ИСПОЛЬЗОВАНИЕ ТВЕРДОТЕЛЬНЫХ ФОТОПРИЕМНИКОВ В РЕЖИМЕ СЧЕТА ФОТОНОВ ДЛЯ КВАНТОВОЙ КРИПТОГРАФИИ

И.Р. ГУЛАКОВ, А.О. ЗЕНЕВИЧ, В.Л. КОЗЛОВ

В настоящее время для защиты информации, передаваемой по волоконно-оптическим линиям связи (ВОЛС), используют методы квантовой криптографии. Заключающей в том, если передача информации в ВОЛС осуществляется слабыми оптическими импульсами, содержащими десятки или сотни фотонов то любая попытка перехвата информации, будет обнаружена. Это связано с тем, что согласно квантовомеханической теории нельзя произвести измерения в системе, не изменив ее состояния. Тогда любая попытка перехвата информации приведет к появлению помех и обнаружению перехвата.

Для реализации такого квантового канала связи необходимо использовать фотоприемники способные регистрировать слабое оптическое излучение. В качестве таких фотоприемников для ВОЛС можно использовать лавинные фотодиоды (ЛФД), работающие в режиме счета фотонов. Поэтому целью данной работы являлась оценка возможности использования лавинных фотодиодов для методов квантовой криптографии.

В качестве объектов исследования были выбраны серийно выпускаемые кремневые лавинные фотодиоды ФД-115л и германиевых ЛФД-2.

Анализ схем включения ЛФД, реализующих режим счета фотонов показал, что для таких целей наиболее подходит стробирование фотодиода прямоугольными импульсами [1, 2]. Поскольку такое включение позволяет значительно понизить вероятность образования темновых импульсов за счет регулирования длительности импульса стробирования и обеспечивает достаточно высокое быстродействия.

На основании методики предложенной в работе [3], проведена оценка мощности оптического излучения P в максимуме чувствительности ЛФД (длина волны оптического излучения λ=0,84 мкм для кремния и λ=1,1 мкм для германия) необходимая для обнаружения импульса с вероятностью ошибки 10^{-5} и она составила P=0,3×10^{-9} Вт для кремниевых и 0,2×10^{-9} Вт для германиевых фотодиодов (это соответствует 300 фотонам). Скорость передачи данных при этом составит 2 Мбит/с. Расчет проведен для длительности импульса стробирования 250 нс, скорости счета темновых импульсов 100 с$^{-1}$ и квантовой эффективности регистрации 0,1.

Проведенные расчеты показали возможность использования кремниевых лавинных фотодиодов для методов квантовой криптографии.

Литература

1. Гулаков И.Р., Холондырёв С.В. Метод счёта фотонов в оптико-физических измерениях. — Минск: Университетское, 1989. 256 с.
2. Гулаков И.Р., Зеневич А.О. Приборы и техника эксперимента. 2001. № 4, С. 21-23.
3. Унгер Г. Оптическая связь. М.: Связь,1979. 264 с.

ШИФРОВАНИЕ ИНФОРМАЦИИ НА ОСНОВЕ МЕТОДА МОДИФИКАЦИИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

К.Я. АВЕРЬЯНОВ, А.А. БОРИСКЕВИЧ

Предложен итерационный метод модификации псевдослучайных последовательностей (ПСП), основанный на формировании последовательности случайных сдвигов из исходной ПСП, сложении по модулю 2 исходной ПСП и ее копии, смещенной на величину первого случайного сдвига из выбранных. Процесс повторяется для каждого значения случайного сдвига из оставшихся с целью получения результирующей непериодической ПСП с хорошими корреляционными свойствами. Перед сложением исходная ПСП и ее сдвинутая копия дополняются нулевыми битами, количество которых определяется величиной случайного сдвига. Величина случайного сдвига не превышает значения 2^{n-1}, где n — количество бит, равное длине сегментов, на которые разбивается исходная ПСП.

На основе метода модификации ПСП предложен метод внесения информации в ПСП. Он состоит в разбиении последовательности данных на равные блоки длиной не меньше 2 бит, добавлении старших разрядов, содержащих единицы, ко всем ненулевым и нулевым блокам (или исключении нулевых блоков) последовательности данных и формировании последовательности случайных сдвигов. Двоичная информация, содержащая в блоках последовательности данных, задает величины случайных сдвигов. В остальном процесс шифрования аналогичен процессу модификации ПСП.

Ключами для извлечения информации является ПСП и длина блока разбиения шифруемой последовательности данных. Процесс расшифровывания заключается в сложении по модулю 2 ключевой ПСП с ПСП, содержащей информацию. Восстанавливаемая последовательность первых нулевых бит соответствует величине случайного сдвига. После отбрасывания данных нулевых бит процесс повторяется до тех пор, пока длина зашифрованной последовательности не достигнет длины ключевой ПСП. Образованная последовательность величин случайных сдвигов с помощью второго ключа, указывающего какой разрядности эти величины в двоичной системе, преобразуются в исходную последовательность данных, дополненную старшими разрядами, содержащими единицы (или нулевыми блоками, исключенными на этапе шифрования).