



10876 Анализ и оценка алгоритмов постквантовой криптографии типа NTRU

Оглавление

Введение	4
1 Исследовательская часть	6
1.1 Введение	6
1.2 Криптографические системы	6
1.3 Квантовая и постквантовая криптография	10
2 Конструкторская часть	13
2.1 Введение	13
2.2 Математическая постановка задачи	13
2.3 Обоснование выбора алгоритма	14
2.4 Атаки, реализуемые на алгоритм	19
2.4.1 Брут форс	19
2.4.2 Атака встреча посередине	20
2.4.3 Атака с подобранным шифротекстом	22
3 Технологическая часть	25
3.1 Технология разработки программного обеспечения	25
3.2 Описание разработки программы	30
4 Организационно-правовая часть	46
5 Организационно -экономическая часть	54
5.1 Введение	54
5.2 Расчет трудоемкости проекта	54
5.2.1 Определение численности исполнителей	64
5.2.2 Диаграмма Гантта	65
5.2.3 Анализ структуры затрат проекта	67
5.2.4 Затраты на выплату заработной платы	67



5.2.5	Отчисления на социальные нужды	69
5.2.6	Материальные затраты	69
5.2.7	Прочие затраты	70
5.2.8	Затраты на организацию рабочих мест	70
5.2.9	Накладные расходы.	71
5.2.10	Суммарные затраты на реализацию программного проекта	71
5.3	Исследование рынка	73
5.3.1	Планирование цены и прогнозирование прибыли	73
5.3.2	Сервисное обслуживание	76
5.3.3	Отчисления на социальные нужды	77
	Заключение	79
	Список использованных источников	80
	ПРИЛОЖЕНИЕ 1	84