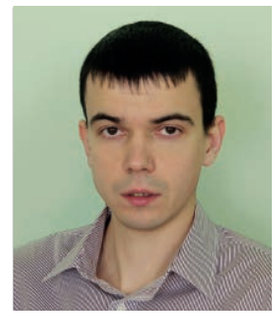
УДК 621.383

Оценка влияния мертвого времени счетчика фотонов на скорость передачи информации в канале однофотонной связи

Получены выражения для оценки скорости передачи информации и пропускной способности однофотонного канала связи, содержащего в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа. По результатам математического моделирования установлены зависимости максимальной скорости передачи информации от средней скорости счета сигнальных импульсов при передаче двоичных символов «1», что позволило обосновать выбор скоростей счета, обеспечивающих наибольшую пропускную способность однофотонного канала связи.



А.М. ТИМОФЕЕВ,
доцент кафедры защиты информации
к. т. н., доцент
УО «Белорусский государственный университет информатики и радиоэлектроники»

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

Введение. При разработке современных инфокоммуникационных систем важно обеспечить как возможность защиты передаваемой информации от несанкционированного доступа, так и высокую скорость обмена данными. Для защиты передаваемой информации от несанкционированного доступа применяют криптографические и криптоподобные преобразования информации, а также используют квантово-криптографические каналы связи [1, 2]. Информационная безопасность систем связи, использующих криптографические и криптоподобные преобразования информации, как правило, основана на вычислительной трудности задействованной математической задачи – факторизации больших чисел и/или дискретного логарифмирования [2], а не на секретности самих преобразований. Это означает, что такая система может рассматриваться как открытая (общедоступная), а ее криптостойкость определяется только секретностью ключа. Данный подход в ряде случаев оправдан и отражает один из основополагающих принципов технологии защиты информации: защищенность системы не должна зависеть от того, что невозможно быстро изменить в случае компрометации. Однако при этом злоумышленник, обладающий достаточными вычислительными ресурсами, может успешно реализовать атаку в приемлемое для себя время. Например, либо непосредственно решив математическую задачу, которая была использована легитимными пользователями для защиты информации, либо выполнив так называемую силовую атаку (методом полного перебора всех возможных ключей) [2].

Информационная безопасность квантово-криптографических систем связи обеспечивается фундаментальными законами квантовой механики. Это выгодно отличает квантово-криптографические системы связи от классических криптосистем, поскольку позволяет достичь абсолютной скрытности и конфиденциальности передаваемой информации [1]. Однако скорость передачи информации квантово-криптографических систем связи весьма низкая и часто не превышает нескольких десятков кбит/с [1], что ограничивает область их практического применения. Связано это с тем, что в квантово-криптографических системах обмен информацией осуществляется по однофотонным каналам связи, поэтому несовершенство оборудования легитимных пользователей может приводить к достаточно большому количеству ошибок при обмене данными и к потерям информации [3], не позволяя достигать высокой скорости передачи информации. Одной из причин таких ошибок является наличие мертвого времени приемного модуля – времени, в

течение которого приемный модуль нечувствителен к падающему на него оптическому излучению [1, 4]. Известные методики оценки скорости передачи информации [5, 6] неприменимы для однофотонных каналов связи, т. к. не учитывают влияние мертвого времени приемного модуля. Поскольку до настоящего времени оценка влияния мертвого времени приемного модуля однофотонного канала связи на скорость передачи информации не выполнялась, это являлось целью данной работы.

Объект исследования – счетчик фотонов с мертвым временем продлевающегося типа. Выбор в качестве объекта исследования такого приемного модуля объясняется тем, что счетчики фотонов являются одними из наиболее высокочувствительных, а их реализация на базе лавинных фотоприемников, включенных по схеме пассивного гашения лавины, приводит к наличию мертвого времени продлевающегося типа [1, 4].

Предметом исследования являлось установить влияние средней скорости счета импульсов при передаче двоичных символов «1» на выходе счетчика фотонов на скорость передачи информации однофотонного асинхронного двоичного несимметричного однородного канала связи без памяти и со стиранием.

Математическая модель однофотонного канала связи. Вначале получим выражение для расчета максимальной скорости передачи информации однофотонного асинхронного двоичного несимметричного однородного канала связи без памяти и со стиранием, используя классификацию каналов связи [5, 6]. Для этого построим математическую модель рассматриваемого канала связи с учетом того, что в качестве приемного модуля использован счетчик фотонов с мертвым временем продлевающегося типа. Дальнейшие рассуждения будут основаны на том, что передача информации осуществляется двоичными символами «0» и «1», вероятности появления которых на входе канала связи обозначим соответственно как $P_s(0)$ и $P_s(1)$, а на выходе – как $P'_s(0)$ и $P'_s(1)$. Вероятность того, что при передаче двоичного символа «0» или «1» на выходе счетчика фотонов не будет зарегистрирован ни символ «0», ни символ «1», обозначим $P'_s(-)$.

Отметим, что алфавит кодовых слов на входе канала связи не совпадает с алфавитом кодовых слов на его выходе, а вероятность отсутствия двоичного символа либо его регистрации на выходе канала связи не зависит ни от того, какой символ был на входе канала («0» или «1»), ни от ранее принятых символов. Учитывая также, что при передаче символа («0» или «1») на выходе канала связи может быть не зарегистрирован ни символ «0», ни символ «1», рассматриваемый канал является дискретным двоичным несимметричным однородным без памяти и со стиранием [5, 6]. Всеми потерями информации, за исключением потерь в счетчике фотонов, пренебрегаем.

Пусть для передачи по каналу 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 при передаче как символа «0», так и 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. Техническое решение, реализующее рассматриваемый канал связи, представлено в [7].

Скорость передачи информации C определяется как количество информации I, приходящееся на среднее время передачи одного бита (одного символа) τ_b [5, 6]:

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

где $H(B)$ – энтропия на выходе канала связи, $H(B/A)$ – условная энтропия, определяющая ненадежность канала связи или потери информации.

Энтропия на выходе канала связи запишется в следующем виде [5, 6]:

$$H(B) = -P_s'(0)\log_2 P_s'(0) - P_s'(1)\log_2 P_s'(1) - \\ -P_s'(-)\log_2 P_s'(-). \quad (2)$$

Вероятности $P'_s(0)$, $P'_s(1)$ и $P'_s(-)$, входящие в формулу (2), равны соответственно:

$$P_s'(0) = P_s(0)P(0/0) + P_s(1)P(0/1), \quad (3)$$

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

$$P_s'(-) = 1 - P_s'(0) - P_s'(1), \quad (5)$$

где $P(0/0)$ и $P(0/1)$ – вероятности регистрации на выходе канала связи символа «0» при наличии 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 того, что на выходе канала связи не будет зарегистрирован ни символ «0», ни символ «1» при наличии на его входе символов «0» и «1» соответственно.

С учетом выражений (3) ÷ (5) формула энтропии на выходе канала связи примет вид:

$$\begin{aligned} H(B) = &-\left[P_s(0)P(0/0) + \right. \\ &+ \left. P_s(1)P(0/1)\right]\log_2\left[P_s(0)P(0/0) + \right. \\ &+ \left. P_s(1)P(0/1)\right] - \left[P_s(0)P(1/0) + \right. \\ &+ \left. P_s(1)P(1/1)\right]\log_2\left[P_s(0)P(1/0) + \right. \\ &+ \left. P_s(1)P(1/1)\right] - \left[P_s(0)P(-/0) + \right. \\ &+ \left. P_s(1)P(-/1)\right]\log_2\left[P_s(0)P(-/0) + \right. \\ &+ \left. P_s(1)P(-/1)\right]. \end{aligned} \quad (6)$$

Условная энтропия $H(B/A)$ для рассматриваемого канала равна [8]

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

Путем подстановки формул (6) и (7) в выражение (1) получаем:

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

Переходные вероятности $P(0/0)$, $P(-/0)$, $P(1/0)$, $P(0/1)$, $P(-/1)$ и $P(1/1)$ можно определить на основании статистических распределений числа импульсов на выходе счетчика фотонов по методике [8]:

$$P(0/0) = \sum_{N=N_1}^{N_2}\left\{\frac{\left[\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]^N}{N!}\times\right. \\ \left.\times\exp\left[-\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]\right\}, \quad (9)$$

$$P(-/0) = \sum_{N=0}^{N_1-1}\left\{\frac{\left[\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]^N}{N!}\times\right. \\ \left.\times\exp\left[-\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]\right\}, \quad (10)$$

$$P(1/0) = \sum_{N_2+1}^{\infty}\left\{\frac{\left[\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]^N}{N!}\times\right. \\ \left.\times\exp\left[-\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]\right\}, \quad (11)$$

$$P(0/1) = \sum_{N=N_1}^{N_2}\left\{\frac{\left[\left(n_t + n_{s1}\right)\left(\Delta t - \tau_d\right)\right]^N}{N!}\times\right. \\ \left.\times\exp\left[-\left(n_t + n_{s1}\right)\left(\Delta t - \tau_d\right)\right]\right\}, \quad (12)$$

$$P(-/1) = \sum_{N=0}^{N_1-1}\left\{\frac{\left[\left(n_t + n_{s1}\right)\left(\Delta t - \tau_d\right)\right]^N}{N!}\times\right. \\ \left.\times\exp\left[-\left(n_t + n_{s1}\right)\left(\Delta t - \tau_d\right)\right]\right\}, \quad (13)$$

$$P(1/1) = \sum_{N_2+1}^{\infty}\left\{\frac{\left[\left(n_t + n_{s1}\right)\left(\Delta t - \tau_d\right)\right]^N}{N!}\times\right. \\ \left.\times\exp\left[-\left(n_t + n_{s1}\right)\left(\Delta t - \tau_d\right)\right]\right\}, \quad (14)$$

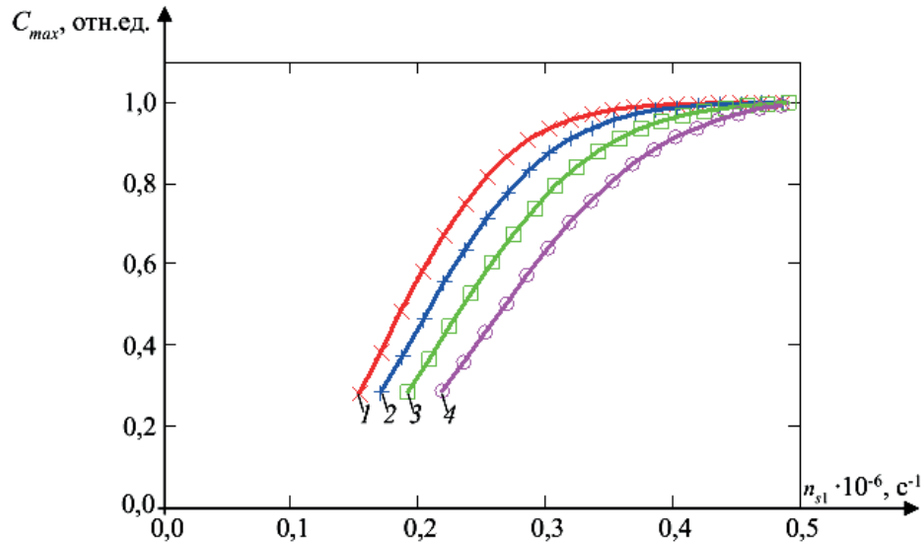
где N_1 и N_2 – нижний и верхний пороговые уровни регистрации соответственно; n_t – средняя скорость счета темновых импульсов на выходе счетчика фотонов; n_{s0} и n_{s1} – средние скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» и «1» соответственно; Δt – среднее время однофотонной передачи; τ_d – средняя длительность мертвого времени продлевающегося типа.

Нижний и верхний пороговые уровни регистрации – это 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.

Темновые и сигнальные – это импульсы, которые появляются на выходе счетчика фотонов соответственно в отсутствие оптического сигнала и в результате воздействия фотонов регистрируемого излучения [4].

Отметим, что для оценки мертвого времени продлевающегося типа используют среднее значение, т. к. его длительность зависит от интенсивности оптического излучения [4].



$N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, средняя длительность передачи одного бита (символа) $\tau_b = 100$ мкс, средняя длительность мертвого времени: 1 – × $\tau_d = 0$ мкс, 2 – + $\tau_d = 5$ мкс, 3 – □ $\tau_d = 10$ мкс, 4 – ○ $\tau_d = 15$ мкс

Рисунок – Зависимости максимальной скорости передачи информации от средней скорости счета сигнальных импульсов при передаче двоичных символов «1»

Таким образом, для оценки скорости передачи информации рассматриваемого канала связи необходимо в формулу (8) подставить соответствующие выражения (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.

Согласно [5, 6], скорость передачи информации принимает максимальное значение C_{max} – пропускную способность, когда энтропия на выходе канала связи $H(B)$ достигает своего максимального значения. Учитывая свойства энтропии, максимальное значение $H(B)$ для рассматриваемого канала связи возможно при равенстве вероятностей $P_s(0)$ и $P_s(1)$. Следовательно, рассчитать наибольшую скорость передачи информации (пропускную способность) однофотонного канала связи, содержащего в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа, можно путем подстановки в (8) соответствующих выражений (9) ÷ (14) при $P_s(0) = P_s(1) = 0{,}5$ и 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.

Результаты математического моделирования канала связи и их обсуждение. Вычисления максимальной скорости передачи информации выполнялись для каналов связи, содержащих в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа при различных значениях τ_d, n_{s0} и n_{s1}.

На рисунке представлены зависимости максимальной скорости передачи информации от средней скорости счета сигнальных импульсов при передаче двоичных символов «1» для различной средней длительности мертвого времени продлевающегося типа.

Все графики нормированы на величину $1/\tau_b$. Зависимости $C_{max}(n_{s1})$ построены в диапазонах 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. Это обусловлено тем, что для рассматриваемого канала связи при $P(1/1) < 0{,}5$ использование счетчиков фотонов для регистрации данных становится нецелесообразным. Оценка переходных вероятностей $P(1/1)$ выполнялась по методике [3]. Для сравнения полученных зависимостей $C_{max}(n_{s1})$ величины средних скоростей счета сигнальных импульсов n_{s0} фиксировались постоянными и выбирались по методике [9]. Вначале определялись диапазоны средних скоростей счета сигнальных импульсов n_{s0}, на которых переходные вероятности $P(0/0) \geq 0{,}5$ при заданных средних длительностях мертвого времени продлевающегося типа, по аналогии с выбором диапазона значений n_{s1}. Затем из каждого полученного диапазона выбиралось оптимальное значение n_{s0}. И критерием оптимальности являлось значение n_{s0}, при котором переходная вероятность $P(0/0)$ максимальна. Такой выбор скорости счета сигнальных

импульсов n_{s0} позволяет обеспечить наибольшее значение 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 $C_{\max}(n_{s1})$ 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 [3, 9]. 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 рисунке.

Из представленных результатов видно, что с ростом средней скорости счета сигнальных импульсов при передаче двоичных символов «1» пропускная способность канала связи увеличивается вплоть до насыщения. Это имеет место как при наличии мертвого времени продлевающегося типа (см. рисунок, кривые 2 ÷ 4), так и при его отсутствии (см. рисунок, кривая 1). Причем при прочих равных параметрах увеличение средней длительности мертвого времени продлевающегося типа приводит к тому, что насыщение зависимостей $C_{\max}(n_{s1})$ наблюдается при более высоких значениях n_{s1}:

при $n_{s1} \geq 35{,}0 \times 10^4$ с$^{-1}$ для $\tau_d = 0$;
при $n_{s1} \geq 38{,}9 \times 10^4$ с$^{-1}$ для $\tau_d = 5$ мкс;
при $n_{s1} \geq 43{,}7 \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс;
при $n_{s1} \geq 50{,}0 \times 10^4$ с$^{-1}$ для $\tau_d = 15$ мкс.

Указанные особенности поведения зависимостей $C_{\max}(n_{s1})$ объясняются характером изменения достоверности принятых данных D с увеличением средних скоростей счета сигнальных импульсов n_{s1} и средней длительности мертвого времени продлевающегося типа.

Под достоверностью будем понимать вероятность того, что принятые данные соответствуют переданным. Достоверность принятых данных для рассматриваемого канала связи равна [3]

$$
\begin{aligned}
D = 0{,}5 \times \Bigg\{ & \sum_{N=N_1}^{N_2} \Big\{ \Big[\big(n_t + n_{s0}\big)\big(\Delta t - \tau_d\big) \Big]^N \times \\
& \times \frac{\exp\Big[-\big(n_t + n_{s0}\big)\big(\Delta t - \tau_d\big) \Big]}{N!} \Big\} \times \\
& \times \Bigg[\sum_{N=N_1}^{N_2} \Big\{ \Big[\big(n_t + n_{s0}\big)\big(\Delta t - \tau_d\big) \Big]^N \times \\
& \times \frac{\exp\Big[-\big(n_t + n_{s0}\big)\big(\Delta t - \tau_d\big) \Big]}{N!} \Big\} + \\
& + \sum_{N=N_1}^{N_2} \Big\{ \Big[\big(n_t + n_{s1}\big)\big(\Delta t - \tau_d\big) \Big]^N \times \\
& \times \frac{\exp\Big[-\big(n_t + n_{s1}\big)\big(\Delta t - \tau_d\big) \Big]}{N!} \Big\} \Bigg]^{-1} + \\
& + \Bigg[1 - \sum_{N=0}^{N_2} \Big\{ \Big[\big(n_t + n_{s1}\big)\big(\Delta t - \tau_d\big) \Big]^N \times \\
& \times \frac{\exp\Big[-\big(n_t + n_{s1}\big)\big(\Delta t - \tau_d\big) \Big]}{N!} \Big\} \Bigg] \times \\
& \times \Bigg[2 - \sum_{N=0}^{N_2} \Big\{ \Big[\big(n_t + n_{s1}\big)\big(\Delta t - \tau_d\big) \Big]^N \times \\
& \times \frac{\exp\Big[-\big(n_t + n_{s1}\big)\big(\Delta t - \tau_d\big) \Big]}{N!} \Big\} - \\
& - \sum_{N=0}^{N_2} \Big\{ \Big[\big(n_t + n_{s0}\big)\big(\Delta t - \tau_d\big) \Big]^N \times \\
& \times \frac{\exp\Big[-\big(n_t + n_{s0}\big)\big(\Delta t - \tau_d\big) \Big]}{N!} \Big\} \Bigg]^{-1} \Bigg\}.
\end{aligned}
\tag{15}
$$

Согласно [3], в исследуемых диапазонах значений средних скоростей счета сигнальных импульсов с увеличением n_{s1} переходная вероятность $P(1/1)$ растет вплоть до насыщения, а переходная вероятность $P(0/1)$ уменьшается, тоже переходя в насыщение. В результате этого с ростом n_{s1} достоверность принятых данных D увеличивается, достигая насыщения. Поскольку величина $(1 - D)$ определяет вероятность того, что принятые данные не соответствуют переданным [3], с увеличением D потери информации уменьшаются, что приводит к снижению условной энтропии $H(B/A)$ и росту максимальной скорости передачи информации. В результате

зависимости $D(n_{s1})$ и $C_{max}(n_{s1})$ имеют не только аналогичный характер изменения с ростом n_{s1} для соответствующих средних длительностей мертвого времени продлевающегося типа, но и одинаковые причины. При наименьших значениях средних скоростей счета сигнальных импульсов в случае передачи двоичных символов «1» для исследуемых диапазонов n_{s1} максимумы статистических распределений смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации символов «1» $P_{st1}(N)$ находятся между нижним N_1 и верхним N_2 пороговыми уровнями регистрации. При этом вероятность, что на выходе канала связи будет зарегистрирован символ «0», когда на вход канала связи подается символа «1», максимальна. Как видно из формул (12) и (14), в этом случае переходная вероятность $P(0/1)$ также максимальна, что в свою очередь не позволяет достичь наибольшего значения переходной вероятности $P(1/1)$. С увеличением n_{s1} происходит сдвиг максимумов статистических распределений $P_{st1}(N)$ в сторону больших значений N [3]. Это приводит к увеличению вероятности регистрации на выходе счетчика фотонов импульсов в количестве, превышающем верхний пороговый уровень регистрации N_2. В результате переходная вероятность $P(0/1)$ уменьшается вплоть до наименьшего значения, а переходная вероятность $P(1/1)$ растет, достигая наибольшего значения [3]. Это приводит к тому, что в диапазоне n_{s1}, на котором с увеличением n_{s1} переходная вероятность $P(1/1)$ растет, а переходная вероятность $P(0/1)$ уменьшается, наблюдается рост как зависимостей $C_{max}(n_{s1})$, так и зависимостей $D(n_{s1})$ за счет снижения отношения $P(0/1) / P(1/1)$ с увеличением n_{s1}. В диапазонах n_{s1}, на которых $P(1/1) \approx 1$ и $P(0/1) \approx 0$, зависимости $D(n_{s1})$ неизменны и близки к единице за счет того, что отношения $P(0/1) / P(1/1) \approx 0$, поэтому в этих диапазонах зависимости $C_{max}(n_{s1})$ также практически неизменны и близки к единице (см. рисунок).

Как видно из рисунка, в диапазонах средних скоростей счета сигнальных импульсов при передаче двоичных символов «1», на которых зависимости $C_{max}(n_{s1})$ растут, увеличение средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приема приводит к уменьшению пропускной способности канала связи.

Так, например, при $n_{s1} = 33{,}5 \times 10^4$ с$^{-1}$ максимальная скорость передачи информации C_{max} равна
0,97 отн. ед. для $\tau_d = 0$;
0,94 отн. ед. для $\tau_d = 5$ мкс;
0,87 отн. ед. для $\tau_d = 10$ мкс;
0,76 отн. ед. для $\tau_d = 15$ мкс.

Это объясняется тем, что в этих диапазонах значений n_{s1} увеличение τ_d при прочих равных параметрах приводит к снижению достоверности принятых данных. Такое снижение величины D обусловлено уменьшением переходных вероятностей $P(1/1)$ и ростом переходных вероятностей $P(0/1)$ с увеличением τ_d, что достаточно подробно исследовано в работе [3]. При увеличении τ_d максимумы статистических распределений $P_{st1}(N)$ сдвигаются в сторону меньших значений N. За счет этого 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 результате имеет место рост отношения $P(0/1) / P(1/1)$, что приводит к уменьшению достоверности принятых данных D [3] и, следовательно, к снижению C_{max}.

Выполненная оценка показала, что для рассматриваемого канала связи пропускная способность достигает своей максимальной величины при наибольших значениях переходных вероятностей $P(0/0)$ и $P(1/1)$, которые с увеличением τ_d в свою очередь обеспечиваются при более высоких значениях n_{s0} и n_{s1} соответственно: при $n_{s0} = 66{,}6 \times \times 10^3$ с$^{-1}$ и $n_{s1} = 35{,}0 \times 10^4$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} = 74{,}1 \times \times 10^3$ с$^{-1}$ и $n_{s1} = 38{,}9 \times 10^4$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s0} = = 83{,}5 \times 10^3$ с$^{-1}$ и $n_{s1} = 43{,}7 \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс; при $n_{s0} = 95{,}6 \times 10^3$ с$^{-1}$ и $n_{s1} = 50{,}0 \times 10^4$ с$^{-1}$ для $\tau_d = = 15$ мкс.

Сопоставление результатов, представленных в данной работе, с полученными ранее в [3, 9] позволяет сделать вывод о следующем. Для однофотонного асинхронного двоичного несимметричного однородного канала связи без памяти и со стиранием достижение наибольшей скорости передачи информации возможно в случае подбора оптимальных значений мощностей оптических сигналов, используемых для передачи двоичных символов «0» W_1 и символов «1» W_2. При этом в качестве критерия оптимальности для выбора W_1 и W_2 могут быть использованы значения n_{s0} и n_{s1} соответственно, при которых переходные вероятности $P(0/0)$ и $P(1/1)$ максимальны. Следует отметить, что скорости счета сигнальных импульсов n_{s0} и n_{s1} могут быть рассчитаны по формулам [10]

$$n_{s0} = (\eta_p W_0)/(h\nu) \text{ и } n_{s1} = (\eta_p W_1)/(h\nu), \qquad (16)$$

где η_p – квантовая эффективность регистрации счетчика фотонов, h – постоянная Планка, ν – частота оптического излучения. Квантовая эффективность – это отношение числа зарегистрированных приемным модулем фотонов оптического излучения к общему числу поступивших фотонов [4].

Заключение. Применительно к однофотонному асинхронному двоичному несимметричному однородному каналу связи без памяти и со стиранием, содержащему в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа, получено выражение для расчета максимальной скорости передачи информации.

Выполненные исследования показали, что пропускная способность канала связи достигает своего максимума при наибольших значениях переходных вероятностей $P(0/0)$ и $P(1/1)$. С увеличением средней длительности мертвого времени продлевающегося типа τd это становится возможным при более высоких значениях скоростей счета сигнальных импульсов n_{s0} и n_{s1}: при $n_{s0} = 66{,}6 \times 10^3$ с$^{-1}$ и $n_{s1} = 35{,}0 \times 10^4$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} = 74{,}1 \times 10^3$ с$^{-1}$ и $n_{s1} = 38{,}9 \times 10^4$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s0} = 83{,}5 \times 103$ с$^{-1}$ и $n_{s1} = 43{,}7 \times 104$ с$^{-1}$ для $\tau_d =$ 10 мкс; при $n_{s0} = 95{,}6 \times 103$ с$^{-1}$ и $n_{s1} = 50{,}0 \times 104$ с$^{-1}$ для $\tau_d = 15$ мкс.

ЛИТЕРАТУРА

1. **Килин, С.Я.** Квантовая криптография: идеи и практика / С.Я. Килина; под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. – Минск: Белорус. наука, 2007. – 391 с.
2. **Бабаш, А.В.** Криптография / А.В. Бабаш, Г.П. Шанкин; под ред. А.П. Шерстюка и Э.А. Применко. – М.: СОЛОН-ПРЕСС, 2007. – 512 с.
3. **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.
4. **Гулаков, И.Р.** Фотоприемники квантовых систем: монография / И.Р. Гулаков, А.О. Зеневич. – Минск: УО ВГКС, 2012. – 276 с.
5. **Клюев, Л.Л.** Теория электрической связи / Л.Л. Клюев. – Минск: Технoперспектива, 2008. – 423 с.
6. **Биккенин, Р.Р.** Теория электрической связи / Р.Р. Биккенин, М.Н. Чесноков. – М.: Издательский цент «Академия», 2010. – 336 с.
7. **Тимофеев, А.М.** Устройство для передачи и приема двоичных данных по волоконно-оптическому каналу связи / А.М. Тимофеев // Приборы и методы измерений. – 2018. – т. 9.– № 1. – С. 17–27.
8. **Тимофеев, А.М.** Энтропия потерь однофотонного асинхронного волоконно-оптического канала связи с приемником на основе счетчика фотонов с продлевающимся мертвым временем / А.М. Тимофеев // Актуальные проблемы науки XXI века. – 2018. – вып. 7. – С. 5–10.
9. **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.
10. **Гольданский, В.И.** Статистика отсчетов при регистрации ядерных частиц / В.И. Гольданский, А.В. Куценко, М.И. Подгорецкий; под ред. Б.Л. Лившиц. – М.: Государственное издательство физико-математической литературы, 1959. – 411 с.

Expressions for estimating the information transfer rate and throughput of a single-photon communication channel are obtained. These expressions take into account the prolonged dead time of the photon counter used as a receiving module of the communication channel. The dependences of the maximum information transfer rate on the average count rate of signal pulses when transmitting binary symbols «1» are established by the results of mathematical modeling of this communication channel. This made it possible to determine the justification for the choice of counting rates, providing the highest throughput of a single-photon communication channel.

Key words: *photon counter, dead time, single-photon communication channel.*

Получено 14.10.2019.