ОТЗЫВ

на диссертационную работу докторанта PhD Усатовой Ольги Александровны на тему: «Разработка и исследование алгоритма аутентификации пользователей информационно-коммуникационных систем», представленной на соискание степени доктора философии (PhD) по специальности «6D100200 – Системы информационной безопасности».

1. Актуальность темы исследования и ее связи с общенаучными и общегосударственными программами

Актуальность темы исследования обуславливается динамично развивающимся направлением цифровых услуг. Перед обществом остро стоит вопрос обеспечения надежности и защищенности персональных данных, а также разработка отечественных программных продуктов в области обеспечения безопасности.

Диссертационная работа Усатовой О.А. выполнена в соответствии с приоритетными программами развития науки Республики Казахстан, в частности работа выполнена в рамках проекта программно–целевого финансирования «Разработка программных и программно–аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» (2018-2019гг.) и грантового финансирования научных исследований по теме: «Разработка казахстанского сегмента защищенного трансграничного информационного взаимодействия» (2020г.).

2. Научные результаты и их обоснованность.

Целью диссертационной работы Усатовой О.А. является исследование и реализация алгоритма аутентификации двухфакторной для обеспечения защиты информации в информационно-коммуникационных системах.

Докторантом получены следующие результаты:

1) Разработан алгоритм аутентификации пользователя на основе второго фактора, основанный на генерации тригонометрических функций путем усложнения масштабирования функций при вычислении одноразового пароля, являющегося вторым фактором. Масштабирование выполняется матричным представлением вариантов тригонометрических функций и использованием хеш-функций для вычисления координат и параметров генерируемой тригонометрической функции по текущему времени, секретной строке, логину и паролю первого аутентификационного кода.

2) Разработана модель процесса аутентификации пользователя на основе второго фактора, отличающаяся от известных тем, что она открытая и может генерировать наборы функций получения второго аутентификационного кода для каждой отдельной системы.

3) Предложена схема информационной системы программной реализации двухфакторной аутентификации с использованием мобильного устройства.

3. Степень обоснованности и достоверности каждого научного результата (научного положения), выводов и заключения соискателя, сформулированных в диссертации.

Результаты исследования автора являлись основой при разработке информационной системы ТОО «Digital Media Center», которые позволили повысить уровень защиты электронной информации и надежность функционирования системы. Автором получено авторское свидетельство на программное обеспечение «Система аутентификации с использованием второго фактора для контроля доступа к данным – Security Code of the 2FA».

В целом представленные результаты и выводы достоверны, подтверждены теоретическими разработками, вычислительными экспериментами и в основном, отражают новизну диссертации, сформулированную автором.

Основные результаты диссертационной работы докладывались и обсуждались на семинарах кафедры Казахского национального университета имени аль-Фараби, Института информационных и вычислительных технологий КН МОН РК и Международных научно-практических конференциях.

4. Степень новизны каждого научного результата (положения), вывода соискателя, сформулированных в диссертации.

Автором получены следующие результаты:

– разработан алгоритм генерации тригонометрических функций путем усложнения масштабирования функций;

– предложена архитектура информационной системы двухфакторной аутентификации;

- реализовано клиент-серверное приложение для двухфакторной аутентификации при защите информации в информационно-коммуникационных системах.

Вынесенные на защиту научные положения аргументированы и обоснованы.

5. Оценка внутреннего единства полученных результатов.

Диссертационная работа состоит из введения, трех разделов, заключения, списка использованной литературы и приложений. Все разделы работы, в том числе и полученные соискателем результаты, характеризуются внутренним единством и взаимосвязанностью по исследуемым вопросам.

6. Соблюдение в диссертации принципа самостоятельности

Диссертационная работа соискателя является самостоятельным и имеющим научную и практическую значимость исследованием. Основные результаты, полученные автором работы, докладывались на международных

конференциях, опубликованы в научных журналах, в том числе: 5 - в научных изданиях, рекомендуемых КОКСОН МОН РК, 2 - в международных научных изданиях, входящих в базу данных Scopus, 8 - в материалах международных научно-практических конференций.

7. Замечания, предложения по диссертации

Положительно оценивая диссертацию в целом, отметим в ней отдельные спорные положения и замечания:

1) проведен узкий анализ существующих отечественных и зарубежных решений в области аутентификации;

2) в разработанной системе двухфакторной аутентификации первый фактор является постоянным и хранимым в системе, что снижает стойкость системы аутентификации;

3) основной новизной является алгоритм формирования второго фактора, то есть одноразового пароля, состоящего из шести цифр, что не отвечает требованиям, предъявляемым к паролям в Республике Казахстан;

4) в диссертации по тексту и в списке литературы имеются редакторские и корректорские замечания.

Указанные замечания не снижают общую положительную оценку работы, выполненной диссертантом, и могут служить ориентиром при постановке задач в рамках дальнейшего исследования данной актуальной темы.

8. Соответствие содержания диссертации в рамках требований Правил присуждения ученых степеней

На основании вышеизложенного считаю, что диссертационная работа Усатовой О.А. на тему «Разработка и исследование алгоритма аутентификации пользователей информационно-коммуникационных систем», представленная на соискание степени доктора философии (PhD) по специальности «6D100200 – Системы информационной безопасности» соответствует требованиям «Правил присуждения ученых степеней» КОКСОН МОН РК, предъявляемым к работам такого рода, как по содержанию, так и по объему, а соискатель Усатова О.А. заслуживает присуждения степени доктора философии (PhD) по специальности «6D100200 – Системы информационной безопасности».

Официальный рецензент:
PhD, ассоциированный профессор,
директор института
информационных технологий
Алматинского университета энергетики
и связи имени Гумарбека Даукеева

Картбаев Т.С.