УДК 621.383

А. М. Тимофеев
Белорусский государственный университет информатики и радиоэлектроники

СКОРОСТЬ ПЕРЕДАЧИ ИНФОРМАЦИИ ОДНОФОТОННОГО КАНАЛА СВЯЗИ С ПРИЕМНЫМ МОДУЛЕМ НА ОСНОВЕ СЧЕТЧИКА ФОТОНОВ С МЕРТВЫМ ВРЕМЕНЕМ ПРОДЛЕВАЮЩЕГОСЯ ТИПА

Построена математическая модель канала связи, содержащего в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа. На основе этой модели получено выражение для оценки максимальной скорости передачи информации канала связи.

Установлено, что с увеличением средней скорости счета сигнальных импульсов при передаче символов «0» n_{s0} максимальная скорость передачи информации C_{max} вначале практически не изменяется, однако затем спадает. Причем при прочих равных параметрах с увеличением средней длительности мертвого времени продлевающегося типа τ_d этот спад наблюдается при больших значениях n_{s0}: при $n_{s0} = 66{,}6 \cdot 10^3$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} = 74{,}1 \cdot 10^3$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s0} = 83{,}5 \cdot 10^3$ с$^{-1}$ для $\tau_d = 10$ мкс; при $n_{s0} = 95{,}6 \cdot 10^3$ с$^{-1}$ для $\tau_d = 15$ мкс.

Ключевые слова: счетчик фотонов, мертвое время, канал связи, скорость передачи информации.

A. M. Timofeev
Belarusian State University of Informatics and Radioelectronics

INFORMATION TRANSFER RATE OF A SINGLE PHOTON COMMUNICATION CHANNEL WITH A RECEIVER MODULE BASED ON A PHOTON COUNTER WITH A DEAD TIME OF A PROLONGED TYPE

A mathematical model of a communication channel has been constructed, containing as counter module a photon counter with a dead time of prolonged type. An expression for estimating the maximum data transfer rate of a communication channel was derived from this model.

It has been established that with an increase in the average count rate of signal pulses when transmitting symbols "0" n_{s0}, the maximum information transfer rate C_{max} practically does not change at first, but then decreases. All other things being equal, with an increase in the average duration of the dead time of a prolonged type τ_d, this decrease is observed for large values of n_{s0}: when $n_{s0} = 66.6 \cdot 10^3$ s^{-1} for $\tau_d = 0$; when $n_{s0} = 74.1 \cdot 10^3$ s^{-1} for $\tau_d = 5$ μs; when $n_{s0} = 83.5 \cdot 10^3$ s^{-1} for $\tau_d = 10$ μs; when $n_{s0} = 95.6 \cdot 10^3$ s^{-1} for $\tau_d = 15$ μs.

Key words: photon counter, dead time, communication channel, data transfer rate.

Введение. В настоящее время достаточно активно разрабатывают системы связи, которые решают разнообразные задачи в области информационной безопасности, например, обеспечение конфиденциальности передаваемой информации, определение подлинности источника информации и самой информации и пр. [1, 2].

Одним из способов решения такого рода задач является использование криптографического или криптоподобного преобразования передаваемой информации [1, 2]. Однако информационная безопасность систем связи, в которых применяют криптографические методы защиты информации, может оказаться под угрозой. Связано это, прежде всего, с тем, что преобладающее большинство криптографических алгоритмов и стандартов являются общедоступными [1, 2]. В результате, если злоумышленник обладает достаточно большими вычислительными возможностями и изымет из канала связи, например, зашифрованные данные, то он сможет взломать шифртексты и получить доступ к конфиденциальным данным.

Другим способом решения задач обеспечения информационной безопасности передаваемой информации считается использование систем квантово-криптографической связи, которые характеризуются абсолютной скрытностью и конфиденциальностью передаваемой информации [3–5]. Отличительной особенностью квантово-криптографических систем связи является использование однофотонных волоконно-оптических каналов связи, в которых данные передаются посредством предельно слабого оптического излучения со средним числом фотонов не более десяти в расчете на каждый бит (символ). Отметим, что регистрация такого маломощного оптического излучения осуществляется с помощью высокочувствительных приемных модулей – счетчиков фотонов [6–8].

Однако современные системы однофотонной связи не позволяют достигать высоких

скоростей передачи данных [3]. Это связано, в частности, с тем, что скорость передачи данных для указанных систем связи ограничена быстродействием счетчиков фотонов. Для оценки быстродействия счетчика фотонов используют такой параметр, как длительность его мертвого времени – интервала времени, в течение которого счетчик фотонов не чувствителен к падающему на него оптическому излучению [3, 6–12].

Поскольку до настоящего времени оценка влияния мертвого времени счетчика фотонов на скорость передачи информации однофотонного канала связи не выполнялась, это являлось целью данной работы.

Объектом исследования выступал асинхронный 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 [6, 7]. Мертвым временем продлевающегося типа характеризуются счетчики фотонов на базе лавинных фотоприемников, включенных по схеме пассивного гашения лавины [6, 11, 12].

Предметом исследования являлось установление влияния продлевающегося мертвого времени счетчика фотонов на максимальную скорость передачи информации канала связи.

Основная часть. Дальнейшие рассуждения будут основаны на том, что канал связи построен на базе приемопередающих устройств [7]. Вначале построим математическую модель канала связи. Для этого воспользуемся методикой, описанной в работах [13, 14].

Рассматриваемый канал связи является двоичным, алфавит кодовых слов на входе которого представляется символами «0» и «1». Обозначим вероятности появления символов «0» и «1» на входе канала связи как $P_s(0)$ и $P_s(1)$ соответственно.

Для передачи в канал связи каждого двоичного символа используются оптические сигналы различной мощности: символ «0» передается оптическим сигналом мощностью W_1, а символ «1» – W_2 ($W_1 < W_2$). При этом в течение длительности времени передачи одного бита τ_b в канал связи поступает в среднем не более десяти фотонов как при передаче символа «0», так и при передаче символа «1».

Между каждой парой символов находится так называемый «защитный» временной интервал длительностью $\tau_b / 2$, в течение которого данные в канал связи не передаются.

Прием данных осуществляется посредством счетчика фотонов, выполненного на базе лавинного фотоприемника, включенного по схеме пассивного гашения лавины. Поскольку символы «0» и «1» передаются импульсами различной мощности, то на выходе счетчика фотонов за время однофотонной передачи $\Delta t = \tau_b / 2$ формируется различное количество электрических импульсов, которое будет прямо пропорционально мощности оптического излучения [7].

При регистрации оптического излучения счетчик фотонов подсчитывает количество импульсов и принимает решение, какой двоичный символ поступил на его вход, используя для этого нижний N_1 и верхний N_2 пороговые уровни регистрации [7]. Если на выходе счетчика фотонов зарегистрировано импульсов в количестве N_1–N_2, то принимается решение, что передан символ «0». При превышении зарегистрированных импульсов числа N_2 делается вывод, что передан символ «1». В случае регистрации импульсов в количестве, меньшем, чем N_1, принимается решение, что символ отсутствует.

Следовательно, согласно [13, 14], канал связи является несимметричным, поскольку алфавит кодовых слов на входе канала связи не совпадает с алфавитом кодовых слов на его выходе. Обозначим вероятности появления символов «0» и «1» на выходе канала связи как $P'_s(0)$ и $P'_s(1)$ соответственно, а вероятность того, что на выходе канала связи символ отсутствует, – $P'_s(-)$.

Всеми потерями информации, за исключением потерь в счетчике фотонов, пренебрегаем.

Далее получим выражение для оценки максимальной скорости передачи информации рассматриваемого канала связи.

Скорость передачи информации C – это количество информации I, приходящееся на среднее время передачи одного бита (одного символа) τ_b [13, 14]:

$$C = I / \tau_b = \left[H(B) - H(B / A)\right] / \tau_b, \quad (1)$$

где $H(B)$ – энтропия на выходе канала связи; $H(B / A)$ – условная энтропия, определяющая «ненадежность» канала или потери информации при воздействии помех.

Для оценки условной энтропии воспользуемся формулой, полученной в [12]:

$$H(B / A) = -P_s(0)\left[P(0/0)\log_2 P(0/0) + P(1/0)\log_2 P(1/0) + P(-/0) \times \log_2 P(-/0)\right] - P_s(1)\left[P(0/1)\log_2 P(0/1) + P(1/1)\log_2 P(1/1) + P(-/1)\log_2 P(-/1)\right], \quad (2)$$

где $P(0/0)$ и $P(0/1)$ – вероятности регистрации на выходе канала связи символа «0» при нали-

чии на его входе символов «0» и «1» соответственно; $P(1/0)$ и $P(1/1)$ – вероятности регистрации на выходе канала связи символа «1» при наличии на его входе символов «0» и «1» соответственно; $P(-/0)$ и $P(-/1)$ – вероятности стирания символа «0» и символа «1» соответственно, определяемые как вероятности отсутствия символов на выходе канала связи, в то время как на его входе был сформирован символ «0» и символ «1».

Энтропия на выходе канала связи запишется в виде [13, 14]:

$$H(B) = -P_s'(0)\log_2 P_s'(0) - P_s'(1)\log_2 P_s'(1) - P_s'(-)\log_2 P_s'(-). \quad (3)$$

Входящие в формулу (3) вероятности $P_s'(0)$, $P_s'(1)$ и $P_s'(-)$ равны соответственно:

$$P_s'(0) = P_s(0)P(0/0) + P_s(1)P(0/1), \quad (4)$$

$$P_s'(1) = P_s(0)P(1/0) + P_s(1)P(1/1), \quad (5)$$

$$P_s'(-) = P_s(0)P(-/0) + P_s(1)P(-/1). \quad (6)$$

Путем подстановки выражений (4)–(6) в формулу (3) получим:

$$\begin{aligned} H(B) = &-\left[P_s(0)P(0/0) + P_s(1)P(0/1)\right] \times \\ &\times \log_2\left[P_s(0)P(0/0) + P_s(1)P(0/1)\right] - \\ &- \left[P_s(0)P(1/0) + P_s(1)P(1/1)\right] \times \\ &\times \log_2\left[P_s(0)P(1/0) + P_s(1)P(1/1)\right] - \\ &- \left[P_s(0)P(-/0) + P_s(1)P(-/1)\right] \times \\ &\times \log_2\left[P_s(0)P(-/0) + P_s(1)P(-/1)\right]. \end{aligned} \quad (7)$$

Полученные выражения (2) и (7) подставим в формулу (1), тогда

$$\begin{aligned} C = \{ &-\left[P_s(0)P(0/0) + P_s(1)P(0/1)\right] \times \\ &\times \log_2\left[P_s(0)P(0/0) + P_s(1)P(0/1)\right] - \\ &- \left[P_s(0)P(1/0) + P_s(1)P(1/1)\right] \times \\ &\times \log_2\left[P_s(0)P(1/0) + P_s(1)P(1/1)\right] - \\ &- \left[P_s(0)P(-/0) + P_s(1)P(-/1)\right] \times \\ &\times \log_2\left[P_s(0)P(-/0) + P_s(1)P(-/1)\right] + \\ &+ P_s(0)\left[P(0/0)\log_2 P(0/0) + P(1/0) \times \right. \\ &\left. \times \log_2 P(1/0) + P(-/0)\log_2 P(-/0)\right] + \\ &+ P_s(1)\left[P(0/1)\log_2 P(0/1) + P(1/1) \times \right. \\ &\left. \times \log_2 P(1/1) + P(-/1)\log_2 P(-/1)\right] \} / \tau_b. \end{aligned} \quad (8)$$

Переходные вероятности $P(0/0)$, $P(-/0)$, $P(1/0)$, $P(0/1)$, $P(-/1)$ и $P(1/1)$ равны [11]:

$$P(0/0) = \sum_{N=N_1}^{N_2} \left\{ \frac{\left[(n_t + n_{s0})(\Delta t - \tau_d)\right]^N}{N!} \times \right.$$

$$\left. \times \exp\left[-(n_t + n_{s0})(\Delta t - \tau_d)\right] \right\}, \quad (9)$$

$$P(-/0) = \sum_{N=0}^{N_1-1} \left\{ \frac{\left[(n_t + n_{s0})(\Delta t - \tau_d)\right]^N}{N!} \times \right.$$

$$\left. \times \exp\left[-(n_t + n_{s0})(\Delta t - \tau_d)\right] \right\}, \quad (10)$$

$$P(1/0) = 1 - P(0/0) - P(-/0), \quad (11)$$

$$P(0/1) = \sum_{N=N_1}^{N_2} \left\{ \frac{\left[(n_t + n_{s1})(\Delta t - \tau_d)\right]^N}{N!} \times \right.$$

$$\left. \times \exp\left[-(n_t + n_{s1})(\Delta t - \tau_d)\right] \right\}, \quad (12)$$

$$P(-/1) = \sum_{N=0}^{N_1-1} \left\{ \frac{\left[(n_t + n_{s1})(\Delta t - \tau_d)\right]^N}{N!} \times \right.$$

$$\left. \times \exp\left[-(n_t + n_{s1})(\Delta t - \tau_d)\right] \right\}, \quad (13)$$

$$P(1/1) = 1 - P(0/1) - P(-/1), \quad (14)$$

где 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.

Отметим, что для оценки мертвого времени продлевающегося типа используют среднее значение, так как его длительность зависит от интенсивности оптического излучения [6].

Темновые и сигнальные импульсы – это импульсы, которые появляются на выходе счетчика фотонов соответственно в отсутствии оптического сигнала и в результате воздействия фотонов регистрируемого излучения [6, 7].

Таким образом, рассчитать максимальную скорость передачи информации (пропускную способность) канала связи, содержащего в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа, можно путем подстановки в (8) соответствующих выражений (9)–(14) при заданных пороговых уровнях регистрации N_1 и N_2, скоростях счета импульсов n_t, n_{s0} и n_{s1} и длительностях Δt и τ_d с учетом того, что скорость передачи информации достигает своего максимального значения C_{max} при $P_s(0) = P_s(1) = 0{,}5$ [13, 14].

По результатам выполненного математического моделирования рассматриваемого канала связи получены зависимости пропускной способности канала связи от средней скорости счета

сигнальных импульсов n_{s0} для различной средней длительности мертвого времени продлевающегося типа, приведенные на рис. 1.

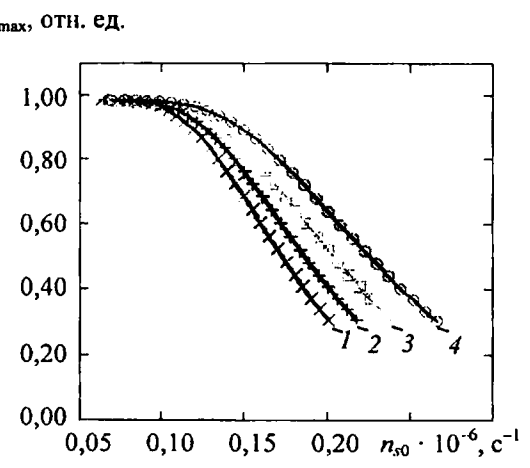

Рис. 1. Зависимость пропускной способности канала связи от средней скорости счета сигнальных импульсов n_{s0}:
$N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, $\tau_b = 100$ мкс,
средняя длительность мертвого времени:
1 – $\tau_d = 0$; *2* – $\tau_d = 5$ мкс;
3 – $\tau_d = 10$ мкс; *4* – $\tau_d = 15$ мкс

Все графики нормированы на величину $1 / \tau_b$. Зависимости $C_{max}(n_{s0})$ построены в диапазонах средних скоростей счета сигнальных импульсов, на которых переходные вероятности $P(0 / 0) \geq 0,5$ 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 $P(0 / 0)$ выполнялась по методике [15]. Для сравнения полученных зависимостей $C_{max}(n_{s0})$ величины средних скоростей счета сигнальных импульсов n_{s1} фиксировались постоянными и выбирались следующим образом. Вначале определялись диапазоны средних скоростей счета сигнальных импульсов n_{s1}, на которых переходные вероятности $P(1 / 1) \geq 0,5$ при заданных средних длительностях мертвого времени продлевающегося типа, по аналогии с выбором диапазона значений n_{s0}. Затем из каждого полученного диапазона выбиралось оптимальное значение n_{s1}. При этом критерием оптимальности являлось наименьшее значение n_{s1}, при котором переходная вероятность $P(0 / 1)$ минимальна. Такой выбор скорости счета сигнальных импульсов n_{s1} позволяет обеспечить наибольшие значения пропускной способности рассматриваемого канала связи. 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 можно выбирать и другими, отличными от 1 и 7, но при сравнении зависимостей $C_{max}(n_{s0})$ 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 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 [16]. 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 аналогично представленному на рис. 1.

Из полученных результатов видно, что для всех исследуемых значений τ_d с увеличением средних скоростей счета сигнальных импульсов n_{s0} зависимости $C_{max}(n_{s0})$ вначале практически не изменяются и близки к 1,0 отн. ед., однако затем спадают. Причем с увеличением средней длительности мертвого времени продлевающегося типа этот спад наблюдается при больших значениях n_{s0}. Так, например, зависимости $C_{max}(n_{s0})$ начинают уменьшаться соответственно при $n_{s0} \geq 66,6 \cdot 10^3$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} \geq 74,1 \cdot 10^3$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s0} \geq 83,5 \cdot 10^3$ с$^{-1}$ для $\tau_d = 10$ мкс; при $n_{s0} \geq 95,6 \cdot 10^3$ с$^{-1}$ для $\tau_d = 15$ мкс.

Указанные особенности поведения зависимостей $C_{max}(n_{s0})$ объясняются характером изменения переходных вероятностей $P(0 / 0)$, $P(1 / 0)$ и $P(– / 0)$ с изменением средних скоростей счета сигнальных импульсов n_{s0}, что иллюстрируется рис. 2.

Для всех исследуемых диапазонов средних скоростей счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» с увеличением n_{s0} переходная вероятность $P(0 / 0)$ растет, достигая наибольшего значения, после чего спадает; вероятность $P(– / 0)$ уменьшается от своего наибольшего значения до значения, близкого к нулю, переходя в насыщение, а вероятность $P(1 / 0)$, напротив, из насыщения, близкого к нулю, начинает расти вплоть до максимума (см. рис. 2).

Указанные особенности изменения переходных вероятностей $P(0 / 0)$, $P(1 / 0)$ и $P(– / 0)$ с увеличением n_{s0} имеют место, как при наличии мертвого времени продлевающегося типа, так и при его отсутствии, и происходят благо-

даря сдвигу максимумов статистических распределений смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации символов «0» $P_{s0}(N)$ [12]. При малых значениях n_{s0} этот максимум близок к $N = 0$, поэтому вероятность того, что на выходе канала связи не будет зарегистрировано ни символа «0», ни символа «1», в то время как на входе канала связи был сформирован символ «0» $P(-/0)$, достаточно большая (см. рис. 2, кривые *1''–4''*), а переходная вероятность $P(1/0) \approx 0$ (см. рис. 2, кривые *1'–4'*). Следовательно, переходная вероятность $P(0/0)$ не достигает своего наибольшего значения (см. формулу (11)).

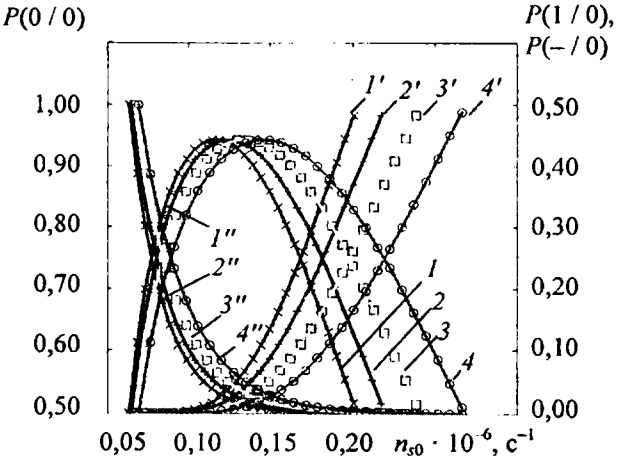

Рис. 2. Зависимости переходных вероятностей $P(0/0)$ (кривые *1–4*), $P(1/0)$ (кривые *1'–4'*) и $P(-/0)$ (кривые *1''–4''*) от средней скорости счета сигнальных импульсов n_{s0}: $N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, $\tau_b = 100$ мкс, средняя длительность мертвого времени: *1* – $\tau_d = 0$; *2* – $\tau_d = 5$ мкс; *3* – $\tau_d = 10$ мкс; *4* – $\tau_d = 15$ мкс

Однако с увеличением n_{s0} происходит сдвиг максимумов статистических распределений $P_{s0}(N)$ в сторону больших значений N, следовательно, повышается вероятность регистрации на выходе счетчика фотонов импульсов в количестве N_1–N_2. Это способствует уменьшению переходной вероятности $P(-/0)$ и росту переходной вероятности $P(0/0)$ вплоть до ее максимума. При этом вероятность регистрации на выходе счетчика фотонов импульсов в количестве, превышающем верхний пороговый уровень регистрации N_2, остается весьма малой, поэтому переходная вероятность $P(1/0) \approx 0$ (см. рис. 2).

При дальнейшем увеличении средней скорости счета сигнальных импульсов n_{s0} максимумы статистических распределений $P_{s0}(N)$ продолжают сдвигаться в сторону еще больших значений N. Это приводит к увеличению вероятности того, что на выходе счетчика фотонов будет зарегистрировано импульсов в количестве, превышающем верхний пороговый уровень регистрации N_2, поэтому переходная вероятность $P(-/0)$ продолжает уменьшаться и, достигая значения, близкого к нулю, переходит в насыщение (см. рис. 2, кривые *1''–4''*). Вместе с тем переходная вероятность $P(1/0)$ начинает расти вплоть до своего наибольшего значения (см. рис. 2, кривые *1'–4'*). В свою очередь, это приводит к уменьшению переходной вероятности $P(0/0)$, как следует из формулы (11) и иллюстрируется рис. 2 (см. кривые *1–4*).

Следует отметить, что в диапазоне n_{s0}, на котором зависимости $P(0/0)$ от n_{s0} растут, увеличение средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приема приводит к уменьшению переходной вероятности $P(0/0)$ и к росту переходной вероятности $P(-/0)$. Это объясняется тем, что при увеличении τ_d максимумы статистических распределений $P_{s0}(N)$ сдвигаются в сторону меньших значений N, как показано в работе [12]. В результате такого смещения повышается вероятность регистрации на выходе счетчика фотонов импульсов в количестве, меньшем, чем N_1, поэтому $P(0/0)$ уменьшается, а $P(-/0)$, напротив, растет. Так, например, при $n_{s0} = 52{,}8 \cdot 10^3$ с$^{-1}$ переходные вероятности $P(0/0)$ и $P(-/0)$ равны соответственно $92{,}56 \cdot 10^{-2}$ и $6{,}79 \cdot 10^{-2}$ для $\tau_d = 0$; $90{,}77 \cdot 10^{-2}$ и $8{,}88 \cdot 10^{-2}$ для $\tau_d = 5$ мкс; $88{,}20 \cdot 10^{-2}$ и $11{,}63 \cdot 10^{-2}$ для $\tau_d = 10$ мкс; $84{,}71 \cdot 10^{-2}$ и $15{,}21 \cdot 10^{-2}$ для $\tau_d = 15$ мкс.

Из рис. 2 также видно, что в диапазоне n_{s0}, на котором зависимости $P(0/0)$ от n_{s0} спадают, увеличение средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приема приводит к уменьшению переходных вероятностей $P(1/0)$ и к росту переходных вероятностей $P(0/0)$. Объясняется это тем, что в таком диапазоне значений n_{s0} максимумы $P_{s0}(N)$ располагаются в области достаточно больших значений N, поэтому весьма высока вероятность того, что на выходе счетчика фотонов будет зарегистрировано импульсов в количестве, превышающем верхний пороговый уровень регистрации N_2. При прочих равных параметрах приема эта вероятность уменьшается с ростом τ_d за счет смещения максимумов статистических распределений $P_{s0}(N)$ в область меньших значений N [12]. В свою очередь, при этом повышается вероятность регистрации на выходе счетчика фотонов импульсов в количестве N_1–N_2, поэтому увеличивается переходная вероятность $P(0/0)$ и, вместе с тем, уменьшается переходная вероятность $P(1/0)$. В результате, например, при $n_{s0} = 132{,}8 \cdot 10^3$ с$^{-1}$ переходные вероятности $P(0/0)$ и $P(1/0)$ равны

соответственно $64{,}36 \cdot 10^{-2}$ и $35{,}52 \cdot 10^{-2}$ для $\tau_d = 0$; $73{,}87 \cdot 10^{-2}$ и $25{,}89 \cdot 10^{-2}$ для $\tau_d = 5$ мкс; $82{,}26 \cdot 10^{-2}$ и $17{,}26 \cdot 10^{-2}$ для $\tau_d = 10$ мкс; $88{,}83 \cdot 10^{-2}$ и $10{,}24 \cdot 10^{-2}$ для $\tau_d = 15$ мкс.

В результате в диапазоне n_{s0}, на котором $P(1 / 0) \approx 0$, зависимость $C_{\max}(n_{s0})$ практически неизменна и близка к единице (см. рис. 1 и 2) за счет того, что достоверность принятых данных также близка к единице [15, 17]. В диапазоне n_{s0}, на котором с увеличением n_{s0} переходная вероятность $P(0 / 0)$ уменьшается, а переходная вероятность $P(1 / 0)$ растет, спад зависимости $C_{\max}(n_{s0})$ объясняется уменьшением достоверности принятых данных за счет роста потерь информации.

Как отмечалось ранее, с увеличением средней длительности мертвого времени продлевающегося типа спад зависимости $C_{\max}(n_{s0})$ наблюдается при больших значениях n_{s0}. Это обусловлено следующим. При прочих равных параметрах приема наименьшая вероятность ошибочной регистрации символов «0» $P_{\text{ош}0} = 1 - P(0 / 0) = P(1 / 0) + P(- / 0)$ с увеличением τ_d достигается при больших значениях средних скоростей счета сигнальных импульсов n_{s0}, что достаточно подробно объясняется в работе [12]. Отметим, что, согласно [12], наименьшие значения $P_{\text{ош}0} = 0{,}06$ достигаются соответственно при $n_{s0} = 66{,}6 \cdot 10^3$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} = 74{,}1 \cdot 10^3$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s0} = 83{,}5 \cdot 10^3$ с$^{-1}$ для $\tau_d = 10$ мкс; при $n_{s0} = 95{,}6 \cdot 10^3$ с$^{-1}$ для $\tau_d = 15$ мкс. Этим же значениям средних скоростей счета сигнальных импульсов при передаче символов «0» для исследуемых τ_d соответствуют n_{s0}, при превышении которых зависимости $C_{\max}(n_{s0})$ начинают уменьшаться, как отмечалось выше.

Также из рис. 1 видно, что в диапазонах средних скоростей счета сигнальных импульсов n_{s0}, на которых зависимости $C_{\max}(n_{s0})$ уменьшаются, рост средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приводит к увеличению пропускной способности канала связи. Так, например, при $n_{s0} = 91{,}5 \cdot 10^3$ с$^{-1}$ пропускная способность канала связи $C_{\max}$ равна 0,75 отн. ед. для $\tau_d = 0$; 0,81 отн. ед. для $\tau_d = 5$ мкс; 0,87 отн. ед. для $\tau_d = 10$ мкс; 0,92 отн. ед. для $\tau_d = 15$ мкс. Это обусловлено тем, что при увеличении τ_d максимумы статистических распределений $P_{s0}(N)$ сдвигаются в сторону меньших значений N, как отмечалось выше. В результате такого смещения в указанном диапазоне значений n_{s0} увеличение средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приводит к уменьшению переходной вероятности $P(1 / 0)$ и к росту переходной вероятности $P(0 / 0)$. При этом повышается достоверность принятых данных и уменьшаются потери информации [12, 15, 17], что, в свою очередь, увеличивает пропускную способность канала связи.

Заключение. Построена математическая модель асинхронного канала однофотонной связи, в котором в качестве приемного модуля использовался счетчик фотонов с мертвым временем продлевающегося типа.

По результатам математического моделирования установлено, что с увеличением средней скорости счета сигнальных импульсов при передаче символов «0» n_{s0} пропускная способность канала связи $C_{\max}$ вначале практически не изменяется, однако затем спадает. Причем при прочих равных параметрах с увеличением средней длительности мертвого времени продлевающегося типа этот спад наблюдается при больших значениях n_{s0}: при $n_{s0} = 66{,}6 \cdot 10^3$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} = 74{,}1 \cdot 10^3$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s0} = 83{,}5 \cdot 10^3$ с$^{-1}$ для $\tau_d = 10$ мкс; при $n_{s0} = 95{,}6 \cdot 10^3$ с$^{-1}$ для $\tau_d = 15$ мкс.

Получено, что в диапазонах средних скоростей счета сигнальных импульсов n_{s0}, на которых зависимости $C_{\max}(n_{s0})$ уменьшаются, рост средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приводит к увеличению пропускной способности канала связи. Так, например, при $n_{s0} = 91{,}5 \cdot 10^3$ с$^{-1}$ пропускная способность канала связи $C_{\max}$ равна 0,75 отн. ед. для $\tau_d = 0$; 0,81 отн. ед. для $\tau_d = 5$ мкс; 0,87 отн. ед. для $\tau_d = 10$ мкс; 0,92 отн. ед. для $\tau_d = 15$ мкс.

Результаты, полученные в настоящей работе, могут быть использованы при создании высокоскоростных систем квантово-криптографической асинхронной связи, содержащих в качестве приемных модулей счетчики фотонов с мертвым временем продлевающегося типа.

Автору настоящей работы видятся весьма важными исследования теоретического характера по оценке влияния средней скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «1» на пропускную способность канала связи. Не менее актуальными также являются и экспериментальные исследования, направленные на обоснование выбора лавинного фотоприемника, используемого при построении счетчика фотонов. Эти фотоприемники могут отличаться как по структуре полупроводниковых областей, так и по площади фоточувствительной поверхности. В этой связи особый интерес представляет определение того, как эти параметры влияют на пропускную способность рассматриваемого канала связи, что также планируется выполнить в ходе дальнейших комплексных исследований.

Литература

1. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. М.: НОУ «Интуит», 2016. 244 с.
2. Бабаш А. В., Шангин Г. П. Криптография. М.: СОЛОН-ПРЕСС, 2007. 512 с.
3. Килин С. Я. Квантовая криптография: идеи и практика / под ред. С. Я. Килина, Д. Б. Хорошко, А. П. Низовцева. Минск: Белорус. наука, 2007. 391 с.
4. Калачев А. А. Элементная база дальнодействующей квантовой связи. Часть 1 // Фотоника. 2017. № 1. С. 88–98. DOI: 10.22184/1993-7296.2017.61.1.88.98.
5. Румянцев К. Е., Пленкин А. П. Эффективность синхронизации системы квантового распределения ключа на однофотонных лавинных фотодиодах // Известия ЮФУ. Технические науки. 2016. № 9. С. 4–15. DOI: 10.18522/2311-3103-2016-9-415.
6. Гулаков И. Р., Зеневич А. О. Фотоприемники квантовых систем: монография. Минск: УО ВГКС, 2012. 276 с.
7. Тимофеев А. М. Устройство для передачи и приема двоичных данных по волоконно-оптическому каналу связи // Приборы и методы измерений. 2018. Т. 9, № 1. С. 17–27. DOI: 10.21122/2220-9506-2018-9-1-17-27.
8. Тимофеев А. М. Достоверность принятой информации при ее регистрации в однофотонном канале связи при помощи счетчика фотонов // Информатика. 2019. Т. 16, № 2. С. 90–98.
9. Reduced deadtime and higher rate photon-counting detection using a multiplexed detector array / S. A. Castelletto [et al.] // Journal of Modern Optics. 2007. Vol. 54. P. 337–352. DOI: 10.1080/09500340600779579.
10. Single-photon detectors combining high efficiency, high detection rates, and ultra-high timing resolution / I. E. Zadeh [et al.] // APL Photonics. 2017. Vol. 2. P. 111301-1–111301-7. DOI: 10.1063/1.5000001.
11. Тимофеев А. М. Энтропия потерь однофотонного асинхронного волоконно-оптического канала связи с приемником на основе счетчика фотонов с продлевающимся мертвым временем // Актуальные проблемы науки XXI века. 2018. Вып. 7. С. 5–10.
12. Тимофеев А. М. Оценка влияния продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации данных квантово-криптографических каналов связи // Вестник связи. 2018. № 1. С. 56–62.
13. Клюев Л. Л. Теория электрической связи. Минск: Техноперспектива, 2008. 423 с.
14. Биккенин Р. Р., Чесноков М. Н. Теория электрической связи. М.: Издат. центр «Академия», 2010. 336 с.
15. Тимофеев А. М. Методика повышения достоверности принятых данных счетчика фотонов на основе анализа скорости счета импульсов при передаче двоичных символов «0» // Приборы и методы измерений. 2019. Т. 10, № 1. С. 80–89. DOI: 10.21122/2220-9506-2019-10-1-80-89.
16. Тимофеев А. М. Влияние времени однофотонной передачи информации на вероятность ошибочной регистрации данных асинхронных квантово-криптографических каналов связи // Вестник ТГТУ. 2019. Т. 25, № 1. С. 36–46. DOI: 10.17277/vestnik.2019.01.pp.036-046.
17. Тимофеев А. М. Влияние времени однофотонной передачи информации на достоверность ее приема в квантово-криптографическом канале связи // Системный анализ и прикладная информатика. 2019. № 1. С. 67–72. DOI: 10.21122/2309-4923-2019-1-67-72.

References

1. Laponina O. R. *Osnovy setevoy bezopasnosti: kriptograficheskiye algoritmy i protokoly vzaimodeystviya* [Basics of network security: cryptographic algorithms and interaction protocols]. Moscow, NOU «Intuit» Publ., 2016. 244 p.
2. Babash A. V., Shangin G. P. *Kriptografiya* [Cryptography]. Moscow, SOLON-PRESS Publ., 2007. 512 p.
3. Kilin S. Ya. *Kvantovaya kriptografiya: idei i praktika* [Quantum cryptography: ideas and practices]. Minsk, Belorus. nauka Publ., 2007. 391 p.
4. Kalachev A. A. Components of long-distance quantum communication. Part 1. *Fotonika* [Photonics], 2017, no. 1, pp. 88–98. DOI: 10.22184/1993-7296.2017.61.1.88.98.
5. Rumyantsev K. E., Plenkin A. P. The effectiveness of synchronization of quantum key distribution system at the single-photon avalanche photodiodes. *Izvestiya YuFU. Tekhnicheskiye nauki* [Izvestiya SFedU. Engineering Sciences], 2016, no. 9, pp. 4–15. DOI: 10.18522/2311-3103-2016-9-415.
6. Gulakov I. R., Zenevich A. O. *Fotopriemniki kvantovykh sistem: monografiya* [Photodetectors of quantum systems: monograph]. Minsk, UO VGKS Publ., 2012. 276 p.

7. Timofeev A. M. Device for binary data transmitting and receiving over a fiber-optic communication channel. *Pribory i metody izmereniy* [Devices and methods of measurements], 2018, vol. 9, no. 1, pp. 17–27. DOI: 10.21122/2220-9506-2018-9-1-17-27.

8. Timofeev A. M. The reliability of the received information if it is registered in the single photon communication channel using the photon counter. *Informatika* [Informatics], 2019, vol. 16, no. 2, pp. 90–98 (In Russian).

9. Castelletto S. A., Degiovanni I. P., Schettini V., Migdall A. L. Reduced deadtime and higher rate photon-counting detection using a multiplexed detector array. *Journal of Modern Optics*, 2007, vol. 54, pp. 337–352. DOI: 10.1080/09500340600779579.

10. Zadeh I. E., Los J. W., Gourgues R. B., Steinmetz V., Bulgarini G., Dobrovolskiy S. M., Zwiller V., Dorenbos S. N. Single-photon detectors combining high efficiency, high detection rates, and ultra-high timing resolution. *APL Photonics*, 2017, vol. 2, pp. 111301-1–111301-7. DOI: 10.1063/1.5000001.

11. Timofeev A. M. Entropy of losses of a single-photon asynchronous fiber-optic communication channel with a receiver based on a photon counter with prolonged dead time. *Aktual'nyye problemy nauki XXI veka* [Current issues of science in the 21st century], 2018, issue 7, pp. 5–10 (In Russian).

12. Timofeev A. M. Estimation of the photons counter lasting dead time influence on the probability of erroneous data registration of quantum-cryptographic communication channels. *Vestnik svyazi* [Communication bulletin], 2018, no. 1, pp. 56–62 (In Russian).

13. Klyuev L. L. *Teoriya elektricheskoy svyazi* [The theory of electrical communication]. Minsk, Tekhnoperspektiva Publ., 2008. 423 p.

14. Bikkenin R. R., Chesnokov M. N. *Teoriya elektricheskoy svyazi* [The theory of electrical communication]. Moscow, Izdatel'skiy tsentr «Akademiya» Publ., 2010. 336 p.

15. Timofeev A. M. Methods of increasing the reliability of the received data of the photon counter based on the analysis of the pulse counting rate during the transmission of binary symbols «0». *Pribory i metody izmereniy* [Devices and methods of measurements], 2019, vol. 10, no. 1, pp. 80–89. DOI: 10.21122/2220-9506-2019-10-1-80-89.

16. Timofeev A. M. The effect of single photon transmission time on the probability of erroneous registration of asynchronous data of quantum cryptographic communication channels. *Vestnik TGTU* Bulletin of TSTU], 2019, vol. 25, no. 1, pp. 36–46. DOI: 10.17277/vestnik.2019.01.pp.036-046.

17. Timofeev A. M. The influence of the time of single photon transmission of information on the reliability of its reception in a quantum cryptographic communication channel. *Sistemnyy analiz i prikladnaya informatika* [System analysis and applied information science], 2019, no. 1, pp. 67–72. DOI: 10.21122/2309-4923-2019-1-67-72.

Информация об авторе

Тимофеев Александр Михайлович – кандидат технических наук, доцент, доцент кафедры защиты информации. Белорусский государственный университет информатики и радиоэлектроники (220013, г. Минск, ул. П. Бровки, 6, Республика Беларусь). E-mail: tamvks@mail.ru

Information about the author

Timofeev Alexander Mikhaylovich – PhD (Engineering), Assosiate Professor, Assistant Professor, the Department of Information Security. Belarusian State University of Informatics and Radioelectronics (6, P. Brovki str., 220013, Minsk, Republic of Belarus). E-mail: tamvks@mail.ru

Поступила 22.03.2019