

Алексей Петренко

# КВАНТОВО- УСТОЙЧИВЫЙ БЛОКЧЕЙН

КАК ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ  
БЛОКЧЕЙН-ЭКОСИСТЕМ  
И ПЛАТФОРМ В УСЛОВИЯХ АТАК  
С ИСПОЛЬЗОВАНИЕМ  
КВАНТОВОГО КОМПЬЮТЕРА



Издание осуществлено при финансовой поддержке  
Российского фонда фундаментальных исследований по проекту № 20-04-60080

Опорный образовательный центр по направлениям цифровой экономики на базе Университета Иннополис



Санкт-Петербург • Москва • Минск

2023

# Оглавление

<b>Вводное слово ректора Университета Иннополис А. Г. Тормасова</b> .....	6
<b>Введение</b> .....	9
<b>Глава 1. Актуальность создания квантово-устойчивых блокчейн-экосистем и платформ цифровой экономики Российской Федерации</b> .....	15
1.1. Общие сведения о технологии блокчейн .....	16
Что понимается под блокчейном .....	18
Как развивался блокчейн .....	22
Какие типы блокчейна существуют .....	29
Каковы перспективы блокчейна .....	35
1.2. Структура и поведение типового блокчейна .....	39
Связный список .....	39
Цепочка хешей .....	42
1.3. Проблема обеспечения киберустойчивости блокчейна .....	52
Сопроблемы обеспечения киберустойчивости блокчейна .....	55
1.4. Возможные представления киберустойчивого блокчейна .....	66
<b>Глава 2. Модели угроз безопасности блокчейн-экосистемам и платформам цифровой экономики Российской Федерации</b> .....	85
2.1. Модель угроз безопасности цифровой экономики Российской Федерации на основе аналитики зарубежных национальных квантовых программ .....	86
Квантовая инициатива США .....	89
Квантовые программы стран мира .....	97
Общая модель квантовых угроз безопасности .....	102
2.2. Модель квантовых угроз безопасности блокчейн-экосистемам и платформам цифровой экономики Российской Федерации .....	107
Криптопримитивы «Биткойна» .....	111
Уязвимости «Биткойна» .....	117

Сценарии комбинированных атак. ....	121
Возможные квантово-устойчивые решения. ....	127
Промежуточные итоги. ....	128
2.3. Общая модель угроз безопасности блокчейн-экосистем и платформ цифровой экономики Российской Федерации. ....	129
Алгоритмы консенсуса. ....	132
Смарт-контракты. ....	134
Оракулы. ....	136
Узлы сети. ....	139
Клиентские приложения. ....	140
Как обеспечить требуемую безопасность блокчейна. ....	141
2.4. Оценка последствий кибератак злоумышленников на блокчейн-экосистемы и платформы цифровой экономики ведущих стран мира. ....	143
2020 год. ....	143
2021 год. ....	147
2022 год. ....	148

**Глава 3. Модели и методы анализа квантовой устойчивости блокчейн-экосистем и платформ цифровой экономики Российской Федерации. .... 151**

3.1. Метод оценки квантовой устойчивости блокчейн-экосистем и платформ цифровой экономики Российской Федерации. ....	152
Вербальная и математическая задача исследования. ....	152
Предлагаемый метод оценки квантовой устойчивости блокчейна. ....	156
Разработка платформы «Квант-К». ....	162
3.2. Реализация квантового алгоритма Шора на квантовой схеме. ....	172
Квантовый алгоритм факторизации Шора. ....	180
3.3. Реализация квантового алгоритма поиска Гровера на квантовой схеме. ....	187
Разработка алгоритма криптоанализа системы асимметричного шифрования RSA. ....	193
Разработка квантового алгоритма криптоанализа системы Эль-Гамала. ....	198

3.4. Выработка требований к инструментальным средствам квантового криптоанализа .....	199
Математические пакеты Maple и Mathematica .....	202
Эмуляторы квантовых вычислений .....	205
Квантовые компьютеры .....	209
<b>Глава 4. Модели и методы синтеза квантово-устойчивых блокчейн-экосистем и платформ цифровой экономики Российской Федерации .....</b>	<b>217</b>
4.1. Эталонная модель квантово-устойчивой блокчейн-экосистемы или платформы цифровой экономики Российской Федерации .....	218
Международный технический комитет ИСО/ТК 307 (ISO/TC 307) .....	219
Международный союз электросвязи (МСЭ-Т) .....	222
Институт стандартов NIST США .....	227
Европейское агентство ENISA .....	231
Возможная модель квантово-устойчивой блокчейн-платформы .....	234
4.2. Постквантовые криптопримитивы для квантово-устойчивых блокчейн-экосистем и платформ .....	244
Постквантовые криптопримитивы .....	254
4.3. Метод параметрического выбора постквантовых криптопримитивов .....	264
4.4. Примеры создания и пилотного внедрения квантово-устойчивых блокчейнов .....	275
<b>Заключение .....</b>	<b>285</b>
<b>Список литературы .....</b>	<b>289</b>
<b>Сведения об авторе .....</b>	<b>319</b>