ОТЗЫВ

официального оппонента на диссертацию Радюкевич Марины Львовны
на тему «Формирование общего секрета с помощью синхронизируемых искусственных нейронных сетей для криптографических применений»
на соискание ученой степени кандидата технических наук
по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

1. Соответствие диссертации специальности и отрасли науки, по которым она представляется к защите

По уровню научной и практической значимости диссертационная работа соответствует требованиям ВАК Республики Беларусь, предъявляемым к диссертационным работам на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность по пунктам: «Методы и алгоритмы для анализа и синтеза криптографических, стеганонографических преобразований информации», «Разработка новых и повышение эффективности существующих технических и программных средств защиты информации», «Обеспечение безопасности информационных технологий, включая телекоммуникационные и информационные системы».

2. Актуальность темы диссертации

За последнее десятилетие наблюдается значительный рост киберугроз. С ростом числа интернет-подключенных устройств и развитием технологий угрозы кибербезопасности становятся все более серьезными и традиционные методы криптографии теряют свою эффективность. Поэтому возникает потребность в разработке новых и более криптостойких методов обеспечения безопасности данных. Исследования в области синхронизируемых искусственных нейронных сетей представляют инновационный подход к обеспечению безопасности данных. Разработка криптографических методов, основанных на синхронизируемых искусственных нейронных сетях, может привести к созданию новых практических решений для обеспечения безопасности данных в сети и приложениях.

В связи с вышеизложенным, тема диссертации Радюкевич М.Л., посвященная разработке структуры и параметров синхронизируемых искусственных нейронных сетей, позволяющих формировать секрет по открытым каналам связи с наиболее возможной криптостойкостью и выработка рекомендаций по повышению конфиденциальности и быстродействия формируемого общего секрета, является актуальной.

3. Степень новизны результатов, которые выносятся на защиту

В результате работы получены следующие новые результаты:

1) дана оценка потенциальной способности технологии синхронизируемых искусственных нейронных сетей (далее – СИНС) соответствовать требованиям практического применения в криптографии; обоснована структура и значения

параметров СИНС, позволяющих формировать общий секрет с максимально возможной конфиденциальностью, обмениваясь информацией по открытым каналам связи; предложены вероятностные характеристики для оценки секретности формируемой последовательности и корреляции с последовательностью атакующей сети.

2) предложен метод повышения конфиденциальности формируемого общего секрета, базирующийся на существенном уменьшение корреляции между результатами синхронизации легальных сетей и атакующей сетью за счет применения интеграции результатов многократно повторяемых синхронизаций;

3) предложен комбинированный метод формирования общего секрета с помощью двухэтапной процедуры, включающий неполную синхронизацию легальных ИНС на первом этапе, обеспечивающую заданную степень совпадения, формируемых случайных последовательностей, и на втором этапе согласование этих последовательностей по методу согласования слабо совпадающих бинарных последовательностей, обеспечивающий устойчивость к известным атакам и ускорение формирования общего секрета;

4) предложен комбинированный метод с секретной модификацией результатов синхронизации, заключающийся в секретном, независимом друг от друга изменении бинарных последовательностей ИНС А и В, сформированных после первого этапа метода, позволяющий при незначительном увеличении количества обменов информацией, обеспечить криптостойкость по отношению к атаке отложенным перебором, соизмеримую с криптостойкостью случайной бинарной последовательности размером более 256 битов.

4. Обоснованность и достоверность основных результатов и рекомендаций, сформулированных в диссертации

Основные выводы данной диссертации обоснованы и подтверждены достоверными данными. Соискатель подробно рассмотрел и проанализировал текущее состояние технологии СИНС, а также тщательно проработал теоретический фундамент и успешно продемонстрировал, что метод формирования общего секрета на основе СИНС может быть эффективным с точки зрения безопасности и скорости.

Анализ математических моделей проведен последовательно, результаты логически обоснованы. Обоснованность и достоверность результатов проведенных исследований подтверждена:

– имитационным моделированием с помощью специально разработанного программного обеспечения;

– практической реализацией метода формирования общего секрета в условиях компрометации подходов, базирующихся на применении классических односторонних функций, разрабатываемого государственным предприятием «НИИ ТЗИ».

Общие результаты диссертации вытекают из поставленных исследовательских задач, и их новизна и эффективность подкрепляются представленными расчетами и экспериментами. Такой методологический подход

свидетельствует о высоком научном уровне и отличной методической подготовке соискателя.

5. Научная, практическая и экономическая значимость результатов и основных положений диссертации

Научная значимость результатов и основных положений заключается в дальнейшем развитии технологии открытого формирования ключевой информации с помощью СИНС, устойчивой к совокупности возможных атак, использующих синхронизацию собственных сетей с атакуемой сетью. Применение в качестве итоговой бинарной последовательности обобщенный результат многократно повторенных синхронизаций с помощью одной сети или с помощью нескольких сетей экспоненциально уменьшает возможности атакующих сетей. Использование при этом двухэтапной процедуры формирования общего секрета делает технологию конкурентной по безопасности с известными.

Практическая значимость заключается в разработке алгоритмов формирования ключевой информации на основе СИНС, отличающихся простотой реализации, не требующих большого объема предварительных вычислений.

6. Полнота опубликования основных результатов диссертации

Изложенные в диссертационной работе материалы, основные научные положения и выводы опубликованы в 12 печатных работах. В том числе 4 статьи в научных журналах, 8 статей и тезисов докладов в сборниках материалов конференций. Уровень изданий, в которых опубликованы результаты, соответствует требованиям ВАК Республики Беларусь.

В качестве наиболее значимых публикаций можно выделить:

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.

5. 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.

7. Оценка оформления диссертации

Изложение диссертации соответствует требованиям ВАК Республики Беларусь. Материал изложен последовательно, с использованием общепринятых терминов и определений. К недостаткам оформления можно отнести обилие обозначений физических величин с различными подстрочными индексами, затрудняющих восприятие материала, а также одновременное использование англоязычных и русскоязычных аббревиатур известных технологий.

8. Соответствие научной квалификации соискателя ученой степени, на которую он претендует

По уровню выполнения диссертационной работы и важности полученных результатов квалификация соискателя соответствует присуждения ученой степени кандидата технических наук.

9. Недостатки диссертации

В качестве недостатков диссертационной работы можно отметить:

1. Использование метода формирования общего секрета предполагает проверку его идентичности между абонентами с помощью хэш-функции, которая является однонаправленной функцией. Поэтому не совсем корректно считать, что данные методы не используют такие функции.

2. Безопасность метода формирования общего секрета с использованием синхронизируемых искусственных нейронных сетей ограничена исключительно ИНС TPM-архитектуры (TreeParityMachine) и параметрами традиционных нейронных сетей.

3. Для бинарных последовательностей можно использовать различные функции и операции, аналогичные свертке, в зависимости от конкретных задач и целей. Однако в работе другие функции не представлены.

10. Заключение

Диссертационная работа Радюкевич Марины Львовны написана на актуальную тему, выполнена на высоком научном уровне, представляет научный и практический интерес и свидетельствует о высокой научной квалификации автора.

Научные положения и выводы, изложенные в работе, аргументированы теоретически и подтверждены практикой.

Основные положения и выводы, изложенные в диссертации, оригинальны и являются результатом научно-исследовательской работы, проведенной автором под руководством руководителя – доктора технических наук, профессора Голикова В.Ф.

Содержание автореферата соответствует положениям и выводам, изложенным в диссертации.

Представленная диссертация на соискание ученой степени кандидата технических наук удовлетворяет требованиям п. 20 Положения ВАК Беларуси, поскольку содержит новые научно обоснованные результаты, использование которых обеспечивает решение важной практической задачи – формирование

общего секрета с помощью синхронизируемых искусственных нейронных сетей для криптографических приложений и соответствует специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Степень кандидата наук может быть присуждена Радюкевич М.Л. за обоснование структуры и значений параметров ИНС, позволяющих формировать общий секрет с максимально возможной конфиденциальностью; разработку метода повышения конфиденциальности формируемого общего секрета, базирующийся на существенном уменьшение корреляции между результатами синхронизации легальных сетей и атакующей сетью; разработку комбинированного метода формирования общего секрета с помощью двухэтапной процедуры, включающий неполную синхронизацию легальных ИНС на первом этапе, обеспечивающую заданную степень совпадения, формируемых случайных последовательностей, и на втором этапе согласование этих последовательностей по методу согласования слабо совпадающих бинарных последовательностей; разработку комбинированного метода с секретной модификацией результатов синхронизации, заключающейся в секретном, независимом друг от друга изменении бинарных последовательностей ИНС А и В, сформированных после первого этапа метода.

Официальный оппонент
заведующий кафедрой
телекоммуникационных систем
УО Белорусская государственная
академия связи,
кандидат технических наук, доцент С.И. Половеня
27.09.2023г.

Подпись С.И. Половени удостоверяю:
Начальник отдела кадров П.Н. Литвиненко

Совет по защите диссертаций при БГУИР
«28» сентября 2023 г.
Вх. № 05.02-11/164