ДОСТИЖЕНИЕ НАИМЕНЬШИХ ПОТЕРЬ ИНФОРМАЦИИ В КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ

Тимофеев А. М., канд. техн. наук, доцент
Белорусский государственный университет информатики и радиоэлектроники (г. Минск)

Ключевые слова: счетчик фотонов, мертвое время, канал связи.

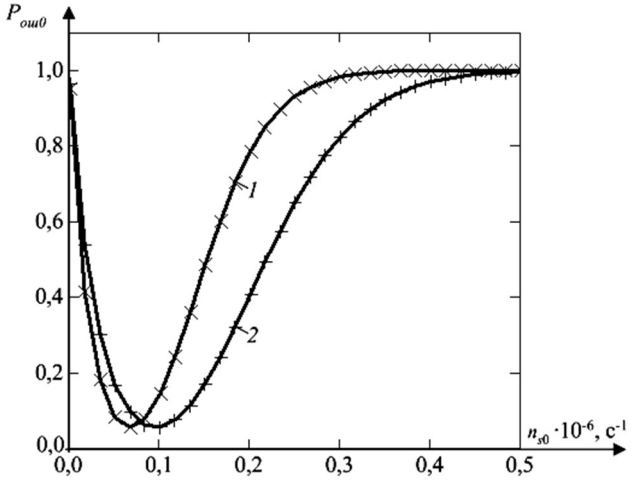
Введение. При обеспечении информационной безопасности инфраструктуры современных информационных ресурсов используют комплексный подход, который подразумевает применение квантово-криптографических каналов связи [1]. Это обусловлено тем, что такие каналы связи характеризуются высокой конфиденциальностью передаваемой информации [1, 2]. Вместе с тем, при реализации квантово-криптографических каналов связи весьма важно использовать высоконадежное оборудование, поэтому в качестве приемного оборудования целесообразно применять счетчики фотонов [1–3]. Однако счетчики фотонов имеют ненулевое мертвое время, в течение которого они не чувствительны к падающему оптическому излучению, в результате чего возникают ошибки при регистрации данных [1–3]. Поскольку до настоящего времени оценка влияния мертвого времени счетчика фотонов на потери передаваемой информации применительно к квантово-криптографическим каналам связи не выполнялась, это являлось целью данной работы. Объектом исследования являлся квантово-криптографический канал связи, в котором в качестве приемного модуля использовался счетчик фотонов с мертвым временем продлевающегося типа. Предметом исследования являлось установить влияние продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации двоичных символов «0».

Математическое моделирование канала связи. На основании выражений для оценки вероятности ошибочной регистрации данных и статистических распределений, полученных в работе [4], применительно к счетчикам фотонов с рассматриваемым типом мертвого времени вероятность ошибочной регистрации двоичных символов «0» равна:

$$P_{ош0} = 1 - \sum_{N=N_1}^{N_2} \frac{\left[\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]^N \exp\left[-\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]}{N!}, \qquad (1)$$

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_{s0} – средняя скорость счета сигнальных импульсов на выходе счетчика фотонов при передаче двоичных символов «0», Δt – среднее время однофотонной передачи, τ_d – средняя длительность мертвого времени продлевающегося типа.

На рисунке представлены зависимости вероятности ошибочной регистрации двоичных символов «0» от средней скорости счета сигнальных импульсов n_{s0} для различной средней длительности мертвого времени продлевающегося типа.



$N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, средняя длительность передачи одного бита (символа) $\tau_b = 100$ мкс, средняя длительность мертвого времени: 1 – × $\tau_d = 0$, 2 – + $\tau_d = 15$ мкс

Рисунок. **Зависимость вероятности ошибочной регистрации двоичных символов «0» от средней скорости счета сигнальных импульсов n_{s0}**

Из результатов, представленных на рисунке, видно, что с увеличением n_{s0} зависимости $P_{ош0}(n_{s0})$ сначала спадают, достигая своего наименьшего значения, а затем растут. Это имеет место как при наличии мертвого времени (см. рисунок, кривая 2), так и при его отсутствии (см. рисунок, кривая 1), что наблюдалось в ходе экспериментальных исследований рассматриваемого канала связи [3] и объясняется теми же причинами. Спад зависимости $P_{ош0}(n_{s0})$ в основном обусловлен снижением вероятности того, что на выходе канала связи не будет зарегистрирован ни символа «0», ни символа «1», в то время как на входе канала связи был сформирован символ «0». Рост же этой зависимости происходит преимущественно за счет повышения вероятности того, при передаче символа «0» на выходе канала связи будет зарегистрирован символ «1». Увеличение средней длительности мертвого времени продлевающегося типа приводит к повышению средних скоростей счета сигнальных импульсов n_{s0}, при которых достигаются наименьшие значения $P_{ош0}$. Так, например, наименьшие значения $P_{ош0} = 0{,}06$ достигаются при $n_{s0} = 66{,}6 \times 10^3$ с$^{-1}$ и $n_{s0} = 95{,}6 \times 10^3$ с$^{-1}$ соответственно для $\tau_d = 0$ и $\tau_d = 15$ мкс.

Заключение. Полученные результаты математического моделирования показали, что для достижения наименьших потерь информации важно подбирать среднюю скорость счета сигнальных импульсов n_{s0} при передаче двоичных символов «0».

Литература

1. Килин, С. Я. Квантовая криптография: идеи и практика / С. Я. Килин. – Минск : Белорус.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. Оценка влияния интенсивности оптического сигнала на вероятность ошибочной регистрации данных в однофотонном канале связи / А. М. Тимофеев // Информатика. – 2021. – Т. 18. – № 2. – С. 72-82.

4. 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.