УДК 535.8

МЕРА ПРОТИВОДЕЙСТВИЯ АТАКЕ С ПЕРЕИЗЛУЧЕНИЕМ ФОТОНОВ ДЛЯ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ОДНИМ ДЕТЕКТОРОМ ОДИНОЧНЫХ ФОТОНОВ

Слобожанкин И.С. (ИТМО), **Геллерт М.Е.** (ИТМО)
Научный руководитель – кандидат физико-математических наук, Наседкин Б.А. (ИТМО)

Введение. Надежность систем квантового распределения ключей (КРК) обеспечивается фундаментальными принципами квантовой механики. Ключ, используемый в системах, случайный, а любая попытка взлома квантового канала будет замечена [1]. В современных системах КРК используются детекторы одиночных фотонов (ДОФ) на основе лавинного фотодиода (ЛФД) [2]. Их конструктивная особенность заключается в том, что с некоторой вероятностью после срабатывания ЛФД могут переизлучить фотон, который может вернуться в квантовый канал и нести информацию о распределяемой последовательности, что является уязвимостью систем, в которых используются ДОФ на основе ЛФД. Проблема переизлучения ЛФД актуальна, так как существует вероятность атаки на системы КРК с использованием данного эффекта [3].

Основная часть. Для исследования эффекта переизлучения была собрана схема из двух детекторов – исследуемого ДОФ на основе ЛФД и регистрирующего сверхпроводникового ДОФ. В результате измерений были получены две зависимости – распределение числа переизлученных фотонов, зарегистрированных сверхпроводниковым детектором, от времени и зависимость числа переизлученных фотонов от длительности окна срабатывания исследуемого ДОФ. На основании полученных результатов можно заключить, что большая часть переизлученных фотонов находится в пределах длительности окна срабатывания исследуемого детектора.

Для решения задачи противодействия атаке с эффектом переизлучения был проведен конструктивный анализ схемы системы КРК с одним детектором. Было выявлено, что переизлучённый фотон будет нести информацию о распределяемой последовательсности, при условии его прохождения через фазовый модулятор, на который подаётся значение фазы, аналогичное той, с которой был промодулирован зарегистрированный фотон. На основании этого было сформулировано неравенство, которое позволяет определить минимальную длину волокна, необходимую для того, чтобы исключить ситуацию, описанную ранее.

Выводы. Проведено измерение и анализ эффекта переизлучения фотонов детектором одиночных фотонов на основе лавинного фотодиода. В результате предложено неравенство, которое позволяет определить минимальную длину волокна между фазовым модулятором и ДОФ в блоке получателя, при которой для систем КРК с одним ДОФ и активным выбором базиса исключается возможность реализации атаки с переизлучением детектора.

Список использованных источников:

1. Pirandola S. et al. Advances in quantum cryptography // Advances in optics and photonics. – 2020. – Т. 12. – №. 4. – С. 1012-1236.
2. Lee Q. et al. Enhanced Photon Number Resolving Detection with High-Efficient InGaAs/InAlAs Single Photon Avalanche Diode. – 2023.
3. Ivan Vybornyi et al. Backflash Light as a Security Vulnerability in Quantum Key Distribution Systems – 2020.