

## **ОТЗЫВ**

**научного консультанта на диссертационную работу Усатовой Ольги Александровны «Разработка и исследование алгоритма аутентификации пользователей информационно-коммуникационных систем», представленную на соискание ученой степени доктора философии по специальности «6D100200 – Системы информационной безопасности»**

Диссертационная работа Усатовой О.А. посвящена разработке и исследованию алгоритма аутентификации, позволяющего обеспечить целостность электронных документов при хранении и обмене в информационно-коммуникационных системах, на основе второго фактора (2FA). Проведен обзор и анализ существующих систем защиты информации в базах данных, исследованы алгоритмы многофакторной аутентификации, разработан алгоритм двухфакторной аутентификации, а также создана информационная система с целью обеспечения целостности и защиты информационно-коммуникационных систем.

В первом разделе описаны известные методы и средства защиты информационных систем на основе двухфакторной аутентификации, а также принципы построения защиты информации в базе данных при аутентификации пользователя. Классифицированы известные методы двухфакторной аутентификации, используемые в информационных системах, рассмотрены алгоритмы и протоколы аутентификации с использованием одноразового пароля. Проведен анализ некоторых кибератак, рассмотрены ряд компаний, предоставляющих услуги по защите информации хранящихся в базах данных. Рассмотрены также проблемы, которые возникают при использовании готовых решений аутентификаторов.

Во втором разделе представлены результаты, полученные при разработке модели защиты информационной системы при идентификации пользователя на основе двухфакторной аутентификации. Описан разработанный алгоритм генерации одноразового пароля с использованием программы аутентификатора и мобильного приложения, для аутентификации пользователя на основе второго фактора. Предложенная модель, основанная на использовании комбинации двух факторов: постоянного и временного паролей.

Третий раздел посвящен результатам, полученным при построении программной реализации предложенного алгоритма двухфакторной аутентификации. Разработана информационная система, состоящая из 3 взаимодействующих модулей: пользователя, мобильного приложения и серверной части. Описана работа СУБД MongoDB, в которой хранятся и обрабатываются данные. Поэтапно изложена структура работы приложения. Рассмотрены созданные генераторы случайных секретных слов и тригонометрических функций для формирования одноразового пароля двухфакторной аутентификации. Программно реализована информационная система защиты информации при

аутентификации пользователя на основе одноразового пароля и проведено исследование корректности выполнения предложенного алгоритма.

Практическая значимость результатов диссертации: полученные результаты вносят вклад в развитие и создание системы обеспечения информационной безопасности в Казахстане. Полученные результаты являются новыми и выполнялись в соответствии с календарными планами проекта программно-целевого финансирования КН МОН РК «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» (отчет за 2018-2019 г.); научный руководитель проекта - д.т.н., ассоц. профессор Нысанбаева С.Е., грантового финансирования КН МОН РК «Разработка казахстанского сегмента защищенного трансграничного информационного взаимодействия» (отчет за 2020 г.), научный руководитель проекта - д.т.н., профессор, Бияшев Р.Г.

Основные результаты диссертации также представлены в 15 казахстанских и зарубежных публикациях. Получены 2 авторских свидетельства:

- Сертификат регистрации авторского права на алгоритм «Двухфакторная аутентификация в автоматизированной системе управления» №712144534 от 2018.10.01, компании «WORKS COPYRIGHT», это цифровая сертификация, юридически признанная во всем мире для регистрации авторских прав авторов, NewYork – NY-USA;

- Авторское свидетельство о внесении сведений в государственный реестр прав на объекты, охраняемые авторским правом РК, № 4330 от 28 июня 2019г., «Система аутентификации с использованием второго фактора для контроля -к данным –Security Code of the 2FA».

Результаты исследований доложены на специализированных и международных конференциях и семинарах в Казахстане и за рубежом (Польше и Китае). Усатову О.А. характеризует ответственность, самостоятельность и инициативность при выполнении научных исследований по теме диссертационной работы, стремление к познанию нового и достижению поставленной цели.

Считаю, что представленная диссертация Усатовой О.А. отвечает всем требованиям, предъявляемым к докторским диссертациям (PhD) и рекомендуется к защите на соискание ученой степени PhD доктора по специальности «6D100200 - Системы информационной безопасности».

**ГНС Лаборатории информационной  
безопасности Института информационных  
и вычислительных технологий КН МОН РК,  
д.т.н., ассоциированный профессор**

 С.Е.Нысанбаева