

О Т З Ы В

на автореферат диссертации Радюкевич Марины Львовны
«Формирование 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

В настоящее время научное сообщество уделяет особое внимание разработке альтернативных методов криптографических преобразований. В диссертационной работе решается задача более углубленного изучения технологии формирования общего секретного числа с помощью синхронизируемых искусственных нейронных сетей (СИНС), известной под названием Synchronization of Neural Networks, оценке ее криптостойкости и разработке методов повышения конфиденциальности и быстродействия формируемого общего секрета по отношению к классической СИНС.

Научная новизна исследования состоит в решении важной научно-технической задачи, связанной с повышением конфиденциальности и быстродействия формирования общего секрета для криптографических применений, с использованием СИНС.

В автореферате соискателя определены цель работы и основные задачи исследования, показана актуальность темы, сформулированы положения, выносимые на защиту и рекомендации по практическому использованию результатов, отмечен личный вклад соискателя.

Из автореферата видно, что диссертационные исследования прошли апробацию на научных семинарах и конференциях путем публикации ее результатов в научных журналах, что подтверждает обоснованность и достоверность сформулированных в автореферате полученных результатов.

В качестве замечания следует указать следующее:

1. Метод совместного использования некоторого количества проведенных синхронизаций искусственных нейронных сетей А и В для повышения безопасности формируемого секрета проанализирован для случая побитового сложения соответствующих битов полученных бинарных последовательностей, однако возможны и другие алгоритмы сжатия, возможно более эффективные.

Данное замечание не снижает теоретической и практической ценности полученных в работе автора результатов. Радюкевич М.Л. заслуживает присвоения ученой степени кандидата технических наук по заявляемой специальности.

Первый проректор
учреждения образования
«Полоцкий государственный
университет имени Евфросинии Полоцкой»,
кандидат физико-математических наук, доцент

22 сентября 2023г.



О.В.Голубева

Я, Голубева Оксана Валерьевна, даю согласие на обработку моих персональных данных, связанную с защитой диссертации и оформлением аттестационного дела М.Л.Радюкевич.

Голубева Оксана Валерьевна

Подпись Голубева О.В.
Специалист по кадрам



Весько