УДК 535.15

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРОВЕДЕНИЯ АТАКИ “ТРОЯНСКИЙ КОНЬ” НА СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА В ДИАПАЗОНЕ 1500 – 2000 НМ

Толочко Д.А. (Университет ИТМО)
Научный руководитель – научный сотрудник Наседкин Б.А.
(Университет ИТМО)

В данной работе описывается возможность проведения атаки «Троянский конь» на блоки отправителя и получателя схемы действующей системы квантового распределения ключа (КРК), с учетом специфики пропускания всех входящих в схему волоконно-оптических элементов, исследованной методом спектроскопии в диапазоне 1500–2000 нм. Рассчитывается граница конфиденциальности исследуемой системы, предложен метод защиты путем ослабления подаваемого на вход сигнала.

Введение. На сегодняшний день существует множество атак как теоретических – направленных на непосредственный взлом самого ключа, так и экспериментальных – направленных на недостатки технической реализации системы КРК. Ярким примером последних является атака типа «троянский конь», являющаяся одной из самых эффективных актуальных атак. Такая атака подразумевает, что Ева посылает импульс в часть Алисы или Боба и, получая отраженный сигнал, может иметь частичную или полную информацию об используемом ключе. Так как нарушитель оперирует на длине волны, отличной от длины волны работы волоконно-оптических линий связи, необходимо иметь четкое представление о спектральных характеристиках всех используемых в системе элементах в максимально возможном диапазоне, чтобы учесть все выявленные уязвимости и защитить систему от взлома, ведь защищенность устройства зависит как от всей схемы в целом, так и от каждого отдельного элемента структуры в частности.
В работе предлагается рассмотреть конфиденциальность действующего примера системы КРК и провести реализацию атаки «троянский конь». Также рассматриваются меры противодействия нелегитимным пользователям, нивелирующие обнаруженные уязвимости технической реализации системы.

Основная часть. Полученные спектры пропускания вышеуказанных волоконно-оптических элементов, показали, что некоторые элементы ведут себя непредсказуемо вне диапазона, применяемого на данный момент легитимными пользователями систем КРК, например, спектральный фильтр после определенной длины волны перестает вести себя как фильтр. Такие недостатки элементов влияют на всю схему в целом, угрожая её безопасности, ставя под угрозу передаваемые данные. Мы рассчитали модель нижней границы конфиденциальности системы, которая показывает значение минимально возможной для совершения атаки интенсивности подаваемого излучения. Меньшие значения интенсивности будут затухать при прохождении системы, большие значения (выше верхней границы конфиденциальности), будут использовать недочеты схемы, захватывая часть секретной информации. Были проведены измерения и анализ полученных данных по ослаблению подаваемого в систему сигнала за счет нарушения условия полного внутреннего отражения в волокне при его намотке с использованием разных радиусов намотки и количества витков. Такой способ противодействия атаке «троянский конь» является более универсальным, чем использования аттенюаторов, так как позволяет осуществить более гибкую реконфигурацию схемы.

Выводы. Приведены и проанализированы графики пропускания волоконно-оптических элементов: изолятор, спектральный фильтр, светоделитель, фазовый модулятор. Исследована

возможность проведения атаки путем расчета модели минимально возможной для совершения атаки интенсивности подаваемого излучения. Рассмотрен метод защиты путем использования нарушения условия полного внутреннего отражения в волокне при его намотке на катушки определённого радиуса.

Толочко Д.А. (автор) Подпись

Наседкин Б.А. (научный руководитель) Подпись