УДК 004.056

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ МЕТОДОМ НЕЧЕТКОЙ КЛАСТЕРИЗАЦИИ

Андреев Н.А., Бариев М.С., Коблов А.Ю.
Научный руководитель: доцент, Бибиков С.В.
Университет ИТМО, Санкт-Петербург

В связи с появлением и развитием технологий квантовых вычислений классические криптосистемы становятся более уязвимыми. В качестве контрмеры были предложены алгоритмы квантового распределения ключей, которые обеспечивают секретность ключевой информации за счёт физических принципов.

Как и любая часть системы защиты информации, квантовые сети должны быть проанализированы с точки зрения вносимых рисков и уязвимостей. В данной работе предложена методика оценки рисков информационной безопасности систем квантового распределения ключей методом нечёткой кластеризации. В ходе исследования были выполнены следующие результаты:

- описана методика оценки риска методом нечёткой кластеризации и обосновано его преимущество перед другими методами оценки риска информационной безопасности;
- построена модель изучаемой системы, определены основные угрозы и типовые уязвимости таких систем;
- проведена оптимизация метода для систем квантовой криптографии;
- дана общая методика интерпретации получаемых результатов.