УДК 535.8

МЕРА ПРОТИВОДЕЙСТВИЯ АТАКЕ С ВРЕМЕННЫМ СДВИГОМ ОСЛЕПЛЯЮЩИХ ИМПУЛЬСОВ НА СИСТЕМУ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА БОКОВЫХ ЧАСТОТАХ

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

Введение. На данный момент в системах квантового распределения ключей (КРК) в качестве детекторов наиболее часто используют детекторы одиночных фотонов (ДОФ), основанные на лавинных фотодиодах. Данный тип детекторов зачастую работает в режиме стробирования, в связи с этим детекторы обладают чувствительностью к времени попадания импульса. Злоумышленник может использовать эту уязвимость детекторов для проведения атак на системы КРК. При этом при использовании мультифотонных импульсов можно перевести ДОФ в суперлинейный режим работы [1], позволяющий при незначительном изменении числа фотонов в импульсе получить значительное изменение вероятности срабатывания детектора. В рамках данной работы была рассмотрена атака на систему квантового распределения ключей на боковых частотах (КРК БЧ), основывающаяся на суперлинейном режиме работы ДОФ.

Основная часть. Предлагаемая в данной работе атака на систему КРК БЧ представляет собой вариацию атаки с подставными состояниями [2]. Предполагается, что в случае успешной регистрации состояний отправителя злоумышленник пересылает их получателю. В случае же неудачного измерения злоумышленник отправляет излучение, компенсирующее ошибку в измерениях. Злоумышленник подбирает временной сдвиг и число фотонов на боковых частотах в импульсе таким образом чтобы в случае деструктивной интерференция (разность фаз модулирующих радиочастотных сигналов Евы и Боба равна π) не приводит к срабатыванию детектора, а для случая конструктивной интерференции (разность фаз модулирующих радиочастотных сигналов Евы и Боба равна 0) вероятность срабатывания в 2 раза выше, чем вероятность, ожидаемая в системе легитимными пользователями. Такой подбор вероятностей детектирования в различных исходах позволяет нарушителю компенсировать потери, вызванные не угаданными базисами, а для легитимных пользователей наличие нарушителя останется незамеченным ввиду того, что общее число срабатываний останется неизменным. Таким образом после публичного раскрытия информации Бобом у злоумышленника будет почти такой же выбор, как и получателя. Это означает, что Ева может украсть почти всю информацию о секретном ключе, при этом не оставит почти никаких следов присутствия.

В связи с этим было выделено две основные задачи экспериментальных исследований. Исследование возможности со стороны злоумышленника управлять ДОФ за счет перевода его в суперлинейный режим работы. Также важным аспектом экспериментальных работ является подбор оптимальных значений временного сдвига и количества фотонов на боковых частотах для проведения атаки.

Выводы. В ходе данной работы была исследована возможность управления ДОФ на базе лавинных фотодиодов за счет перевода данных детекторов в суперлинейный режим работы. Также были подобраны оптимальные значения среднего числа фотонов в импульсе и временного сдвига для проведения атаки. Были предложены контрмеры позволяющие обезопасить систему КРК БЧ от предлагаемой атаки

Список использованных источников:

1. Lydersen L. et al. Superlinear threshold detectors in quantum cryptography //Physical Review A—Atomic, Molecular, and Optical Physics. – 2011. – Т. 84. – №. 3. – С. 032320.

2. Makarov* V., Hjelme D. R. Faked states attack on quantum cryptosystems //Journal of Modern Optics. – 2005. – Т. 52. – №. 5. – С. 691-705.