УДК 535.015

ОГРАНИЧЕНИЯ ПРИМЕНИМОСТИ СПЕКТРАЛЬНЫХ ИЗМЕРЕНИЙ ПРИ АНАЛИЗЕ СТОЙКОСТИ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ К КВАНТОВОМУ ВЗЛОМУ

Соломатин О.А. (ИТМО)

Научный руководитель – кандидат физико-математических наук Наседкин Б.А. (ИТМО)

Введение. Одним из видов атак на системы квантового распределения ключей, при которых происходит воздействие лазерным излучением [1-3], является атака “Троянский конь” [4]. Реализация этой атаки подразумевает прохождение зондирующих импульсов, отправленных злоумышленником, через элементы оптической схемы до кодирующего устройства с целью извлечения информации. При этом излучение проходит через набор оптических компонентов, каждый из которых вносит свои потери, вследствие чего мощность излучения уменьшается. Одним из оптических элементов выступает CWDM-фильтр [5], который обладает определенным коэффициентом пропускания на рабочей длине волны. Однако, при последовательном подключении нескольких фильтров, их потери не складываются. Данная особенность должна быть учтена при оценке возможности реализации атаки “Троянский конь”.

Основная часть.

1) Измерения проводились для одного и для двух последовательно подключенных CWDM-фильтров.
2) Для обоих случаев были измерены потери, вносимые одним или двумя фильтрами. При сравнении видно, что на рабочей длине волны потери в обоих случаях одинаковы. На других участках исследуемого диапазона длин волн видно, что при наличии двух фильтров в схеме потери, вносимые этими фильтрами, меньше ожидаемых потерь, полученных при суммировании потерь, измеренных у отдельно взятых фильтров, на 30 дБ.
3) В отличие от других компонентов оптической схемы CWDM-фильтры вносят потери, которые не складываются друг с другом в случае использования нескольких фильтров.

Выводы. Проведен анализ вносимых каскадом CWDM-фильтров потерь. В случае прохождения оптического излучения через каскад фильтров реальные вносимые потери могут отличаться от прогнозируемых на 30 дБ. Изменение потерь на такую величину может сыграть большую роль при оценке реализации атаки "Троянский конь".

Список использованных источников:

1. Sun S.-H., Xu F., Jiang M.-S., Ma X.-C., Lo H.-K., Liang L.-M. Effect of source tampering in the security of quantum cryptography // Physical Review A. 2015 V. 92 N. 2. P. 22304.
2. Makarov V., Bourgoin J.-P., Chaiwongkhot P., Gagné M., Jennewein T., Kaiser S., Kashyap R., Legré M., Minshull C., Sajeed S. Creation of backdoors in quantum communications via laser damage // Physical Review A. 2016 V. 94 N 3 P. 30302.
3. Huang A., Li R., Egorov V., Tchouragoulov S., Kumar K., Makarov V. Laser-damage attack against optical attenuators in quantum key distribution // Physical Review Applied. 2020 V. 13 N. 3. P. 34017.
4. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems // Phys. Rev. A 73, 022320 (2006).
5. B. Nasedkin. Quantum key distribution component loopholes in 1500 – 2100 nm range perspective for Trojan-horse attacks // arXiv preprint arXiv:2211.16815 (2022).