СВЕДЕНИЯ О НАИБОЛЕЕ ЗНАЧИМЫХ РЕЗУЛЬТАТАХ НАУЧНЫХ ИССЛЕДОВАНИЙ И РАЗРАБОТОК КАФЕДРЫ ПРИКЛАДНОЙ ИНФОРМАТИКИ УГЛТУ в 2019 г.

1. Наименование результата:

Метод перестановок линейных кодов криптосистемы одноранговой сети

2. Результат научных исследований и разработок (выбрать один из п. 2.1 или п. 2.2)

2.1. Результат фундаментальных научных исследований		2.2. Результат прикладных научных исследований и экспериментальных разработок	
- теория		- методика, алгоритм	
- метод	+	- технология	
- гипотеза		- устройство, установка, прибор, механизм	
- другое (расшифровать):		- вещество, материал, продукт	
		- штаммы микроорганизмов, культуры клеток	
		- система (управления, регулирования, контроля, проектирования, информационная)	
		- программное средство, база данных	+
		- другое (расшифровать):	

3. Результат получен при выполнении научных исследований и разработок по тематике, соответствующей Приоритетным направлениям развития науки, технологий и техники в Российской Федерации:

- Безопасность и противодействие терроризму	
- Индустрия наносистем	
- Информационно-телекоммуникационные системы	+
- Науки о жизни	
- Перспективные виды вооружения, военной и специальной техники	
- Рациональное природопользование	
- Транспортные и космические системы	
- Энергоэффективность, энергосбережение, ядерная энергетика	

4. Коды ГРНТИ: 20.23.25; 28.23.35;

5. Назначение:

Для защиты кодов криптосистем от кибератак

6. Описание, характеристики:

Предлагаются методы перестановок для эффективных криптосистем на основе РС- и БЧХ-кодов и преобразованиях Фурье-Галуа-Клиффорда

7. Преимущества перед известными аналогами:

Повышенная защищенность кодов связками ключей. Для подбора ключа методом перебора требуется не менее 2^{5000} операций.

8. Область(и) применения:

В экспертных системах искусственного интеллекта для хранения, анализа, приеме и передаче больших объемов цифровых данных в одноранговых сетях (peer-to-peer network) , в среде блокчейн – технологии и ей подобных.

9. Правовая защита:

Свидетельство о государственной регистрации программ для ЭВМ № 2018663320, 2018665257, 2018665086, 2018664314

10. Стадия готовности к практическому использованию:

Готовы к практическому использованию

11. Авторы:

Часовских Виктор Петрович, профессор кафедры прикладной информатики УГЛТУ и Бессонов Алексей Борисович, доцент кафедры прикладной информатики УГЛТУ

Зав. кафедрой Часовских В.П.