DOI: 10.37791/2687-0649-2021-16-3-120-133

Оценка криптостойкости к деструктивному воздействию «просмотр передаваемых данных» в случае использования квантовых компьютеров

А. А. Гавришев[1*], ***В. А. Бурмистров***[2]
[1] *ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, Россия*
[2] *МБУК «СЦС», Ставрополь, Россия*
** rammsteinstav@yandex.ru*

Аннотация. В данной работе проведена оценка криптостойкости известных криптографических методов и методов на основе шумоподобных сигналов, схожих по своим свойствам с «ограниченным» белым шумом и применяемых для расширения спектра передаваемых сообщений, к деструктивному воздействию «просмотр передаваемых данных» (атака, направленная на раскрытие шифртекста), основанному на полном переборе («лобовая» атака) кодовых структур (пространства ключей), в случае использования квантовых компьютеров. Установлено, что необходимым значением количества кодовых структур (пространства ключей), с учетом постоянно совершенствующихся и развивающихся вычислительных мощностей квантовых компьютеров, на ближайшие годы следует считать значение 10^{32} и выше, обеспечивающее криптостойкость минимум 3 года. Показано, что алгоритм Гровера схож с деструктивным воздействием «просмотр передаваемых данных» (атака, направленная на раскрытие шифртекста), основанном на полном переборе («лобовая» атака) всех кодовых структур (пространства ключей) с помощью современных суперЭВМ. Установлено, что известные криптографические методы потенциально могут применяться в постквантовую эпоху, а методы на основе шумоподобных сигналов потенциально, при условии их обнаружения и осведомленности о методах, положенных в их основу (без знания ключа), не могут применяться в постквантовую эпоху. Перспективным подходом в постквантовую эпоху для вопросов обеспечения информационной безопасности, по мнению авторов, является использование хаотических сигналов.

Ключевые слова: квантовые компьютеры, криптостойкость, количество кодовых структур (пространство ключей), полный перебор («лобовая» атака), информационная безопасность

Для цитирования: *Гавришев А. А., Бурмистров В. А.* Оценка криптостойкости к деструктивному воздействию «просмотр передаваемых данных» в случае использования квантовых компьютеров // Прикладная информатика. 2021. Т. 16. № 3. С. 120–133. DOI: 10.37791/2687-0649-2021-16-3-120-133