"Халықаралық ақпараттық технологиялар университеті" АҚ

АО "Международный университет информационных технологий"

JSC "International Information Technology University"

22.09.2020 № 111

Алматы қ. г.Алматы

ОТЗЫВ

официального рецензента на диссертационную работу PhD докторанта 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 связь с общенаучными и общегосударственными программами

Разработка отечественных программных продуктов для защиты информационно-коммуникационных систем является необходимой и важной для нашей республики, так как многие организации сталкиваются с ежедневными атаками на компьютерные системы, в которых хранится и обрабатывается информация.

Диссертационная работа Усатовой О.А. посвящена актуальной проблеме – разработке алгоритма аутентификации пользователя в информационно-коммуникационной системе, так как любая информационная система требует дополнительной защиты для безопасного электронного документооборота.

2. Научные результаты в рамках требований к диссертациям и их обоснованность.

Научные результаты Усатовой О.А. по теме диссертации получены на основе корректной постановки задач исследования и их последовательным решениям. В диссертации приведены следующие полученные результаты:

- Разработана модель процесса двухфакторной аутентификации пользователя с использованием второго фактора. Отличие этой модели от известных состоит в том, что она является открытой и способна генерировать наборы функций получения второго аутентификационного кода для каждой отдельной системы.

- Создан алгоритм двухфакторной аутентификации пользователя с применением генерации тригонометрических функций путем усложнения масштабирования функций при вычислении второго фактора, которым в диссертации является одноразовый пароль. 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.

- Разработана структура информационной системы, для программной реализации алгоритма двухфакторной аутентификации с применением в ней смартфона.

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

Каждый результат выполненной Усатовой О.А. работы получен путем обоснования, выбора и разработки соответствующего алгоритма и модели, сравнения с имеющимися в литературе экспериментальными и расчетными данными, с результатами других авторов. При этом наблюдалось весьма хорошее согласие, что и свидетельствует в пользу достоверности и обоснованности выводов, сформулированных в диссертации.

Результаты неоднократно докладывались на семинарах и международных научных конференциях. Большая часть из них опубликована в профильных научных изданиях с высоким рейтингом. Для решения поставленных в работе задач автором применен ряд продуктивных инструментов в области защиты информации. Решение каждой задачи опирается на полученные результаты предыдущих этапов исследования, что обусловливает их взаимосвязанность и взаимозависимость, а также внутреннее единство полученных результатов.

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

Результаты, полученные в диссертации Усатовой О.А., являются новыми и дополняют известные:

1) Предложенная модель процесса двухфакторной аутентификации пользователя на основе второго фактора отличается от известных тем, что она является открытой и может генерировать наборы функций получения второго аутентификационного кода для каждой отдельной системы.

2) Разработан алгоритм двухфакторной аутентификации пользователя, основанный на генерации тригонометрических функций путем усложнения масштабирования функций, выполняется матричным представлением вариантов тригонометрических функций и использованием хеш-функций для вычисления координат и параметров генерируемой тригонометрической функции по текущему времени, секретной строке и аккаунта пользователя.

3) Построена схема информационной системы алгоритма двухфакторной аутентификации с использованием мобильного устройства для ее внедрения и использования в закрытой сети.

4) Реализовано клиент-серверное приложение для алгоритма двухфакторной аутентификации для защиты информации в информационно-коммуникационных системах.

5. Практическая и теоретическая значимость научных результатов, направленной на решение актуальной проблемы, теоретической и прикладной задачи

Диссертационная работа Усатовой О.А. является квалифицированным трудом, содержащим научно обоснованные результаты, использование которых позволит решать задачи защиты данных хранящихся в информационных системах.

Полученные диссертантом научные результаты имеют как практическую, так и общетеоретическую значимость: использованы новые подходы к исследованию предметной области, позволившие ей получить новые результаты в области защиты и безопасности информационных систем при аутентификации пользователя. Реализованное клиент-серверное приложение имеет практическое значение и состоит в возможности его использования для защиты электронных данных в информационно-коммуникационных системах.

6. Соблюдение в диссертации принципа самостоятельности

Представленная диссертационная работа соискателя является самостоятельным и имеющим научную и практическую значимость исследованием. Результаты работы подтверждены актом внедрения и апробированы публикациями в журналах, рекомендуемых ККСОН, в международных журналах, входящих в базу Scopus, а также полученные результаты докладывались на международных конференциях. Опубликовано 15 научных работ, из них 5 - в научных изданиях рекомендуемых КН МОН РК, 2 - в международных научных изданиях, входящих в базу данных Scopus, 8 - в материалах международных научно-практических конференций.

7. Соответствие аннотации содержанию диссертации

Аннотация описывает каждый из 3 разделов и соответствует содержанию диссертационной работы.

8. Замечания, предложения по диссертации

Последовательность основных этапов выполнения и структура диссертации соответствуют логике научного исследования, полностью отвечает ее цели и задачам. При этом соблюдено внутреннее единство результатов диссертации. Положительно оценивая диссертацию в целом, отметим в ней отдельные спорные положения и замечания.

В диссертационной работе следовало бы рассмотреть варианты пароля более 8 символов, а также процесс авторизации в разработанном алгоритме, что в свою очередь усиливало бы практическую ценность разработки.

Однако, работа соответствует требованиям и указанные замечания не снижают актуальность и хорошее качество выполненных исследований и ее результатов.

9. Заключение о возможности присуждения соискателю степени доктора философии (PhD) по специальности «6D100200 – Системы информационной безопасности»

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 всем требованиям «Правил присуждения ученых степеней» ККСОН МОН РК, предъявляемым к работам такого рода, а соискатель Усатова О.А. заслуживает присуждения искомой степени доктора философии (PhD) по специальности «6D100200 – Системы информационной безопасности».

Официальный рецензент:
к.т.н, ассистент профессор,
Международный университет
информационных технологий Аманжолова С.Т.