

ПРИЕМО-ПЕРЕДАЮЩЕЕ УСТРОЙСТВО НА ОСНОВЕ КАНАЛОВ ОДНОФОТОННОЙ СВЯЗИ ДЛЯ ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

А.М. Тимофеев

В настоящее время при реализации систем защиты информации достаточно часто применяют каналы однофотонной передачи информации, например, в системах квантово-криптографической связи [1–3]. Эти каналы позволяют обеспечивать абсолютную скрытность и конфиденциальной передаваемой информации за счет использования маломощных оптических импульсов, содержащих в среднем от одного

до десяти фотонов на каждый передаваемый бит (символ). Одной из основных задач при этом является регистрация столь слабых оптических импульсов, для чего используют высокочувствительные приемные модули – счетчики фотонов. Однако счетчики фотонов ввиду неидеальности своих технико-эксплуатационных характеристик могут снижать достоверность зарегистрированных данных. В частности, при увеличении мертвого времени счетчика фотонов достоверность зарегистрированных данных уменьшается при прочих равных параметрах приема [2]. В свою очередь, это может снизить уровень информационной безопасности системы связи в целом и уменьшить пропускную способность каналов однофотонной связи [3]. Для достижения наибольшей достоверности зарегистрированных данных необходимо получить статистические распределения смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации двоичных данных [2]. Поскольку до настоящего времени отсутствуют устройства, позволяющие сформировать указанные выше распределения, целью данной работы является разработка такого устройства. Объектом исследования являлся асинхронный двоичный несимметричный однородный однофотонный канал связи без памяти и со стиранием [2, 3]. Разработано приемно-передающее устройство на основе каналов однофотонной связи для передачи конфиденциальных данных. Устройство позволяет сформировать массив данных, содержащий статистические распределения смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов, не требует использования для передачи данных поляризационного оптического излучения, что, в сравнении с известными, упрощает его, ускоряет процесс обмена информацией за счет устранения процедуры согласования базисов, в которых переданы и приняты двоичные символы, а также уменьшает ошибку передачи данных, связанную с деполяризацией оптического излучения.

Литература

1. Килин С.Я., Хорошко Д.Б., Низовцев А.П. Квантовая криптография: идеи и практика. Мн., Белорусская наука, 2007. 378 с.
2. Тимофеев А.М. Достоверность принятой информации при ее регистрации в однофотонном канале связи при помощи счетчика фотонов // Информатика. 2019. Т. 16, № 2. С. 90–98.
3. Тимофеев А.М. Скорость передачи информации однофотонного канала связи с приемным модулем на основе счетчика фотонов с мертвым временем продлевающегося типа // Труды БГТУ. Сер. 3. Физико-математические науки и информатика. 2019. № 2. С. 79–86.