ОТЗЫВ

научного руководителя на диссертационную работу
Радюкевич Марины Львовны

«Методы формирования общего секрета с помощью синхронизируемых искусственных нейронных сетей для криптографических применений», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Диссертационная работа Радюкевич М.Л. посвящена повышению безопасности и быстродействия метода формирования общего секретного числа с помощью синхронизируемых искусственных нейронных сетей у абонентов криптографической системы, использующих открытый канал связи. Сформированные таким образом бинарные последовательности могут затем быть использованы в качестве криптографических ключей или иной общей для абонентов секретной информации. Подобная задача в настоящее время на практике решается с использованием протоколов асимметричной криптографии, в то же время ведется поиск альтернативных решений, так как все возрастающие вычислительные мощности современных компьютеров, перспектива создания квантовых компьютеров, а также разработка математических методов решения обратных задач, представляют потенциальную угрозу асимметричной криптографии.

Одним из таких альтернативных решений является технология Synchronization of Neural Networks, использующая синхронизируемые искусственные нейронные сети.

Актуальность данной тематики обусловлена недостаточностью уровня конфиденциальности формируемого секрета и значительного количества тактов обмена информацией для достижения синхронизма, что не позволяет рассматриваемой технологии найти практическое применение.

Для достижения поставленной цели диссертант в рамках типовой технологи Synchronization of Neural Networks, содержащей однослойную ИНС проанализировала ее возможности и сформировала базовый набор параметров ИНС, обеспечивающий некоторый уровень конфиденциальности формируемого секрета при приемлемом числе тактов обмена информацией. Разработала методы повышения конфиденциальности формируемого общего секрета по отношению к наиболее опасным атакам со стороны злоумышленника. Предложенные методы позволяют снизить вероятность взлома сформированной секретной последовательности до вероятности взлома бинарной последовательности длиной несколько сотен битов полным перебором. Основным методом проведения расчетов использовалось статистическое моделирование с помощью специально разработанной программной модели синхронизируемых искусственных нейронных сетей,

что по сути является экспериментальным подтверждением достоверности полученных результатов.

Научная значимость полученных результатов заключается в разработке методов формирования общего секрета высокой конфиденциальности с помощью синхронизируемых искусственных нейронных сетей за счет снижения уровня корреляции между результирующими числами, сформированными сетями аутентифицируемых абонентов и атакующей сетью за счет интеграции результатов многократно повторяемых синхронизаций, а также применения комбинированного метода с помощью двухэтапной процедуры, включающей неполную синхронизацию ИНС на первом этапе, и устранении несовпадений на втором этапе.

Практическая значимость заключается в возможности решения задачи распределения ключевой информации в криптографических системах в условиях дискредитации классических математических односторонних функций.

Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» в период с 2019 по 2022 г. В процессе работы над диссертацией Радюкевич М.Л. проявила себя как высококвалифицированный и грамотный специалист, умеющий самостоятельно решать научные задачи и анализировать полученные результаты. Основные результаты работы опубликованы в 12 научных трудах и апробированы на научно-технических конференциях различного уровня. Предложенный метод формирования ключевых последовательностей использовался в опытно-конструкторской работе шифр «Невод», выполняемой в рамках государственной научно-технической программы «Кибербезопасность» на 2021 – 2025 годы и внедрен в учебный процесс БГУИР в качестве материалов для проведения лекционных и лабораторных занятий по дисциплине «Криптографическая защита информации».

Учитывая изложенное, считаю, что диссертационная работа «Методы формирования общего секрета с помощью синхронизируемых искусственных нейронных сетей для криптографических применений», по уровню проведенных исследований и полученных результатов, их научной новизны и практической значимости отвечает требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность». Ее автор, Радюкевич М.Л., заслуживает присуждения ученой степени кандидата технических наук за получение новых научно обоснованных результатов, включающих:

- обоснование структуры и значений параметров ИНС, позволяющих в рамках известной технологии Synchronization of Neural Networks формировать общий секрет с максимально возможной конфиденциальностью, обмениваясь информацией по открытым каналам связи при ограниченном количестве тактов синхронизации;

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

- комбинированный метод формирования общего секрета с помощью двухэтапной процедуры, включающий неполную синхронизацию 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, повышающий криптостойкость к известным атакам на несколько порядков и ускорение формирования общего секрета в два раза;

- комбинированный метод с секретной модификацией результатов синхронизации, заключающейся в секретном, независимом друг от друга изменении бинарных последовательностей ИНС *A* и *B*, сформированных после первого этапа метода, позволяющей при незначительном увеличении количества обменов информацией, обеспечить криптостойкость по отношению к атаке отложенного перебора, соизмеримую с криптостойкостью случайной бинарной последовательности размером более 256 битов.

Научный руководитель
д.т.н., профессор,
пенсионер
31.08.2023

В.Ф. Голиков