УДК 621.383

ДОСТОВЕРНОСТЬ ПРИНЯТЫХ ДАННЫХ В КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ

А.М. ТИМОФЕЕВ
Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Введение. Существующие системы квантово-криптографической связи характеризуются максимально высоким уровнем информационной безопасности, что достигается за счет использования квантово-механического ресурса при кодировании передаваемых данных [1, 2]. При этом обмен информацией осуществляется посредством маломощных оптических импульсов, содержащих не более десяти фотонов в расчете на каждый бит (символ). Одной из основных задач, решаемых при построении квантово-криптографических систем связи, является регистрация таких маломощных импульсов. С этой целью целесообразно использовать наиболее высокочувствительные приемные модули – счетчики фотонов [1, 2]. Вместе с тем, особенно важно обеспечивать достаточно высокую достоверность данных, зарегистрированных счетчиками фотонов [3].

Под достоверностью будем понимать вероятность того, что принятые данные соответствуют переданным [3].

Известные методы оценки показателей надежности [4, 5], учитывающие ошибки при передаче информации, не применимы для систем квантово-криптографической связи. В частности, методы, представленные в работах [4, 5], не учитывают мертвое время счетчика фотонов. В течение этого времени счетчик фотонов не чувствителен к падающему на него оптическому излучению, что приводит к ошибкам при передаче данных и к уменьшению достоверности принятых данных [1–3].

В связи с этим целью данной работы являлось установить влияние скорости счета импульсов на выходе счетчика фотонов на достоверность данных, зарегистрированных в квантово-криптографическом канале связи.

Объектом исследования являлся асинхронный двоичный несимметричный однородный однофотонный канал связи без памяти и со стиранием, содержащий в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа. Выбор в качестве объекта исследования такого канала связи обусловлен тем, что его использование не требует наличия дополнительных линий связи для передачи и приема синхроимпульсов [3]. Мертвым временем продлевающегося типа характеризуются счетчики фотонов на базе лавинных фотоприемников, включенных по схеме пассивного гашения лавины [2].

Предметом исследования являлось установить влияние средней скорости счета импульсов при передаче двоичных символов «1» на выходе счетчика фотонов на достоверность зарегистрированных данных.

1. Выражение для оценки достоверности зарегистрированных данных. Дальнейшие рассуждения будут основаны на том, что передача информации осуществляется по квантово-криптографическому каналу связи двоичными символами («0» и «1») в течение длительности времени τ_b. Причем при передаче символов «0» и «1» используются оптические сигналы мощностью $И_1$ и $И_2$ соответственно ($И_1 < И_2$), которые содержат от одного до нескольких десятков фотонов и транслируются в линию связи в течение времени однофотонной передачи $\Delta t = \tau_b / 2$, а прием – с помощью счетчика фотонов, выполненного на базе лавинного фотоприемника, включенного по схеме пассивного гашения лавины [2]. Следовательно, в течение времени $t_з = \tau_b / 2$ данные в канал связи не передаются, т. е. между каждой парой символов находится так называемый «защитный» временной интервал. Поскольку символы «0» и «1» передаются импульсами различной мощности, то на выходе счетчика фотонов за время Δt формируется различное количество электрических импульсов, которое будет прямо пропорционально мощности оптического излучения. Всеми потерями информации, за исключением потерь в счетчике фотонов, пренебрегаем.

Достоверность зарегистрированных данных можно определить на основании соответствующих достоверностей зарегистрированных символов «0» D_0 и символов «1» D_1, полученных в работе [3]:

$$D = 0.5 \times \left\{ \sum_{N=N_1}^{N_2} \frac{[(n_t + n_{s0})(\Delta t - \tau_d)]^N \exp[-(n_t + n_{s0})(\Delta t - \tau_d)]}{N!} \times \right.$$
$$\times \left[\sum_{N=N_1}^{N_2} \frac{[(n_t + n_{s0})(\Delta t - \tau_d)]^N \exp[-(n_t + n_{s0})(\Delta t - \tau_d)]}{N!} + \right.$$
$$\left. + \sum_{N=N_1}^{N_2} \frac{[(n_t + n_{s1})(\Delta t - \tau_d)]^N \exp[-(n_t + n_{s1})(\Delta t - \tau_d)]}{N!} \right]^{-1} +$$
$$+ \left[1 - \sum_{N=0}^{N_2} \frac{[(n_t + n_{s1})(\Delta t - \tau_d)]^N \exp[-(n_t + n_{s1})(\Delta t - \tau_d)]}{N!} \right] \times \quad (1)$$
$$\times \left[\left[2 - \sum_{N=0}^{N_2} \frac{[(n_t + n_{s1})(\Delta t - \tau_d)]^N \exp[-(n_t + n_{s1})(\Delta t - \tau_d)]}{N!} - \right. \right.$$
$$\left. \left. - \sum_{N=0}^{N_2} \frac{[(n_t + n_{s0})(\Delta t - \tau_d)]^N \exp[-(n_t + n_{s0})(\Delta t - \tau_d)]}{N!} \right] \right]^{-1} \Bigg\},$$

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} и n_{s1} – средние скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» и «1» соответственно, τ_d – средняя длительность мертвого времени продлевающегося типа.

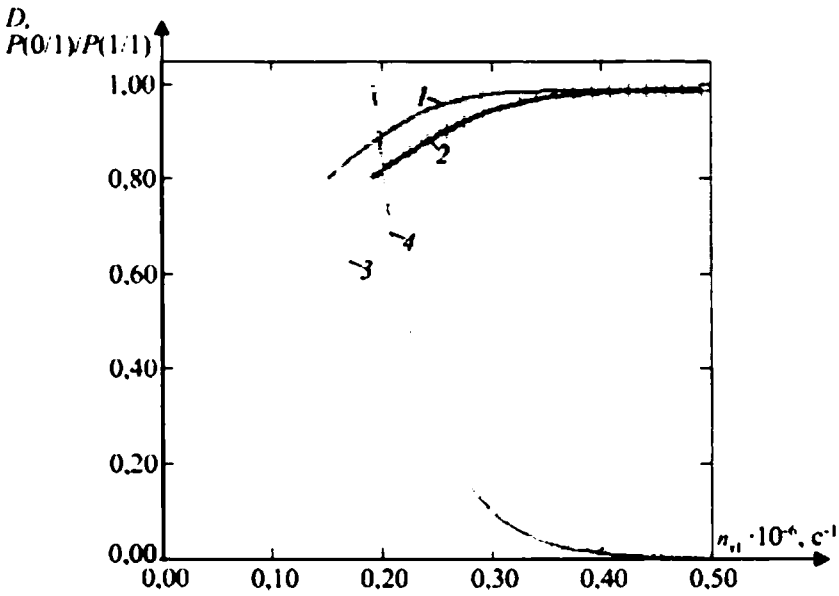
Нижний и верхний пороговые уровни регистрации – это соответственно наименьшее и наибольшее число зарегистрированных на выходе счетчика фотонов импульсов, при котором делается вывод, что передан символ «0». При превышении зарегистрированных импульсов числа N_2 делается вывод, что передан символ «1», а при регистрации импульсов в количестве, меньшем, чем N_1, принимается решение, что символ отсутствует [3].

Темновые и сигнальные – это импульсы, которые появляются на выходе счетчика фотонов соответственно в отсутствии оптического сигнала и в результате воздействия фотонов регистрируемого излучения [2]. Отметим, что для оценки мертвого времени продлевающегося типа используют среднее значение, поскольку его длительность зависит от интенсивности оптического излучения [2].

2. Результаты математического моделирования и их обсуждение. Вычисление достоверности зарегистрированных данных выполнялось для квантово-криптографических каналов связи, содержащих в качестве приемного модуля счетчик фотонов при различных значениях n_{s1} при отсутствии мертвого времени продлевающегося типа, а также при его наличии.

На рисунке 1 представлены зависимости достоверности принятых данных от средней скорости счета сигнальных импульсов n_{s1}.

При построении зависимостей, показанных на рисунке 1, величины средних скоростей счета сигнальных импульсов n_{s0} фиксировались постоянными и выбирались по методике, описанной в работе [3]. При этом критерием оптимальности являлось наименьшее значение n_{s0}, при котором вероятность регистрации на выходе канала связи символов «1» при наличии символов «0» на входе канала связи $P(1/0)$ минимальна [6]. Расчет проводился для одинаковых значений нижнего и верхнего пороговых уровней регистрации $N_1 = 1$ и $N_2 = 7$, средней скорости счета темновых импульсов $n_t = 10^3$ с$^{-1}$ и среднего времени передачи одного бита (символа) $\tau_b = 100$ мкс. Необходимо также отметить, что пороговые уровни регистрации N_1 и N_2 можно выбирать и другими, отличными от 1 и 7, но при сравнении зависимостей $D(n_{s1})$ для различных средних длительностей мертвого времени N_1 и N_2 следует фиксировать



$N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, $\tau_b = 100$ мкс

Рис. 1. Зависимости достоверности принятых данных (кривые *1* и *2*) и отношения $P(0/1) / P(1/1)$ (кривые *3* и *4*) от средней скорости счета сигнальных импульсов n_{s1} при отсутствии мертвого времени (кривые *1* и *3*, $\tau_d = 0$) и при наличии мертвого времени (кривые *2* и *4*, $\tau_d = 10$ мкс)

постоянными, как и среднее значение скорости счета темновых импульсов n_t и среднее время передачи одного бита (символа) τ_b. При этом важно учитывать, что для рассматриваемого канала связи τ_d не может превышать Δt, которое, в свою очередь, должно быть меньше средней длительности передачи одного бита (символа) τ_b на величину защитного временного интервала. В противном случае использование счетчиков фотонов для регистрации данных становится нецелесообразным [3, 6]. Отметим, что при других значениях N_1, N_2, и отношениях $\tau_d/\Delta t$, n_t/n_{s0} и n_t/n_{s1} проявление эффекта мертвого времени продлевающегося типа для рассматриваемого канала связи аналогично представленному на рисунке 1.

Зависимости $D(n_{s1})$ построены в диапазонах средних скоростей счета сигнальных импульсов, на которых вероятности регистрации на выходе канала связи символов «1» при наличии этих символов на входе канала связи удовлетворяют условию [6]

$$P(1/1) \geq 0.5. \qquad (2)$$

Из полученных результатов видно, что с увеличением средних скоростей счета сигнальных импульсов n_{s1} зависимости $D(n_{s1})$ растут, достигая насыщения, что имеет место как при наличии мертвого времени, так и при его отсутствии (см. рис. 1, кривые 1 и 2). Причем наличие мертвого времени продлевающегося типа приводит к тому, что это насыщение происходит при больших значениях n_{s1}, чем при отсутствии мертвого времени: при $n_{s1} \geq 35.0 \times 10^4$ с$^{-1}$ для $\tau_d = 0$ и при $n_{s1} \geq 43.7 \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс. Указанные особенности поведения зависимостей $D(n_{s1})$ объясняются характером изменения зависимостей переходных вероятностей $P(1/1)$ и $P(0/1)$ с увеличением средних скоростей счета сигнальных импульсов n_{s1}. Эти зависимости могут быть получены на основании методики [7], поэтому в настоящей работе они не приведены.

Выполненная оценка показала, что с увеличением средней скорости счета сигнальных импульсов n_{s1} вероятность $P(1/1)$ растет вплоть до насыщения, а вероятность $P(0/1)$ уменьшается, тоже переходя в насыщение. Это наблюдается как при наличии мертвого времени продлевающегося типа, так и при его отсутствии. Причем насыщение зависимостей $P(1/1)$ и $P(0/1)$ от n_{s1} происходит при одних и тех же средних скоростях счета сигнальных импульсов n_{s1} для соответствующих средних длительностей мертвого времени продлевающегося типа. Такое поведение зависимостей $P(1/1)$ и $P(0/1)$ с ростом n_{s1} объясняется тем, что статистические распределения смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации символов «1» $P_{s1}(N)$ имеют явно выраженный максимум, свойственный распределению Пуассона [2]. При наименьших значениях n_{s1} этот максимум находится между нижним N_1 и верхним N_2 пороговыми уровнями регистрации [8]. В этом случае достаточно велика вероятность $P(0/1)$. С увеличением n_{s1} происходит сдвиг максимумов статистических распределений $P_{s1}(N)$ в сторону больших значений N [8], поэтому переходная вероятность $P(1/1)$ растет, достигая наибольшего значения. В результате в диапазоне n_{s1}, на котором с увеличением

n_{s1} переходная вероятность $P(1/1)$ растет, а переходная вероятность $P(0/1)$ уменьшается, рост зависимости $D(n_{s1})$ объясняется снижением отношения $P(0/1)$ / $P(1/1)$ с увеличением n_{s1} (рис. 1, ривые 3 и 4).

В диапазоне n_{s1}, на котором $P(1/1) \approx 1$ и $P(0/1) \approx 0$, зависимость $D(n_{s1})$ практически неизменна и близка к единице за счет того, что отношение $P(0/1)$ / $P(1/1) \approx 0$ (см. рисунок 1). В диапазонах средних скоростей счета сигнальных импульсов n_{s1}, на которых зависимости $P(1/1)$ от n_{s1} растут, а $P(0/1)$ от n_{s1} уменьшаются, увеличение средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приводит к уменьшению переходных вероятностей $P(1/1)$ и к росту переходных вероятностей $P(0/1)$. Это обусловлено тем, что при увеличении τ_d максимумы статистических распределений $P_{s1}(N)$ сдвигаются в сторону меньших значений N [8]. В результате такого смещения повышается вероятность регистрации на выходе счетчика фотонов импульсов в количестве, меньшем N_2, поэтому $P(1/1)$ уменьшается, а $P(0/1)$ растет. В свою очередь, это приводит, к тому, что на всех исследуемых диапазонах средних скоростей счета сигнальных импульсов n_{s1} при прочих равных параметрах с увеличением τ_d достоверность принятых данных уменьшается за счет роста отношения $P(0/1)$ / $P(1/1)$. В результате, например, при $n_{s1} = 28{,}0 \times 10^4$ с$^{-1}$ достоверность принятых данных D и отношение $P(0/1)$ / $P(1/1)$ равны соответственно $97{,}29 \times 10^{-2}$ и $3{,}17 \times 10^{-2}$ для $\tau_d = 0$; $92{,}76 \times 10^{-2}$ и $14{,}72 \times 10^{-2}$ для $\tau_d = 10$ мкс.

Заключение. Применительно к асинхронному двоичному несимметричному однородному однофотонному каналу связи без памяти и со стиранием, содержащем в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа, установлено, что с ростом средней скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «1» достоверность принятых данных растет, достигая насыщения. Причем при прочих равных параметрах увеличение средней длительности мертвого времени продлевающегося типа приводит к уменьшению достоверности принятых данных, что происходит за счет роста отношения вероятности регистрации на выходе канала связи символов «0» при наличии символов «1» входе канала связи к вероятности регистрации на выходе канала связи символов «1» при наличии этих символов входе канала связи.

Результаты, полученные в настоящей работе, могут быть использованы при создании систем квантово-криптографической асинхронной связи, позволяющих с высокой достоверностью выявлять несанкционированный доступ к каналу связи за счет уменьшения погрешности определения количества ошибок легитимного приемного оборудования, в качестве которого используются счетчики фотонов с мертвым временем продлевающегося типа.

Список литературы

1. Килин, С. Я. Квантовая криптография: идеи и практика / С.Я. Килин ; под ред. С. Я. Килина [и др.]. – Минск : 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. Дмитриев, С. А. Волоконно-оптическая техника: современное состояние и перспективы / С. А. Дмитриев, Н. Н. Слепов. – 2-е изд., перераб. и доп. – М. : ООО «Волоконно-оптическая техника», 2005. – 576 с.

5. Щеглов, А. Ю. Анализ и проектирование защиты информационных систем. Контроль доступа к компьютерным ресурсам: методы, модели, технические решения / А. Ю. Щеглов. – СПб. : Профессиональная литература, 2017. – 416 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. Скорость передачи информации однофотонного канала связи с приемным модулем на основе счетчика фотонов с мертвым временем продлевающегося типа / А. М. Тимофеев // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – 2019. – № 2. – С. 79–86.

8. Тимофеев, А. М. Влияние времени однофотонной передачи информации на вероятность ошибочной регистрации данных асинхронных квантово-криптографических каналов связи / А. М. Тимофеев // Вестник БГТУ. – 2019. – Т. 25, № 1. – С. 36–46.