О Т З Ы В

на автореферат диссертационной работы
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

Диссертационная работа М.Л. Радюкевич посвящена разработке нового механизма, который может быть использованы для решения важной криптографической задачи – формирования общего ключа (секрета).

Данная задача имеет важное прикладное значение, так как протоколы формирования общего ключа получили повсеместное распространение и используются при необходимости организовать защищенное соединение, которое будет обеспечивать конфиденциальности, целостность и подлинность информации, передаваемой по открытому каналу связи.

В последнее время устоявшиеся в этой области криптографические протоколы находятся под угрозой т.к. основаны на вычислительной сложности решения задач дискретного логарифмирования и факторизации, которые обладают низкой стойкостью при организации атаки с использованием квантового компьютера. Поэтому во всем мире ведутся исследовательские работы, направленные на поиск достойных аналогов известным протоколам формирования общего ключа, которые бы обладали защитой от атак с применением квантовых вычислений.

Автором работы предлагается использование технологии формирования общего секрета с использованием синхронизируемых искусственных нейронных сетей. В работе рассматривается уже существующая технология и проводится оценка ее криптографической стойкости, в результате которой делается вывод о наличии серьезных недостатков, затрудняющих ее использование в прикладных целях. Автором работы предлагается ряд методов, позволяющим улучшить базовую технологию: метод повышения конфиденциальности формирования общего секрета, комбинированный метод формирования общего секрета с помощью двухэтапной процедуры и комбинированный метод с секретной модификацией результатов синхронизации. Каждый из методов обосновывается теоретическими выкладками и практическим моделированием.

Вместе с тем, по содержанию автореферата имеются следующие замечания:

– не изложена необходимость перехода на несимметричный интервал возможных значений весовых коэффициентов;

– не представлена последовательность шагов при комбинированном методе с секретной модификацией результатов синхронизации.

Отмеченные замечания принципиально не влияют на полученные в работе результаты и могут быть рекомендованы для дальнейших исследований автора.

В целом, автореферат диссертации дает достаточно полное представление о проделанной работе и полученных результатах. Основные научные результаты диссертации были обсуждены на международных и республиканских конференциях, опубликованы в рецензируемых научных изданиях. Отмеченные замечания не влияют на общую положительную оценку работы.

На основании автореферата и списка публикаций автора, считаю, что диссертационная работа выполнена на высоком научном уровне, по содержанию и новизне полученных результатов соответствует требованиям Высшей аттестационной комиссии Республики Беларусь, предъявляемым к кандидатским диссертациям, а соискатель Радюкевич Марина Львовна заслуживает присвоения ученой степени кандидата технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность.

Заместитель генерального директора
по научной работе государственного
научного учреждения «Объединенный
института проблем информатики
Национальной академии наук Беларусь»,
кандидат технических наук, доцент С.Н.Касанин

26 сентября 2023 г.

Я, Касанин Сергей Николаевич, даю согласие на обработку моих персональных данных, связанную с защитой диссертации и оформлением аттестационного дела М.Л. Радюкевич.

С.Н.Касанин

Личную подпись Касанина Сергея Николаевича заверяю.
Начальник отдела кадровой и правовой работы

Отдел кадровой и правовой работы

Г.И. Степанцов

сентября 2023 г.

Ознакомлена 27.09.23 /Радюкевич М.Л./

Совет по защите диссертаций при БГУИР
«27» сентября 2023 г.
Вх. № 05.02-11/163