

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет радиофизики и компьютерных технологий
Кафедра интеллектуальных систем

Аннотация к магистерской диссертации

**Обеспечение информационной безопасности облачных
вычислений с использованием гомоморфного шифрования**

специальность 1-31 80 07 «Радиофизика»

Кустов Иван Андреевич

Научный руководитель: профессор кафедры интеллектуальных систем,
Садов Василий Сергеевич, кандидат технических наук, доцент

Минск, 2021

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Магистерская диссертация: 62 страницы, 2 рисунка, 6 таблиц, 26 источников, 2 приложения.

ОБЛАЧНЫЕ ТЕХНОЛОГИИ, БЕЗОПАСНОСТЬ, ГОМОМОРФНОЕ ШИФРОВАНИЕ.

Объект исследования: Гомоморфное шифрование и его применение для обеспечения безопасности облачных технологий.

Цель работы: Изучение применимости гомоморфного шифрования в сфере облачных технологий.

Результат: Произведен сравнительный анализ алгоритмов шифрования, выбран алгоритм, предложено его улучшение, разработано приложение с его использованием.

Область применения: Облачные провайдеры.

АГУЛЬНАЯ ХАРАКТЕРЫСТЫКА РАБОТЫ

Магістарская дысертацыя: 62 старонкі, 2 малюнка, 6 табліц, 26 крыніц, 2 прыкладання.

ВОБЛАЧНЫЯ ТЭХНАЛОГІІ, БЯСПЕКА, ГАМАМОРФНАЕ ШЫФРАВАННЕ

Аб'ект даследавання: Гамаморфнае шифраванне і яго ўжыванне для забеспячэння бяспекі воблачных тэхналогій.

Мэта работы: Вывучэнне дастасавальнасці гамаморфнага шифравання ў сферы воблачных тэхналогій.

Вынік: Зроблены параўнальны аналіз алгарытмаў шифравання, абраны алгарытм, прапанавана яго паляпшэнне, распрацавана прыкладанне з яго выкарыстаннем.

Вобласць прымянення: Воблачныя правайдэры.

GENERAL CHARACTERISTIC OF WORK

Master's thesis: 62 pages, 2 figures, 6 tables, 26 sources, 2 applications.

CLOUD TECHNOLOGIES, SECURITY, HOMOMORPHIC ENCRYPTION.

Object of research: Homomorphic encryption and its application for cloud security.

Objective: Study of the applicability of homomorphic encryption in the field of cloud technologies.

The result: Carried out comparative analysis of encryption algorithms, an algorithm was selected, its improvement was proposed, an application with this algorithm was developed.

The scope: Cloud providers.