АНАЛИЗ КРИПТОСТОЙКОСТИ ДВУХЭТАПНОГО ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Н.В. БРИЧ, В.Ф. ГОЛИКОВ

Пользователи, желающие обменяться защищенной информацией, должны обладать общим секретным ключом. Задача конфиденциальной доставки ключевой информации решается методами асимметричной криптографии. Однако до сих пор не существует математических доказательств односторонности функций, используемых в криптоалгоритмах. Рост производительности компьютеров вынуждает увеличивать размер используемых ключей и сложность односторонних функций. Новые технологии — квантовая механика — вообще переводят экспоненциальные задачи в разряд задач, решаемых за полиномиальное время.

Чтобы исключить возможность создания препятствий для установления связи между санкционированными пользователями по квантовому каналу, был предложен новый протокол передачи ключевой информации, основанный на протоколе BB84. Предложенный двухэтапный протокол формирования ключевой информации 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.

Одним из наиболее распространенных типов атак является съем информации в квантово-криптографическом канале с использованием непосредственного измерения поляризационного состояния фотона. Способ сводится к измерению непосредственно передаваемого состояния, а затем перепосылке нового состояния в зависимости от результата измерения.

В результате исследования установлено, что в некоторых случаях использование согласованных базисов на втором этапе являются уязвимостью протокола. Сделан вывод о необходимости дальнейшего усовершенствования предложенного двухэтапного протокола квантового распределения ключей.

НЕЙРОСЕТЕВЫЕ ТЕХНОЛОГИИ В КРИПТОГРАФИЧЕСКОЙ ПРОБЛЕМЕ ПЕРЕДАЧИ КЛЮЧЕЙ

В.А. ЛИПНИЦКИЙ, Е.В. БЕЛЮЖЕНКО

Защита информации от несанкционированного доступа всегда была актуальной проблемой для нашей цивилизации. К 70-м годам XX века криптография вышла за рамки секретных служб и приобрела публичный характер. Это обусловлено широчайшей информатизацией общества, когда точность, достоверность и конфиденциальность информации становится приоритетом не только для государственных служб, но и для фирм, организаций, компьютерных и телекоммуникационных сетей.

Введение в практику защиты информации односторонних функций, открытых ключей, новейших математических алгоритмов позволило наряду с симметричной криптографией использовать криптографические методы с открытыми ключами. Этот фактор и послужил основой массового применения криптосистем, к примеру, в ситуациях типа «банк-клиент».

Важным применением ассиметричной криптографии явилась возможность открытой передачи ключей для быстродействующих систем, работающих, как правило, с симметричными ключами (протокол Диффи-Хелмана). В 2005 г.