)$, $\overline{n_{AE,r}^c} / (n \times K \times l)$ в двух парах коррелированных БП: K^A с K^B и K^E с K^A для $r = 1$ и $r = 5$.

Таблица 2 – Корреляция векторов ВК при разных r

d	$\overline{n^c_{AB,1}}/(n\times K\times l)$	$\overline{n^c_{AE,1}}/(n\times K\times l)$	$\overline{n^c_{AB,5}}/(n\times K\times l)$	$\overline{n^c_{AE,5}}/(n\times K\times l)$
10	0,532	0,532	0,500	0,499
500	0,594	0,582	0,502	0,501
1000	0,679	0,616	0,537	0,507
2000	0,972	0,648	0,886	0,506
3000	0,999	0,635	0,996	0,502

В качестве процедуры сжатия использовалось побитовое сложение по модулю 2 всех битов множества $\{S_i\}$.

В результате такого сложения для каждой ИНС получаем БП длиной b, в которой каждый бит – сумма битов по модулю 2 из r слагаемых.

Как видно из таблицы 2 для $r=1$ (нет усиления секретности) с увеличением d индикатор корреляции $\overline{n^c_{AB,1}}/(n\times K\times l)$ нарастает от 0,5 (при $d=0$) до 0,999 ($d=3000$) и $\overline{n^c_{AE,1}}/(n\times K\times l)$ от 0,5 до 0,635.

Для $r=5$ реализация предложенной процедуры усиления секретности привела к тому, что максимальная корреляция K^A с K^B практически не изменилась по сравнению с обычной синхронизацией и равна $\overline{n^c_{AB,5}}/(n\times K\times l)=0,996$, а корреляция K^E с K^A значительно снизилась и равна $\overline{n^c_{AE,5}}/(n\times K\times l)=0,502$, что свидетельствует о слабой связи векторов ВК ИНС A и ИНС E.

Далее исследуется влияние предложенного метода усиления секретности на успешность ФОС и его безопасность.

Доказано, что при предложенных значениях параметров СИНС K, n, L, d вероятность успеха криптоаналитика $P_{AE,r}$ зависит от r экспоненциально и может быть выбрана сколь угодно малой увеличением r, в то время как для A и B вероятность $P_{AB,r}$ зависит от r линейно, а успешность обеспечивается относительно небольшим увеличением количества сеансов ФОС.

Однако надо учитывать, что описанный эффект будет иметь место при таких параметрах сетей A и B, когда $P_{AE}\ll 1$, а $P_{AB}\approx 1$.

Важным положительным свойством предложенного метода является и то, что с ростом r возрастает равномерность распределения сформированной БП.

В четвертой главе описывается разработанный комбинированный метод формирования общего секрета. Суть комбинированного метода заключается в том, что на первом этапе используются синхронизация ИНС с заведомо недостаточным для полного совпадения их ВК количеством тактов (формирование частично совпадающих БП), а на втором этапе устраняются несовпадающие биты (устранение ошибок).

Проведенные исследования показали, что уже при $d>2000$ относительное среднее число совпадающих битов $\overline{n^{cb}_{AB}}/b$ приближается к 1,

в то время как $\overline{n_{AE}^{cb}} / b$ близко к 0,5.

Эта закономерность и положена в основу комбинированного метода. На первом этапе абоненты *A* и *B*, синхронизируют СИНС со структурой и параметрами, описанными в предыдущей главе. Процесс останавливается на некотором такте $t = d_{yc}$ $(d_{yc} < d)$, при котором еще не достигнуто полное равенство $w^A(d_{yc})$ и $w^B(d_{yc})$ и вероятность совпадения ВК у сетей *A* и *B* гарантировано ниже чем 1, т. е. синхронизация является досрочно прерванной. Таким же образом производится *r* независимых синхронизаций с различными начальными значениями ВК, а результирующие бинарные векторы $K^A(d_{yc})$ и $K^B(d_{yc})$ вычисляются как некоторая свертка результатов каждой синхронизации:

$$K^A(d_{yc}) = S_1^A(d_{yc}) \oplus S_2^A(d_{yc}) \oplus ... \oplus S_r^A(d_{yc}) = k_1^A, k_2^A, ..., k_b^A; \quad (5)$$

$$K^B(d_{yc}) = S_1^B(d_{yc}) \oplus S_2^B(d_{yc}) \oplus ... \oplus S_r^B(d_{yc}) = k_1^B, k_2^B, ..., k_b^B, \quad (6)$$

где k_i^A, k_i^B – биты последовательностей *A* и *B* соответственно, каждый бит – сумма битов по модулю 2 из *r* слагаемых.

На втором этапе производится устранение несовпадающих битов БП $K^A(d_{yc})$ и $K^B(d_{yc})$. Абоненты *A* и *B* согласованно разбивают свои БП на пары битов либо случайным образом, либо по порядку номеров. Далее *A* и *B* вычисляют четности каждой пары битов $C_i^A = k_j^A \oplus k_{j+1}^A$, $C_i^B = k_j^B \oplus k_{j+1}^B$, где i – номер пары, k_j^A, k_j^B – j-й бит БП *A* и *B* соответственно. Абоненты *A* и *B* сообщают четности пар друг другу по открытому каналу связи и каждый сравнивает четности соответствующих пар C_i^A с C_i^B. Пары битов, имеющие одинаковую четность, остаются в БП, а пары с несовпадающими четностями удаляются, в них содержится один несовпадающий бит. В оставшихся парах имеет место либо 0 несовпадающих битов, т. е. $k_j^A = k_j^B$ и $k_{j+1}^A = k_{j+1}^B$, либо 2, т. е. $k_j^A \neq k_j^B$ и $k_{j+1}^A \neq k_{j+1}^B$. Так как оглашение четности пары позволяет выразить один неизвестный бит через четность и другой бит $k_j^A = C_i^A - k_{j+1}^A$ и $k_j^B = C_i^B - k_{j+1}^B$, то для сохранения секретности из каждой пары удаляется по договоренности один бит. Отобранные таким образом биты объединяются в промежуточные БП, которые содержат меньшее количество несовпадающих битов. Повторяя описанную процедуру еще несколько раз, можно получить полностью совпадающие БП. Количество необходимых итераций λ зависит от числа совпадающих битов в согласуемых БП. В таблице 3 приведена зависимость среднего числа необходимых итераций от среднего числа совпадающих битов.

Таблица 3 – Зависимость числа итераций от среднего числа совпадающих битов

$\overline{n_{AB}^{c}} / b$	0,51	0,52	0,55	0,6	0,7	0,8	0,9
$\overline{\lambda}$	7	5	5	4	3	2	2

Из таблицы 3 следует, что даже при самой слабой корреляции согласуемых БП число необходимых итераций в среднем не превышает 7, что соответствует корреляции БП *A* и БП *B* при $d_{yc} = 1000$. Однако при этом в ходе согласования БП их длина уменьшается как минимум в среднем 2^{λ} раз. Короткая БП может быть взломана простым перебором возможных значений, поэтому целесообразно величину d_{yc} выбирать не менее 2000. При этом $\overline{n_{AB}^{c}} / b \geq 0{,}8$, а число необходимых итераций не превышает 3. Таким образом, вся процедура предлагаемого метода составляет d_{yc} тактов синхронизации и λ тактов фильтрации несовпадающих битов $\tau_k = d_{yc} + \lambda$.

Далее рассматриваются возможные атаки. На первом этапе возможна атака отложенного перебора, криптоаналитик *E* создает свою сеть, идентичную сетям *A* и *B* за исключением начальных значений ВК, синхронизирует (методом отложенного перебора) свою сеть с сетью, например, *A* в надежде, что его сеть успеет полностью синхронизоваться за отведенное число тактов d_{yc}. В этом случае окажется, что $K^E(d_{yc}) = K^A(d_{yc})$ и сформированный ключ будет полностью дискредитирован.

На втором этапе знание *E* объявленных четностей пар битов и тот факт, что за счет синхронизации возникает корреляция между $K^E(d_{yc})$ и $K^A(d_{yc})$, может позволить ему использовать данную информацию для вычисления некоторых битов в итоговой БП.

Вероятность успеха атаки отложенного перебора равна $P(K^E(d_{yc}) = K^A(d_{yc})) = P_{AE,r}(d_{yc})$ и зависит от выбора r и d_{yc}. Например, если *A* и *B* для своих сетей выбрали $K = 3$, $n = 1000$, $L_1 = -7$, $L_2 = 8$, а параметры $r = 5$, $d_{yc} = 2000$, то вероятность успеха атаки отложенного перебора $P_{AE,r} = 1{,}02 \times 10^{-12}$. При этом следует иметь в виду, что число необходимых тактов обмена информацией всего 2000.

На втором этапе метода, когда абоненты *A* и *B* оглашают четности пар БП, сформированных с помощью СИНС, у криптоаналитика *E* появляется возможность сравнения этих четностей с четностями своей БП и сделать определенные выводы относительно ФОС. Показано, что в силу низкой корреляции $K^E(d_{yc})$ и $K^A(d_{yc})$ пары битов $K^E(d_{yc})$ и $K^A(d_{yc})$, равные между собой, неразличимы для *E* по вероятности с парами битов с противоположными значениями и не могут быть установлены.

Таким образом, атака, использующая знание четностей БП, сформированных A и B комбинированным методом, при правильно выбранных параметрах сетей не позволяет дискредитировать ФОС.

Тем не менее, для особо ответственных задач за счет усложнения процедуры комбинированного метода имеется возможность существенно повысить конфиденциальность ФОС.

Комбинированный метод с секретной модификацией результатов синхронизации. При отложенном переборе существует достаточно большое множество начальных значений вектора весовых коэффициентов ИНС E, движение из которых при благоприятных траекториях $x(t)$ позволяет обеспечить пересечение траекторий движения $K^A(t)$ и $K^E(t)$, в смысле равенства всех их элементов. После такого пересечения траектории движения $K^A(d)$ и $K^E(d)$ совпадают при всех последующих тактах синхронизации. В результате обязательно наступит $K^E(d_{yc}) = K^A(d_{yc})$. Таким образом, если при классическом полном переборе значений успех атаки наступает при единственно правильном наборе ВК ИНС E, то в атаке отложенного перебора успех атаки наступает при всех наборах, для которых ВК ИНС E пересеклись с ВК ИНС A на участке от $t = 0$ до $t = d_{yc}$. Этот эффект качественно поясняется на рисунке 2. Необязательность продолжать синхронизацию ИНС A или B до полного совпадения ВК этих сетей в комбинированном методе позволяет до оглашения четностей пар битов C_i^A, C_i^B внести некоторые изменения в БП $K^A(d_{yc})$ абонентом A и в $K^B(d_{yc})$ абонентом B случайным образом, независимо друг от друга.

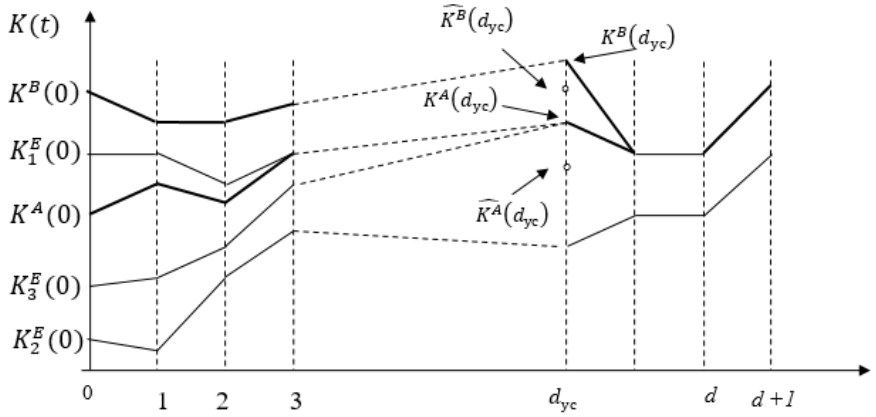

Рисунок 2 – Модификация результата синхронизации

Вносимые изменения в $K^A(d_{yc})$ и $K^B(d_{yc})$ должны обеспечивать невозможность их аналитического вычисления E по объявленным четностям БП $K^A(d_{yc})$ и $K^B(d_{yc})$. Вычисление должно сводиться к перебору вариантов внесенных изменений. Наиболее простой в реализации модификацией можно

считать инвертирование некоторого количества битов, выбранных случайно в БП $K^A(d_{yc})$ и $K^B(d_{yc})$.

Возможные атаки строятся на базе отложенного перебора. Абонент *E* повторяет синхронизации своей сети с зафиксированной синхронизацией ИНС *A* и *B,* перебирая начальные значения ВК своих сетей, и останавливает перебор, если оказалось, что $C_i^E = C_i^A$, где C_i^A соответствует $K^A(d_{yc})$, и процесс удаления несовпадающих битов в $K^E(d_{yc})$ полностью совпал с процессом удаления несовпадающих битов в $K^A(d_{yc})$. Так как при относительно небольших выбранных значениях d_{yc} корреляция между $K^E(t)$ и $K^A(t)$ довольно слабая $(\overline{n_{AE}^c} / b \approx 0{,}5)$, то различные траектории $K^E(t)$ можно считать независимыми между собой, а перебор в данном случае эквивалентен поиску такой единственной совокупности начальных значений ВК своей сети, которые приведут ИНС *E* к попаданию в точку $K^A(d_{yc})$. Следовательно, вероятность успеха такого перебора P_{op1} близка к величине $(2L)^{-K\times n}$. Например, для $L=8$, $K=3$, $n=1000$ имеем $P_{op1} = 4{,}3\times 10^{-3613}$.

Второй вариант атаки заключается в том, что абонент *E*, перебирая начальные значения ВК своих сетей, доводит каждую синхронизацию $K^E(t)$ до $t = d_{yc}$, затем модифицирует полученную БП по аналогии с модификацией, проделанной *A* и *B*, перебирая все возможные варианты инвертирования битов. Вероятность успеха этой атаки равна $P_{op2} \approx P_{AE,r}(d_{yc}) \times (C_V^b)^{-1}$. Если $K=3$, $n=1000$, $L_1=-7$, $L_2=8$, $r=5$, $d_{yc}=2000$, $b=12000$, $V=50$, тогда

$$P_{op2} = (1{,}02\times 10^{-12}) \times (2{,}7\times 10^{-139}) \approx 2{,}75\times 10^{-151}. \qquad (7)$$

Таким образом, комбинированный метод с секретной модификацией результата синхронизации существенно повышает криптостойкость ФОС.

Пятая глава посвящена программной модели для статистического моделирования процессов синхронизации ИНС.

Целью разработки программной модели является реализация статистического моделирования, необходимого для получения результатов в пределах поставленных в диссертации задач исследования, а также реализация комбинированного метода с секретной модификацией результатов синхронизации для формирования общего секрета.

Программа позволяет выполнить моделирование следующих задач исследований:

Задача 1. Частоты повторения значений компонентов сформированного общего секрета в классической технологии СИНС;

Задача 2. Динамика корреляции компонентов векторов в десятичном виде сетей A и B;

Задача 3. Вероятность синхронизации сетей A с B и A с E при изменении параметров n, K, L;

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

Задача 5. Влияние параметра r на корреляцию БП сетей A и B, A и E;

Задача 6. Частоты повторения значений компонентов ФОС после усиления секретности;

Задача 7. Ослабление корреляции БП A и E после усиления секретности;

Задача 8. Оценка вероятностей гипотез;

Задача 9. Корреляция векторов сетей A и B, A и E поэтапно.

Также в программе реализован комбинированный метод с секретной модификацией результатов синхронизации для формирования общего секрета.

До начала выполнения каждой задачи существует возможность задать начальные параметры в окне «Настройки моделирования».

Результаты моделирования задач представляются в виде графика или таблицы в зависимости от задачи.

В **Приложении А** диссертации представлен программный код разработанной программной модели для статистического моделирования процессов синхронизации ИНС.

В **Приложении Б** диссертации представлены копии документов, подтверждающих прикладное значение результатов диссертации.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Формирование общего секрета с помощью синхронизируемых искусственных нейронных сетей представляет собой перспективную технологию создания секретных криптографических ключей, обладающую простотой реализации и не использующую принципы асимметричной криптографии, основанные на вычислительной трудности решения обратных задач. Для статистического моделирования процессов синхронизации искусственных нейронных сетей разработана программная модель [1, 11].

2. Установлено, что традиционная структура искусственных нейронных сетей, используемая в технологии синхронизации искусственных нейронных сетей, с рационально выбранными параметрами n, K, L не позволяет за практически приемлемое число тактов синхронизации обеспечить безопасность формирования общего секрета, соизмеримую с криптостойкостью современных алгоритмов симметричного шифрования [2, 5, 6].

3. Разработан метод повышения конфиденциальности формирования общего секрета, основанный на снижении корреляционной зависимости между бинарными последовательностями криптоаналитика и абонентов A и B

за счет специального сжатия результатов многократной синхронизации искусственных нейронных сетей A и B. В качестве функции сжатия предложена свертка r независимых между собой бинарных последовательностей, сформированных искусственными нейронными сетями A и B, в одну последовательность побитовым сложением по модулю 2 соответствующих элементов последовательностей [2, 7].

4. Проанализирована безопасность формирования общего секрета методом усиления секретности. Доказано, что при предложенных значениях параметров синхронизируемых искусственных нейронных сетей K, n, L, d вероятность успеха криптоаналитика ($P_{AE,r}$) зависит от r экспоненциально и может быть выбрана сколь угодно малой увеличением r, в то время как для A и B вероятность успешного сеанса поддерживается за счет повторных сеансов синхронизации [2, 7].

5. Разработан двухэтапный метод формирования общего секрета, в котором на первом этапе реализуется незавершенная синхронизация искусственных нейронных сетей, а на втором этапе удаляются несовпадающие биты на основе результатов обмена информацией по открытому каналу связи. Исследование безопасности этого метода показали, что в совокупности с методом усиления секретности комбинированный метод позволил вдвое сократить количество обменов информацией между синхронизируемыми искуственными нейронными сетями при увеличении объема отложенного перебора на несколько порядков [3, 8, 9, 10].

6. Для обеспечения криптостойкости сформированного общего секрета, соизмеримой с криптостойкостью современных симметричных криптоалгоритмов против полного перебора всех значений ключа, разработана модификация комбинированного метода [4, 12]. Суть модификации заключается в секретном независимом друг от друга изменении результата синхронизации искусственных нейронных сетей A и B путем инвертирования некоторого количества битов в бинарных последовательностях, полученных после первого этапа.

Рекомендации по практическому использованию результатов

Предложенный комбинированный метод с секретной модификацией результатов синхронизации для ФОС с помощью СИНС может использоваться как метод распределения ключевой информации абонентам сети без применения классических односторонних функций. Реализация данного метода может служить основой при разработке криптографических приложений.

Внедрение результатов диссертации подтверждено актом о практическом использовании результатов исследований и актом внедрения результатов исследования в учебный процесс.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

Статьи в научных рецензируемых изданиях из перечня, установленного ВАК

1. Голиков, В. Ф. Формирование общего секрета с помощью искусственных нейронных сетей / В. Ф. Голиков, М. Л. Радюкевич // Системный анализ и прикладная информатика. – 2019. – № 2. – С. 49–56.

2. Радюкевич, М. Л. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич, В. Ф. Голиков // Информатика. – 2020. − Т. 17, № 1. – С. 102–108.

3. Радюкевич, М. Л. Комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич, В. Ф. Голиков // Доклады Белорус. гос. ун-та информатики и радиоэлектроники. – 2021. – Т. 19, № 1. – С. 79–87.

4. Радюкевич, М. Л. Комбинированный метод формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей // Системный анализ и прикладная информатика. – 2021. – № 3. – С. 51–58.

Статьи в сборниках материалов научных конференций

5. Голиков, В. Ф. Выбор параметров и обоснование структуры синхронизируемых искусственных нейронных сетей в задаче формирования общего секрета [Электронный ресурс] / В. Ф. Голиков, М. Л. Радюкевич, А. П. Слепцов // Информационные технологии в образовании, науке и производстве : VI Междунар. науч.-техн. интернет-конф., 17–18 нояб. 2018 г. – Минск, 2018. – Режим доступа: https://rep.bntu.by/handle/data/50073. – Дата доступа: 12.03.2022.

6. Радюкевич, М. Л. Обоснование структуры и параметров синхронизируемых искусственных нейронных сетей в задаче формирования общего секрета / М. Л. Радюкевич, В. Ф. Голиков // Комплексная защита информации : материалы XXIV науч.-практ. конф., Витебск, 21–23 мая 2019 г. – Витебск, 2019. – С. 253–260.

7. Радюкевич, М. Л. Повышение конфиденциальности общего секрета, сформированного с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич, В. Ф. Голиков // Комплексная защита информации : материалы XXV науч.-практ. конф., Россия, 15–17 сент. 2020 г. – М., 2020. – С. 110–115.

8. Радюкевич, М. Л. Комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич, В. Ф. Голиков // Комплексная защита информации : материалы XXVI науч.-практ. конф., Минск, 25–27 мая 2021 г. – Минск, 2021. – С. 370–375.

9. Радюкевич, М. Л. Возможные уязвимости комбинированного метода формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич // 58-я науч. конф. аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (Минск, 18–22 апреля 2022 года) : материалы конф. по направлению 2: Информационные технологии и управление / [редкол.: Л. Ю. Шилин и др.]. – Минск, 2022. – С. 56–61.

10. Радюкевич, М. Л. Анализ стойкости комбинированного метода формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей / М. Л. Радюкевич // Комплексная защита информации : материалы XXVII науч.-практ. конф., Москва, 24–26 мая 2022 г. – М., 2022. – С. 122–128.

Тезисы докладов на научных конференциях

11. Радюкевич, М. Л. Программная модель для статистического моделирования результатов исследования синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич // Технические средства защиты информации : тез. докладов XX Белорус.-рос. науч.-техн. конф., Респ. Беларусь, Минск, 7 июня 2022 г. / [редкол.: Т. В. Борботько и др.]. – Минск, 2022. – С. 84–85.

12. Радюкевич, М. Л. Формирование криптографического ключа с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич // Технические средства защиты информации : тез. докладов XX Белорус.-рос. науч.-техн. конф., Респ. Беларусь, Минск, 7 июня 2022 г. / [редкол.: Т. В. Борботько и др.]. – Минск, 2022. – С. 85–86.

РЭЗЮМЭ

Радзюкевіч Марына Львоўна

Фарміраванне агульнага сакрэту з дапамогай сінхранізаваных штучных нейронавых сетак для крыптаграфічных прымяненняў

Ключавыя словы: бінарная паслядоўнасць, ключавая інфармацыя, крыптаграфічная абарона інфармацыі, фарміраванне агульнага сакрэту, сінхранізуемыя штучныя нейронавыя сеткі, крыптаграфічныя прымянення.

Мэта працы: Распрацоўка метадаў і алгарытмаў павышэння прыватнасці агульнага сакрэту для крыптаграфічных прымяненняў, які фарміруецца з выкарыстаннем сінхранізаваных штучных нейронавых сетак.

Метады даследавання: Даследаванні праведзены з выкарыстаннем сістэмнага аналізу, прыкладной крыптаграфіі, тэорыі інфармацыі, тэорыі верагоднасцяў, імітацыйнага мадэлявання.

Атрыманыя вынікі і іх навізна: Вырашана важная навукова-тэхнічная задача, якая звязана з павышэннем прыватнасці агульнага сакрэту для крыптаграфічных прымяненняў, які фарміруецца з выкарыстаннем сінхранізаваных штучных нейронавых сетак. Распрацаваны метады павышэння прыватнасці фарміравання агульнага сакрэту, якія забяспечваюць істотнае памяншэнне карэляцыі паміж вынікамі сінхранізацыі сетак аўтэнтыфікаваных абанентаў і атакавалай сеткай, шляхам прымянення або інтэграцыі вынікаў шматразова паўтараных сінхранізацый, або двухэтапнай працэдуры, якая ўключае няпоўную сінхранізацыю штучных нейронных сетак і паслядоўнасцяў па метадзе ўзгаднення слаба супадаючых бінарных паслядоўнасцяў на другім этапе. Гэтыя метады з'яўляюцца новымі. Іх устойлівасць да магчымых нападаў абгрунтавана тэарэтычнымі палажэннямі і пацверджана статыстычным мадэляваннем.

Рэкамендацыі па выкарыстанні і вобласць ужывання: Распрацаваныя метады фармавання агульнага сакрэту з дапамогай сінхранізаваных штучных нейронавых сетак падвышанай канфідэнцыйнасці могуць ужывацца для размеркавання ключавой інфармацыі абанентам сеткі без выкарыстання класічных аднабаковых функцый.

РЕЗЮМЕ

Радюкевич Марина Львовна

Формирование общего секрета с помощью синхронизируемых искусственных нейронных сетей для криптографических применений

Ключевые слова: бинарная последовательность, ключевая информация, криптографическая защита информации, формирование общего секрета, синхронизируемые искусственные нейронные сети, криптографические применения.

Цель работы: Разработка методов и алгоритмов повышения конфиденциальности общего секрета для криптографических применений, формируемого с использованием синхронизируемых искусственных нейронных сетей.

Методы исследования: Исследования проведены с использованием системного анализа, прикладной криптографии, теории информации, теории вероятностей, имитационного моделирования.

Полученные результаты и их новизна: Решена важная научно-техническая задача, которая связана с повышением конфиденциальности общего секрета для криптографических применений, формируемого с использованием синхронизируемых искусственных нейронных сетей. Разработаны методы повышения конфиденциальности формирования общего секрета, которые обеспечивают существенное уменьшение корреляции между результатами синхронизации сетей аутентифицированных абонентов и атакующей сетью, путем применения либо интеграции результатов многократно повторяемых синхронизаций, либо двухэтапной процедуры, включающей неполную синхронизацию искусственных нейронных сетей аутентифицированных абонентов на первом этапе и согласование этих последовательностей по методу согласования слабо совпадающих бинарных последовательностей на втором этапе. Данные методы являются новыми. Их стойкость к возможным атакам обоснована теоретическими положениями и подтверждена статистическим моделированием.

Рекомендации по использованию и область применения: Разработанные методы формирования общего секрета с помощью синхронизируемых искусственных нейронных сетей повышенной конфиденциальности могут применяться для распределения ключевой информации абонентам сети без использования классических односторонних функций.

SUMMARY

Radziukevich Maryna Lvovna

Generating a shared secret using synchronized artificial neural networks for cryptographic applications

Keywords: binary sequence, key information, cryptographic protection of information, formation of a shared secret, synchronized artificial neural networks, cryptographic applications.

Purpose of the work: Development of methods and algorithms for increasing the confidentiality of the general secret for cryptographic applications formed using synchronized artificial neural networks.

Research methods: The research was carried out using system analysis, applied cryptography, information theory, probability theory, simulation modeling.

The results obtained and their novelty: An important scientific and technical problem has been solved, which is associated with increasing the confidentiality of a shared secret for cryptographic applications, which is formed using synchronized artificial neural networks. Methods have been developed to increase the confidentiality of the formation of a shared secret, which provide a significant reduction in the correlation between the results of synchronization of networks of authenticated subscribers and the attacking network, by applying either the integration of the results of repeatedly repeated synchronizations, or a two-stage procedure that includes incomplete synchronization of artificial neural networks of authenticated subscribers at the first stage and the coordination of these sequences by the method of matching weakly matching binary sequences at the second stage. These methods are new. Their resistance to possible attacks is substantiated by theoretical provisions and confirmed by statistical modeling.

Recommendations for use and scope: The developed methods for generating a shared secret using synchronized artificial neural networks with increased confidentiality can be used to distribute key information to network subscribers without using classical one-way functions.

Научное издание

Радюкевич Марина Львовна

ФОРМИРОВАНИЕ ОБЩЕГО СЕКРЕТА С ПОМОЩЬЮ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ КРИПТОГРАФИЧЕСКИХ ПРИМЕНЕНИЙ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность

Подписано в печать 09.01.2023. Формат 60×84 1/16. Бумага офсетная. Гарнитура Таймс.
Опечатано на ризографе. Усл. печ. л. 1,63. Уч.-изд. л. 1,5. Тираж 60. Заказ 4.

Издатель и полиграфическое исполнение: учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя печатных изданий №1/238 от 24.03.2014,
«2/113 от 07.04.2014, №3/615 от 07.04.2014.
ул. П. Бровки, 6, 220013, Минск.