

**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
Факультет компьютерных наук
Департамент программной инженерии**

Отзыв научного руководителя на выпускную квалификационную работу

студента группы БПИ 151 образовательной программы 09.03.04 «Программная инженерия» Куприянова Кирилла Игоревича
на тему: «Криптографические алгоритмы и протоколы для распределенных реестров»

Выпускная квалификационная работа содержит: текст работы на 46 листах, 19 рисунков, 1 таблица, и список использованных источников из 39 наименований.

Процент плагиата из системы Антиплагиат (не может превышать 20 %) – 4.

Основной целью работы является прототипирование инструментальных средств создания технологии распределенного реестра за счет выбора алгоритмов хеширования и цифровой подписи и экспериментального оценивания полученной технологии.

Актуальность работы связана с гигантским числом (более 1000) вариантов технологий распределенного реестра.

Научная новизна работы: разработана новая актуальная классификация криптографических алгоритмов и протоколов для распределённых реестров, дополняющая существующую (но устаревшую) на сегодняшний день классификацию 2014-го года, за счет анализа новых технологий распределенного реестра. Обновлённая классификация отражает фактическое состояние криптографических алгоритмов и протоколов в распределённых реестрах на вторую четверть 2019 года.

Практическая значимость работы: созданы инструментальные средства для автоматизации процесса программирования распределённых реестров. Ядром прототипа инструментальных средств является созданная библиотека на языке Python3.6, в которой собраны реализации проанализированных алгоритмов и протоколов. Прототип инструментальных средств предоставляет генерацию кода технологий распределенного реестра на основе дружественного интерфейса командной строки. Приложение находится в публичном доступе и доступно к установке.

Из-за большого объема работы реализована генерация только технологий блокчейна. Открытость платформы позволяет в дальнейшем расширить реализацию другими технологиями распределенного реестра и алгоритмами защиты приватности.

Проведенные экспериментальные исследования прототипа позволяют принять решения при реализации программного продукта, путем имплементации протоколов и криптографических алгоритмов на языке СИ.

В процессе выполнения ВКР полностью сформированы следующие компетенции:
УК-3 – Способен решать проблемы в профессиональной деятельности на основе анализа и синтеза

УК-5 – Способен работать с информацией: находить, оценивать и использовать информацию из различных источников, необходимую для решения научных и профессиональных задач (в том числе на основе системного подхода)

ПК-2 – Способен к формализации в своей предметной области с учетом ограничений используемых методов исследования

ПК-10 – Способен проектировать, конструировать и тестировать программные продукты

ПК-12 – Способен моделировать, анализировать и использовать формальные методы конструирования программного обеспечения

ПК-14 – Способен создавать программные интерфейсы

ПК-15 – Способен использовать операционные системы, сетевые технологии, средства разработки программного интерфейса, применять языки и методы формальных

спецификаций, системы управления базами данных

ПК-17 – Способен применять основные методы и инструменты разработки программного обеспечения

Работа соответствует названию, отлично структурирована и оформлена в соответствии с требованиями.

На основании вышеизложенного считаю, что работа заслуживает оценки “отлично” (10 из 10), а студент К. И. Куприянов присвоения квалификации бакалавра.

Научный руководитель
к.т.н., профессор ДПИ ФКН

22.05.2019



С.М. Авдошин