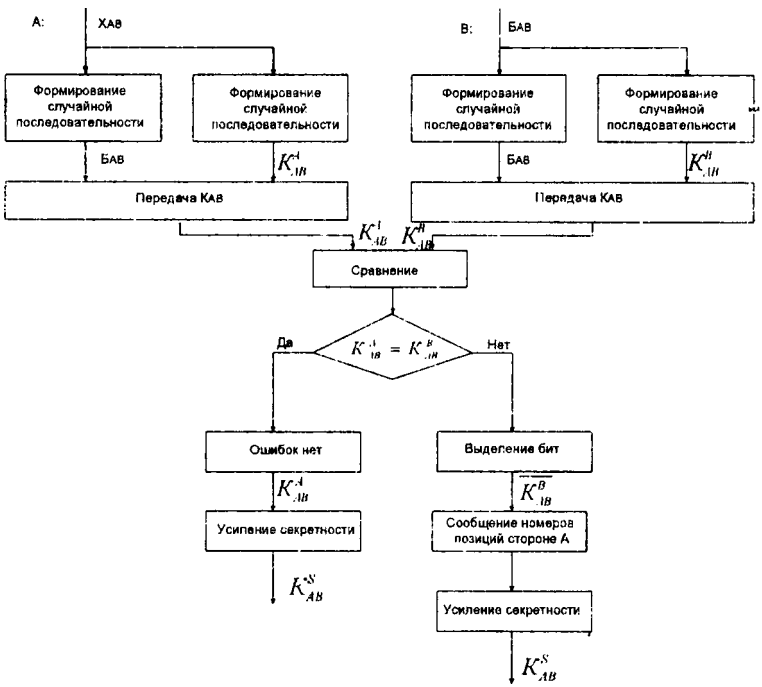
УДК 621.396.1

Формирование ключевой информации в квантовом канале

Голиков В.Ф., Пенкрат Н.В.
Белорусский государственный университет информатики
и радиоэлектроники

Криптостойкость классических квантовых алгоритмов обусловлена принципами квантовой механики. Предложен протокол распределения квантовых ключей, разработанный на основе анализа известных квантовых протоколов, но, в отличие от них, обеспечивающий функционирование квантового канала в условиях прослушивания. Двухэтапный протокол формирования ключевой информации представлен на рисунке.



Протокол основан на невозможности верного определения базисов передающей и принимающей стороны криптоаналитиком для второго сеанса передачи ключа, даже если во время первого сеанса криптоаналитику удалось перехватить передаваемую последовательность с точностью до нескольких битов.