УДК 621.383

ОЦЕНКА НАДЕЖНОСТИ СЧЕТЧИКА ФОТОНОВ С МЕРТВЫМ ВРЕМЕНЕМ НА ОСНОВЕ АНАЛИЗА ВЕРОЯТНОСТИ ОШИБОЧНОЙ РЕГИСТРАЦИИ СИМВОЛОВ «0» В КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ

А.М. ТИМОФЕЕВ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 18 марта 2019

Аннотация. Выполнена оценка надежности счетчика фотонов с мертвым временем продлевающего типа с использованием в качестве критерия вероятности ошибочной регистрации символов «0». Применительно к квантово-криптографическому каналу связи установлено, что с увеличением средней скорости счета сигнальных импульсов на выходе счетчика фотонов вероятность ошибочной регистрации символов «0» вначале уменьшается, после чего растет. Причем рост средней длительности мертвого времени продлевающегося типа приводит к увеличению средних скоростей счета сигнальных импульсов на выходе счетчика фотонов, при которых достигаются наименьшие значения вероятности ошибочной регистрации символов «0».

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

Введение

При обеспечении защиты инфокоммуникационных систем и сетей в настоящее время весьма часто используются квантово-криптографические каналы связи [1, 2]. Такие каналы связи характеризуются высоким уровнем информационной безопасности, т. к. позволяют распределять секретные криптографические ключи, шифровать и расшифровывать пользовательские данные, выполнять взаимную идентификацию и аутентификацию как пользователей, так и данных и др. [1–5]. Как известно, при создании каналов связи необходимо обеспечивать достаточно высокую надежность оборудования легитимных пользователей, что особенно актуально для квантово-криптографических каналов связи [6, 7].

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 [6]. Отметим, что ошибки в квантово-криптографических каналах связи во многом обусловлены тем, что передача информации осуществляется посредством маломощных оптических сигналов, содержащих в среднем от одного до нескольких десятков фотонов на каждый передаваемый бит (символ) [1–5]. Для регистрации таких сигналов в настоящее время преимущественно используются высокочувствительные приемные модули – счетчики фотонов, которые, однако, не способны регистрировать падающее на них оптическое излучение до истечения длительности их мертвого времени после регистрации бита (символа) [4, 8]. Поскольку до настоящего времени оценка влияния мертвого времени счетчика фотонов на вероятность ошибочной регистрации данных не выполнялась, это являлось целью данной работы.

Объектом исследования являлся асинхронный дискретный двоичный квантово-криптографический канал связи, в котором в качестве приемного модуля использовался счетчик фотонов с мертвым временем продлевающегося типа. Выбор в качестве объекта исследования такого канала связи объясняется тем, что в ряде случаев его использование оказывается более предпочтительным, ввиду отсутствия дополнительных линий связи для передачи и приема

синхроимпульсов [8]. Мертвым временем продлевающегося типа характеризуются счетчики фотонов на базе лавинных фотоприемников, включенных по схеме пассивного гашения лавины [1, 8].

Предметом исследования являлось установление влияния продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации символов «0».

Выражение для оценки вероятности ошибочной регистрации символов «0»

Вначале получим выражение для расчета вероятности ошибочной регистрации символов «0», передаваемых по квантово-криптографическому каналу связи. 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 [4, 9, 10]. Всеми потерями информации, за исключением потерь в счетчике фотонов, пренебрегаем.

На основании выражений для оценки вероятности ошибочной регистрации данных и статистических распределений, полученных в работе [9], применительно к счетчикам фотонов с рассматриваемым типом мертвого времени запишем выражение для вероятности ошибочной регистрации символов «0»:

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

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 символов «0», Δt – среднее время однофотонной передачи, τ_d – средняя длительность мертвого времени продлевающегося типа.

Отметим, что для оценки мертвого времени продлевающегося типа используют среднее значение, т. к. его длительность зависит от интенсивности оптического излучения [8].

Темновые и сигнальные – это импульсы, которые появляются на выходе счетчика фотонов соответственно в отсутствии оптического сигнала и в результате воздействия фотонов регистрируемого излучения [8].

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 [4, 9].

Приведенное выше выражение для оценки вероятности ошибочной регистрации символов «0» получено из следующих соображений. При подаче на вход счетчика фотонов регистрируемого излучения на его выходе формируется смесь темновых и сигнальных импульсов. Статистические распределения этих импульсов при наличии на входе счетчика фотонов ослабленного оптического излучения соответствуют распределению Пуассона [1, 8] и определяют выбор нижнего и верхнего пороговых уровней регистрации N_1 и N_2. Причем для рассматриваемого канала связи при передаче символов «0» и «1» используются оптические сигналы мощностью P_1 и P_2 ($P_1 < P_2$), которые транслируются в течение длительности Δt [4, 9]. 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. Поэтому число импульсов, соответствующее символу «0», будет меньше, чем число импульсов, соответствующее символу «1» [4, 8, 9]. При этом вероятность $P_{ош0}$ имеет две составляющие. Первая составляющая определяет вероятность того, что при приеме оптического излучения счетчиком фотонов будет зарегистрировано меньше импульсов, чем установлено нижним пороговым уровенем, а вторая – вероятность того, что при наличии на входе счетчика фотонов оптического сигнала мощностью P_1 на его выходе будет зарегистрировано импульсов больше, чем установлено верхним пороговым уровенем регистрации [9–11]. Вероятность регистрации символов «0» при наличии на входе канала связи символов «0» равна $1 - P_{ош0}$.

На основании представленных рассуждений можно сделать вывод, что приведенное выражение пригодно для определения вероятности ошибочной регистрации символов «0» для рассматриваемого квантово-криптографического канала связи при соблюдении указанных выше ограничений.

Результаты и их обсуждение

Вычисление вероятности ошибочной регистрации двоичных символов «0» выполнялось для каналов связи, содержащих в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа при различных значениях τ_d и n_{s0}.

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

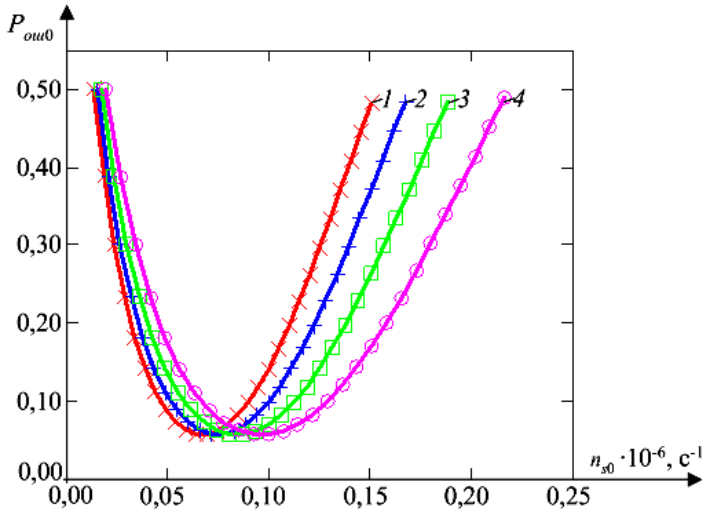

Рис. Зависимость вероятности ошибочной регистрации символа «0» от средней скорости счета сигнальных импульсов n_{s0} при средней длительности мертвого времени:
1 – × τ_d = 0; 2 – + τ_d = 5 мкс; 3 – □ τ_d = 10 мкс; 4 – ○ τ_d = 15 мкс

Зависимости $P_{ош0}(n_{s0})$ построены в диапазонах средних скоростей счета сигнальных импульсов, на которых вероятности регистрации на выходе канала связи символов «0» при наличии на входе канала связи символов «0» $P(0/0)$ составляют не менее 0,5 при заданных средних длительностях мертвого времени продлевающегося типа. Это обусловлено тем, что для рассматриваемого канала связи при $P(0/0) < 0{,}5$ использование счетчиков фотонов для регистрации данных становится нецелесообразным. Оценка переходных вероятностей $P(0/0)$ для рассматриваемого канала связи выполнялась по методике [11].

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) τ_b = 100 мкс. Необходимо отметить, что пороговые уровни регистрации можно выбирать и другими, отличными от 1 и 7, но при сравнении значений $P_{ош0}(n_{s0})$ для различных средних длительностей мертвого времени следует фиксировать N_1 и N_2 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 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 (см. работы [4, 9]); в противном случае использование счетчиков фотонов для регистрации данных становится невозможным. Отметим, что при других значениях N_1 и N_2, и отношениях $\tau_d/\Delta t$ и n_t/n_{s0} проявление эффекта мертвого времени продлевающегося типа для рассматриваемого канала связи аналогично представленному на рисунке.

Из полученных графиков следует, что с увеличением n_{s0} зависимости $P_{ош0}(n_{s0})$ вначале спадают, достигая наименьшего значения $P_{ош0} = 0{,}06$, однако при дальнейшем увеличении n_{s0} –

растут. Причем рост средней длительности мертвого времени продлевающегося типа приводит к увеличению средних скоростей счета сигнальных импульсов n_{s0}, при которых достигаются наименьшие значения $P_{ош0}$. Так, например, наименьшие значения $P_{ош0}$ достигаются при $n_{s0} = 66{,}6 \times 10^3$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} = 74{,}1 \times 10^3$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s0} = 83{,}5 \times 10^3$ с$^{-1}$ для $\tau_d = 10$ мкс; при $n_{s0} = 95{,}6 \times 10^3$ с$^{-1}$ для $\tau_d = 15$ мкс.

Такое поведение зависимостей $P_{ош0}(n_{s0})$ объясняется смещением статистических распределений смеси числа темновых и сигнальных импульсов $P_{st0}(N)$ при передаче символов «0» с изменением средних скоростей счета сигнальных импульсов и мертвого времени продлевающегося типа, что достаточно подробно исследовано автором ранее (см. [10]). Распределения $P_{st0}(N)$ имеют явно выраженный максимум, свойственный распределению Пуассона, который с увеличением средней скорости счета сигнальных импульсов n_{s0} сдвигается в сторону больших значений N, как при наличии мертвого времени продлевающегося типа, так при его отсутствии. При $n_{s0} = 0$ максимум распределения $P_{st0}(N)$ соответствует значению $N = 0$, поэтому вероятность отсутствия импульсов на выходе счетчика фотонов достаточно большая, что определяет высокую вероятность ошибочной регистрации символов «0» (см. рисунок). С увеличением n_{s0} вероятность регистрации импульсов в количестве $N_1 \div N_2$ растет за счет сдвига $P_{st0}(N)$ в сторону больших значений N, поэтому вероятность ошибочной регистрации символов «0» уменьшается, и зависимости $P_{ош0}(n_{s0})$ спадают, достигая наименьшего значения (см. рисунок). При дальнейшем увеличении средней скорости счета сигнальных импульсов n_{s0} максимумы статистических распределений $P_{st0}(N)$ продолжают сдвигаться в сторону еще больших значений N. В результате увеличивается вероятность того, что на выходе счетчика фотонов будет зарегистрировано импульсов в количестве, превышающем верхний пороговый уровень регистрации N_2, поэтому $P_{ош0}$ растет (см. рисунок).

Также из рисунка видно, что в диапазонах средних скоростей счета сигнальных импульсов n_{s0}, на которых зависимости $P_{ош0}(n_{s0})$ уменьшаются, увеличение средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приводит к росту вероятностей ошибочной регистрации символов «0». Однако в диапазонах n_{s0}, на которых зависимости $P_{ош0}(n_{s0})$ растут, увеличение τ_d, напротив, приводит к уменьшению $P_{ош0}$. Так, например, при $n_{s0} = 58{,}5 \times 10^3$ с$^{-1}$ и $n_{s0} = 107{,}8 \times 10^3$ с$^{-1}$ вероятности ошибочной регистрации символов «0» равны соответственно $6{,}24 \times 10^{-2}$ и $18{,}75 \times 10^{-2}$ для $\tau_d = 0$; $7{,}51 \times 10^{-2}$ и $13{,}02 \times 10^{-2}$ для $\tau_d = 5$ мкс; $9{,}57 \times 10^{-2}$ и $8{,}78 \times 10^{-2}$ для $\tau_d = 10$ мкс; $12{,}60 \times 10^{-2}$ и $6{,}27 \times 10^{-2}$ для $\tau_d = 15$ мкс. Объясняется это тем, что при увеличении τ_d максимумы статистических распределений $P_{st0}(N)$ сдвигаются в сторону меньших значений N [10]. При малых значениях n_{s0} максимумы распределений $P_{st0}(N)$ наблюдаются при количестве зарегистрированных импульсов, близких к нижнему пороговому уровню регистрации N_1, поэтому при увеличении средней длительности мертвого времени продлевающегося типа вероятности $P_{ош0}$ растут. Однако при достаточно больших значениях n_{s0} максимумы распределений $P_{st0}(N)$ соответствуют количеству зарегистрированных импульсов, превышающему верхний пороговый уровень регистрации N_2, поэтому с ростом τ_d вероятности ошибочной регистрации символов «0» уменьшаются.

Заключение

Получены зависимости вероятности ошибочной регистрации двоичных символов «0» $P_{ош0}$ от средней скорости счета сигнальных импульсов на выходе счетчика фотонов n_{s0} для различной средней длительности мертвого времени продлевающегося типа τ_d.

Определено, что с увеличением средней скорости счета сигнальных импульсов на выходе счетчика фотонов зависимости $P_{ош0}(n_{s0})$ спадают, достигая наименьшего значения, однако при дальнейшем увеличении n_{s0} – растут.

Установлено, что в диапазонах средних скоростей счета сигнальных импульсов n_{s0}, на которых зависимости $P_{ош0}(n_{s0})$ уменьшаются, увеличение средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приводит к росту вероятностей ошибочной регистрации символов «0». Однако в диапазонах n_{s0}, на которых зависимости $P_{ош0}(n_{s0})$ растут, увеличение τ_d, напротив, приводит к уменьшению $P_{ош0}$.

Результаты, полученные в настоящей работе, могут быть использованы при создании систем квантово-криптографической 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.

ESTIMATION OF THE RELIABILITY OF THE PHOTON COUNTER WITH DEAD TIME BASED ON THE ANALYSIS OF THE PROBABILITY OF ERRONEOUS REGISTRATION OF SYMBOLS «0» IN A QUANTUM CRYPTOGRAPHIC COMMUNICATION CHANNEL

A.M. TIMOFEEV

Abstract. Reliability qualification photon counter with dead time prolonging type was performed. The criterion was the probability of erroneous registration of symbols «0». As applied to the quantum cryptographic communication channel, it has been established that with an increase in the average count rate of signal pulses at the output of the photon counter, the probability of erroneous recording of the symbols «0» first decreases and then increases. Moreover, the increase in the average duration of the dead time of the prolonged type leads to an increase in the average count rate of the signal pulses at the output of the photon counter, at which the smallest values of the probability of erroneous registration of the characters «0» are achieved.

Keywords: photon counter, dead time, communication channels.

Список литературы

1. Килин С.Я. Квантовая криптография: идеи и практика / С.Я. Килин; под ред. С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев. – Минск: Белорус. наука, 2007.
2. Молотков С.Н. // Письма в ЖЭТФ. 2011. Т. 93. Вып. 3. С. 194–201.
3. Румянцев К.Е., Голубчиков Д.М. Квантовая связь и криптография: учебное пособие Таганрог: Изд-во ТТИ ЮФУ, 2009.
4. Тимофеев А.М. // Приборы и методы измерений. 2018. Т. 9. № 1. С. 17–27.
5. Румянцев К.Е., Пленкин А.П. // Известия ЮФУ. Технические науки. 2015. № 8 (169). С. 6–18.
6. Щеглов А.Ю. Анализ и проектирование защиты информационных систем. Контроль доступа к компьютерным ресурсам: методы, модели, технические решения СПб.: Профессиональная литература, 2017.
7. Молотков С.Н. // Письма в ЖЭТФ. 2005. Т. 81. Вып. 11. С. 733–738.
8. Гулаков И.Р., Зеневич А.О. Фотоприемники квантовых систем Минск: УО ВГКС, 2012.
9. Тимофеев А.М. // Актуальные проблемы науки XXI века. 2018. Вып. 7. С. 5–10.
10. Тимофеев А.М. // Вестник связи. 2018. № 1 (147). С. 56–62.
11. Тимофеев А.М. // Приборы и методы измерений. 2019. Т. 10. № 1. С. 80–89.