# ВЛИЯНИЕ НАДЕЖНОСТИ ЛЕГИТИМНОГО ПРИЕМНОГО ОБОРУДОВАНИЯ НА ВЕРОЯТНОСТЬ ОШИБОЧНОЙ РЕГИСТРАЦИИ ДАННЫХ В КВАНТОВО-КРИПТОГРАФИЧЕСКИХ КАНАЛАХ СВЯЗИ

Тимофеев А. М.
Кафедра защиты информации, Белорусский государственный
университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: tamvks@mail.ru

*Применительно к квантово-криптографическому каналу связи получено выражение для оценки вероятности ошибочной регистрации символов «1», учитывающее мертвое время приемного модуля, в качестве которого использован счетчик фотонов. Установлено, что при прочих равных параметрах рост средней длительности мертвого времени продлевающегося типа приводит к увеличению средних скоростей счета сигнальных импульсов, при которых достигаются наименьшие значения вероятностей ошибочной регистрации символов «1».*

## Введение

В настоящее время достаточно интенсивно развиваются системы связи на базе квантово-криптографических каналов. Это обусловлено тем, что такие системы имеют весьма высокий уровень информационной безопасности и, в частности, позволяют обеспечивать абсолютную скрытность и конфиденциальность передаваемых данных [1]. Однако существуют трудности их практической реализации, которые в основном связаны с тем, что данные передаются посредством предельно слабого оптического излучения, содержащего в среднем не более десяти фотонов на каждый передаваемый бит (символ). Для регистрации такого излучения применяют высокочувствительные приемные модули – счетчики фотонов [1, 2]. При этом особенно важно обеспечивать высокую надежность функционирования используемого оборудования [3, 4].

Под надежностью будем понимать свойство оборудования выполнять возложенные на него функции информационной безопасности с сохранением своих характеристик (параметров) в определенных пределах при данных условиях эксплуатации.

Одним из критериев надежности является вероятность ошибочной регистрации данных, методики оценки которой описаны в [5]. Однако эти методики не применимы для квантово-криптографических каналов связи, поскольку не учитывают такой важный параметр приемного модуля, как мертвое время [1, 2]. В течение этого времени приемный модуль не чувствителен к падающему на него оптическому излучению, в результате чего возникают так называемые просчеты, которые влияют на количество ошибок при регистрации данных. В связи с этим целью данной работы являлось установить влияние мертвого времени приемного модуля квантово-криптографического канала связи на вероятность ошибочной регистрации данных.

Объектом исследования являлся квантово-криптографический канал связи, в котором в качестве приемного модуля использован счетчик фотонов.

Предметом исследования являлось установить влияние продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации двоичных символов «1». Данным типом мертвого времени характеризуются счетчики фотонов, построенные на базе лавинных фотоприемников, включенные по схеме пассивного гашения лавины.

## I. Выражение для оценки вероятности ошибочной регистрации символов «1»

Дальнейшие рассуждения будут основаны на том, что передача информации осуществляется с использованием дискретного двоичного асинхронного однородного квантово-криптографического канала связи без памяти и со стиранием. Всеми потерями информации, за исключением потерь в счетчике фотонов, пренебрегаем.

Учитывая статистические распределения, полученные в работах [6, 7], применительно к счетчикам фотонов с рассматриваемым типом мертвого времени запишем выражение для вероятности ошибочной регистрации символов «1»:

$$P_{osh1} = \sum_{N=0}^{N_2} \frac{\left[\left(n_t + n_{s1}\right)\left(\Delta t - \tau_d\right)\right]^N exp[-\left(n_t + n_{s1}\right)\left(\Delta t - \tau_d\right)]}{N!}, \quad (1)$$

где $N_1$ и $N_2$ – нижний и верхний пороговые уровни регистрации соответственно, $n_t$ – средняя скорость счета темновых импульсов на выходе счетчика фотонов, $n_{s1}$ – средняя скорость счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «1», $\Delta t$ – среднее время однофотонной передачи, $\tau_d$ – средняя длительность мертвого времени продлевающегося типа.

## II. Результаты математического моделирования и их обсуждение

На рис. 1 представлена зависимость вероятности ошибочной регистрации символов «1» от средней скорости счета сигнальных импульсов для различной средней длительности мертвого времени продлевающегося типа.

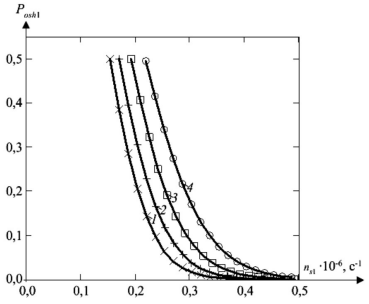


Рис. 1 – Зависимость вероятности ошибочной регистрации символа «1» от средней скорости счета сигнальных импульсов $n_{s1}$ при средней длительности мертвого времени:
1 – $\tau_d = 0$, 2 – $\tau_d = 5$ мкс, 3 –$\tau_d = 10$ мкс,
4 – $\tau_d = 15$ мкс

Расчет проводился для одинаковых значений $N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$ и $\tau_b = 100$ мкс по методикам [3, 4]. Отметим, что при других значениях $N_1$ и $N_2$, и отношениях $n_t/n_{s1}$ проявление эффекта мертвого времени продлевающегося типа для рассматриваемого канала связи аналогично представленному на рис. 1.

Диапазон значений $n_{s1}$ определялся по методикам [6, 7] с учетом того, что вероятность ошибочной регистрации символов «1» $P_{osh1}$ должна быть менее 0,5.

Из представленных результатов видно, что при прочих равных параметрах рост средней длительности мертвого времени продлевающегося типа приводит к увеличению средних скоростей счета сигнальных импульсов $n_{s1}$, при которых достигаются наименьшие значения $P_{osh1} = 0{,}00$: при $n_{s1} = 35,0 \times 10^4$ с$^{-1}$ для $\tau_d = 0$; при $n_{s1} = 38,9 \times 10^4$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s1} = 43,7 \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс; при $n_{s1} = 50,0 \times 10^4$ с$^{-1}$ для $\tau_d = 15$ мкс. Причем с ростом $\tau_d$ вероятность ошибочной регистрации символов «1» $P_{osh1}$ увеличивается. Так, например, при $n_{s1} = 31,0 \times 10^4$ с$^{-1}$ вероятность ошибочной регистрации символов «1» равна $1,31 \times 10^{-2}$ для $\tau_d = 0$; $3,17 \times 10^{-2}$ для $\tau_d = 5$ мкс; $7,19 \times 10^{-2}$ для $\tau_d = 10$ мкс; $15,08 \times 10^{-2}$ для $\tau_d = 15$ мкс.

Такое влияние $\tau_d$ и скорости счета $n_{s1}$ на $P_{osh1}$ объясняется смещением максимумов статистических распределений смеси числа темновых и сигнальных импульсов при передаче символов «1» $P_{st1}(N)$, полученных для рассматриваемого канала связи в работах [6, 7]. При наименьших величинах $n_{s1}$ для исследуемых диапазонов значений скоростей счета сигнальных импульсов этот максимум близок к 0, поэтому вероятность $P_{osh1}$ весьма высока, что следует из формулы (1) и иллюстрируется рис. 1. Однако с увеличением $n_{s1}$ вероятность $P_{osh1}$ уменьшается за счет сдвига максимумов $P_{st1}(N)$ в сторону больших значений $N$. Это приводит к спаду зависимостей $P_{osh1}(n_{s1})$ вплоть до наименьших значений (см. рис. 1). Поскольку, согласно [6, 7], в исследуемых диапазонах $n_{s1}$ увеличение $\tau_d$ при прочих равных параметрах смещает максимумы $P_{st1}(N)$ в сторону 0, $P_{osh1}$ растет с увеличением $\tau_d$ (см. рис. 1).

## Заключение

Таким образом, в данной работе получено выражение для оценки вероятности ошибочной регистрации символов «1», передаваемых по квантово-криптографическому каналу связи, в котором в качестве приемного модуля использован счетчик фотонов с мертвым временем продлевающегося типа.

Выполненные исследования показали, что при прочих равных параметрах рост средней длительности мертвого времени продлевающегося типа приводит к увеличению средних скоростей счета сигнальных импульсов, при которых достигаются наименьшие значения вероятностей ошибочной регистрации символов «1».

## Список литературы


1. Килин, С.Я. Квантовая криптография: идеи и практика / С.Я. Килин. – Мн.: Бел. наука, 2007 – 391 с.
2. Гулаков, И.Р. Фотоприемники квантовых систем: монография / И.Р. Гулаков, А.О. Зеневич. – Минск: УО ВГКС, 2012. – 276 с.
3. Тимофеев, А.М. Методика повышения достоверности принятых данных счетчика фотонов на основе анализа скорости счета импульсов при передаче двоичных символов «0» / А.М. Тимофеев // Приборы и методы измерений. – 2019. – т. 10. – № 1. – С. 80–89.
4. Тимофеев, А.М. Достоверность принятой информации при ее регистрации в однофотонном канале связи при помощи счетчика фотонов / А.М. Тимофеев // Информатика. – 2019. – т. 16.– № 2. – С. 90–98.
5. Дмитриев, С.А. Волоконно-оптическая техника: современное состояние и перспективы / С.А. Дмитриев, Н.Н. Слепов. – М.: «Волоконно-оптическая техника», 2005. – 576 с.
6. Тимофеев, А.М. Оценка влияния продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации данных квантово-криптографических каналов связи / А.М. Тимофеев // Вестник связи. – 2018. – № 1(147). – С. 56–62.
7. Тимофеев, А.М. Влияние времени однофотонной передачи информации на вероятность ошибочной регистрации данных асинхронных квантово-криптографических каналов связи / А.М. Тимофеев // Вестник ТГТУ. – 2019. – т. 25.– № 1. – С. 36–46.