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

Вопросы обеспечения информационной безопасности в связи с обострением международной обстановки, введением санкций и ограничений в отношении Союзного государства, выдвигаются на первый план при обеспечении конфиденциальности, целостности и доступности передаваемой информации между ответственными абонентами. В связи с этим диссертационная работа Радюкевич М.Л. посвященная разработке методов и алгоритмов повышения конфиденциальности общего секрета для криптографических применений, формируемого с использованием синхронизированных искусственных нейронных сетей (СИНС), является актуальной.

К наиболее значимым научным результатам можно отнести:

1. Обоснование структуры и значений параметров СИНС. Позволяющих формировать общий секрет с наиболее высокой конфиденциальностью при обмене информацией по открытым каналам связи.
2. Комбинированный метод формирования общего секрета по двухэтапной процедуре, повышающей криптостойкость к известным атакам на несколько порядков.

Адекватность разработанных методов и алгоритмов обоснована теоретическими положениями и подтверждена статистическим моделированием и практическим использованием результатов исследований.

По содержанию автореферата можно сделать следующие замечания:

1. Из автореферата не вполне ясно обоснование выбора оптимального значения количества тактов синхронизации d между сетями.
2. Предлагаемые методы формирования общего секрета абонентами, использующими открытый канал связи, требуют предварительной их аутенфикации как это учитывается при ФОС.

В целом, судя по автореферату, диссертационная работа «Формирование общего секрета с помощью синхронизируемых искусственных нейронных сетей для криптографических применений» является законченным научным исследованием, а ее автор Радюкевич М.Л. заслуживает присуждения ей ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Научный руководитель – заведующий НИЛ
«Безопасность и электромагнитная
совместимость технических средств»,
профессор кафедры «Автоматика,
телемеханика и связь» УО «Белорусский
государственный университет транспорта»
доктор технических наук, профессор К.А. Бочков

«3» октября 2023г.

Я, Бочков Константин Афанасьевич, даю согласие на обработку моих персональных данных, связанную с защитой диссертации и оформлением аттестационного дела М.Л. Радюкевич.

Бочков Константин Афанасьевич

Личную подпись Бочкова К.А.
удостоверяю
Начальник ОК С.И. Паранин