ЗАКЛЮЧЕНИЕ

совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по диссертации Радюкевич Марины Львовны «Формирование общего секрета с помощью синхронизируемых искусственных нейронных сетей для криптографических применений», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность

Соответствие диссертации специальности и отрасли науки, по которым присуждается ученая степень. Диссертация Радюкевич М.Л. является самостоятельной законченной научно-исследовательской работой и 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.

Научный вклад соискателя в решение научной задачи с оценкой его значимости.

Научный вклад соискателя в решение научной задачи состоит в разработке методов, позволяющих повысить криптостойкость и быстродействие формирования общего секретного ключа с помощью синхронизируемых искусственных нейронных сетей. Значимость научного вклада соискателя состоит в том, что в разработанных им методах по сравнению с их аналогами не используются классические однонаправленные математические функции, что делает возможным применение этих методов на современном этапе развития криптографии.

Конкретные научные результаты, за которые соискателю может быть присуждена ученая степень. Соискатель заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность за новые научно-обоснованные теоретические и экспериментальные результаты, включающие:

- метод повышения конфиденциальности формируемого общего секрета, отличающийся от аналогов тем, что включает в себя процедуру интеграции результатов многократно повторяемых синхронизаций, и позволяющий за счет этого уменьшить корреляцию между результатами синхронизации легальных сетей с атакующей сетью;
- метод формирования общего секрета с помощью двухэтапной процедуры, отличающийся от аналогов тем, что на его первом этапе реализуется неполная синхронизация легальных искусственных нейронных сетей аутентифицируемых абонентов, обеспечивающая заданную степень совпадения формируемых псевдослучайных последовательностей, а на втором этапе – согласование этих последовательностей с помощью метода согласования слабо совпадающих бинарных последовательностей, что позволяет повысить на 5 порядков криптостойкость ключей шифрования к известным атакам (при выбранном количестве сеансов синхронизации $r = 5$) и ускорить в 2,0 раза процесс формирования общего секрета;
- метод модификации результатов синхронизации искусственных нейронных сетей, отличающийся от аналогов тем, что включает в себя процедуру изменения бинарных последовательностей, сформированных с помощью таких сетей, и позволяющий за счет этого получить ключ шифрования, криптостойкость которого по отношению к атаке отложенным перебором соизмерима с криптостойкостью псевдослучайной бинарной последовательности размером не менее 256 битов по отношению к атаке методом полного перебора,

что в совокупности является вкладом в развитие актуального направления научных исследований – методы формирования общего секрета в криптографических системах.

Рекомендации по использованию результатов исследования. Разработанные методы могут использоваться для формирования секретных ключей шифрования. Простота реализации и высокая криптостойкость разработанных методов к известным атакам, в том числе и к атакам на ассиметричные алгоритмы, делают их применение актуальным и обоснованным. Разработанное программное средство для статистического моделирования технологии Synchronization of Neural Networks для обоснования базовых структуры и значений параметров искусственных нейронных сетей может быть использовано для моделирования разработанных методов формирования общего секрета и оценки их эффективности.

Председатель совета по защите диссертаций Т. В. Борботько

Ученый секретарь совета по защите диссертаций О. В. Бойправ