ОТЗЫВ

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 представленной на защиту работе ставится задача в более углубленном изучении 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 (ФОС) по отношению к классической технологии СИНС.

Научная новизна исследования состоит в разработке методов 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 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.

В автореферате соискателя определены цель работы и основные задачи исследования, показана актуальность темы, сформулированы положения, выносимые на защиту, даны рекомендации по практическому использованию результатов, а также отмечен личный вклад соискателя. Из автореферата видно, что результаты диссертационных исследований прошли апробацию на научных семинарах и конференциях, результаты исследований опубликованы в научных журналах, что дает возможность подтвердить достоверность и обоснованность результатов.

Замечание следующее. Из автореферата не видно обоснования использования в качестве процедуры сжатия побитового сложения по

модулю 2 всех битов множества. Возможно использование других процедур было бы более эффективным.

Однако данное замечание не влияет на качество и значимость диссертационного исследования. Радюкевич Марина Львовна заслуживает присвоения ученой степени кандидата технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность.

Директор
Общества с дополнительной
ответственностью «ВИРУСБЛОКАДА»
кандидат технических наук Г.К. Резников

25 сентября 2023 г.

Я, Резников Геннадий Константинович, даю согласие на обработку моих персональных данных, связанную с защитой диссертации и оформлением аттестационного дела М.Л.Радюкевич.

Резников Геннадий Константинович

Подпись Резникова Г.К. удостоверяю

Специалист по кадрам О.А. Кожич