УДК 621.383

ПРОПУСКНАЯ СПОСОБНОСТЬ КВАНТОВО-КРИПТОГРАФИЧЕСКОГО КАНАЛА СВЯЗИ

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

Введение

Одной из важнейших задач в сфере информационной безопасности объектов критической информационной инфраструктуры является обеспечение скрытности и конфиденциальности передаваемой информации [1]. Данными объектами могут быть, например, секретные криптографические ключи. Эти ключи часто требуется распределять по открытым каналам связи, к которым может иметь доступ злоумышленник.

Для решения указанных задач, как правило, применяют комплекс мер, включая использование квантово-криптографических каналов связи. Это позволяет достичь абсолютной скрытности и конфиденциальности передаваемой информации за счет ее кодирования посредством квантово-механического ресурса [2]. При этом обмен информацией осуществляется посредством маломощных оптических импульсов, содержащих не более десяти фотонов в расчете на каждый бит (символ). Регистрация таких сигналов возможна с помощью высокочувствительных приемных моделей, в качестве которых достаточно часто применяют счетчики фотонов [3].

Однако счетчик фотонов ввиду неидеальности своих технико-эксплуатационных характеристик могут приводить к ошибкам при регистрации данных. Одной из причин таких ошибок может являться ненулевое мертвое время счетчика фотонов – это время, в течение которого приемный модуль не чувствителен к падающему на него оптическому излучению [2, 3]. В результате возникают так называемые «просчеты».

Под просчетом понимается событие, когда на вход счетчика фотонов поступает фотон регистрируемого излучения, однако на его выходе фотон не регистрируется.

В свою очередь, «просчеты» приводят к снижению одной из достаточно важных характеристик квантово-криптографических каналов связи – пропускной способности, которая определяется максимальной скоростью передачи информации [4].

В известных литературных источниках отсутствует оценка влияния скорости счета сигнальных импульсов на выходе счетчика фотонов с мертвым временем на пропускную способность квантово-криптографического канала связи. Целью данной работы являлось выполнение такой оценки.

Объектом исследования являлся асинхронный двоичный несимметричный однородный квантово-криптографический 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 [5, 6]. Мертвым временем продлевающегося типа характеризуются счетчики фотонов на базе лавинных фотоприемников, включенных по схеме пассивного гашения лавины [3].

Предметом исследования являлось установить влияние средней длительности мертвого времени продлевающегося типа на пропускную способность квантово-криптографического канала связи.

1. Выражение для оценки пропускной способности квантово-криптографического канала связи. Дальнейшие рассуждения будут основаны на том, что квантово-криптографический канал связи выполнен с использованием приемо-передающий устройств [7]. Математическая модель этого канала связи построена в работе [4].

Для оценки пропускной способности квантово-криптографического канала связи воспользуемся выражением [4]:

$$\begin{aligned} C_{\max} = \{ & -\left[0{,}5\left(P(0/0)+P(0/1)\right)\right]\times\log_2\left[0{,}5\left(P(0/0)+P(0/1)\right)\right] - \\ & -\left[0{,}5\left(P(1/0)+P(1/1)\right)\right]\times\log_2\left[0{,}5\left(P(1/0)+P(1/1)\right)\right] - \\ & -\left[0{,}5\left(P(-/0)+P(-/1)\right)\right]\times\log_2\left[0{,}5\left(P(-/0)+P(-/1)\right)\right] + \\ & +0{,}5\left[P(0/0)\log_2 P(0/0)+P(1/0)\times\log_2 P(1/0)+P(-/0)\log_2 P(-/0)\right] + \\ & +0{,}5\left[P(0/1)\log_2 P(0/1)+P(1/1)\log_2 P(1/1)+P(-/1)\log_2 P(-/1)\right]\}/\tau_b, \end{aligned} \quad (1)$$

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; τ_b – среднее время передачи одного бита (символа).

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

$$P(0/0)=\sum_{N=N_1}^{N_2}\frac{\left[(n_t+n_{s0})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s0})(\Delta t-\tau_d)\right]}{N!}, \quad (2)$$

$$P(-/0)=\sum_{N=0}^{N_1-1}\frac{\left[(n_t+n_{s0})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s0})(\Delta t-\tau_d)\right]}{N!}, \quad (3)$$

$$P(1/0)=1-P(0/0)-P(-/0), \quad (4)$$

(5)

$$P(0/1)=\sum_{N=N_1}^{N_2}\frac{\left[(n_t+n_{s1})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s1})(\Delta t-\tau_d)\right]}{N!}, \quad (6)$$

$$P(1/1)=1-P(0/1)-P(-/1), \quad (7)$$

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 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, 7].

Темновые и сигнальные – это импульсы, которые появляются на выходе счетчика фотонов соответственно в отсутствии оптического сигнала и в результате воздействия фотонов регистрируемого излучения [3].

Отметим, что для оценки мертвого времени продлевающегося типа используют среднее значение, поскольку его длительность зависит от интенсивности оптического излучения [3].

Таким образом, для оценки пропускной способности рассматриваемого канала связи необходимо в формулу (1) подставить соответствующие выражения (2) ÷ (7) 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.

2 Результаты математического моделирования и их обсуждение. Вычисление пропускной способности выполнялось для квантово-криптографических каналов связи, содержащих в качестве приемного модуля счетчик фотонов при различных значениях n_{s0} и n_{s1} при отсутствии мертвого времени продлевающегося типа, а также при его наличии.

На рисунке 1 представлены зависимости пропускной способности квантово-криптографического канала связи от средней скорости счета сигнальных импульсов при передаче двоичных символов «1» при отсутствии мертвого времени продлевающегося типа, а также при его наличии.

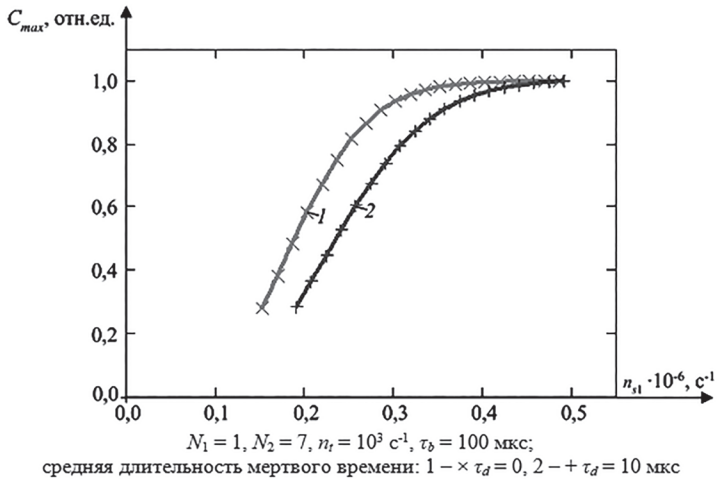

Рисунок 1. Зависимости пропускной способности канала связи от средней скорости счета сигнальных импульсов при передаче двоичных символов «1»

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 [6]. Для сравнения полученных зависимостей $C_{\max}(n_{s1})$ величины средних скоростей счета сигнальных импульсов n_{s0} фиксировались постоянными и выбирались по методике [5]. 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 N_1 и N_2 следует фиксировать постоянными, как и среднее значение скорости счета темновых импульсов n_t и среднее время передачи одного бита (символа) τ_b [5, 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 аналогично представленному на рисунке 1.

Как видно из полученных результатов, с ростом средней скорости счета сигнальных импульсов при передаче двоичных символов «1» пропускная способность канала связи увеличивается вплоть до насыщения, что наблюдается как при наличии мертвого времени продлевающегося типа (см. рисунок 1, кривая 2), так и при его отсутствии (см. рисунок 1, 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 $n_{s1} \geq 43{,}7 \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс. Такие особенности поведения зависимостей $C_{\max}(n_{s1})$ объ-

ясняются характером изменения достоверности принятых данных D с увеличением средних скоростей счета сигнальных импульсов n_{s1} и средней длительности мертвого времени продлевающегося типа [6].

Под достоверностью будем понимать вероятность того, что принятые данные соответствуют переданным [6].

В исследуемых диапазонах значений средних скоростей счета сигнальных импульсов с увеличением n_{s1} достоверность принятых данных D также увеличивается, достигая насыщения. Повышение достоверности принятых данных D приводит к снижению условной энтропии $H(B/A)$ и к росту пропускной способности исследуемого канала связи. Это объясняется следующим. 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 того, что на выходе канала связи будет зарегистрирован символ «0», в то время, когда на вход канала связи подается символа «1», максимальна. В этом случае переходная вероятность $P(0/1)$ также максимальна, что, в свою очередь, не позволяет достигать наибольшего значения переходной вероятности $P(1/1)$. С увеличением n_{s1} происходит сдвиг максимумов статистических распределений $P_{st1}(N)$ в сторону больших значений N, поэтому увеличивается вероятность 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. Таким образом, 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 зависимостей $C_{\max}(n_{s1})$ и $D(n_{s1})$ 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 1) [6].

Как видно из рисунка 1, 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$^{-1}$ пропускная способность $C_{\max}$ равна 0,97 отн.ед. для $\tau_d = 0$; 0,87 отн.ед. для $\tau_d = 10$ 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 [6]. 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 $P(0/1) / P(1/1)$, следовательно, уменьшаются достоверность принятых данных D [6] и пропускная способность канала связи $C_{\max}$.

Для исследуемого канала связи максимальная пропускная способность получена 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 $n_{s0} = 66{,}6 \times 10^3$ с$^{-1}$ и $n_{s1} \geq 35{,}0 \times 10^4$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} = 83{,}5 \times 10^3$ с$^{-1}$ и $n_{s1} \geq 43{,}7 \times \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс.

Заключение

Применительно к асинхронному двоичному несимметричному однородному квантово-криптографическому каналу связи без памяти и со стиранием, содержащем в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа, установлены зависимости пропускной способности от средней скорости счета сигнальных импульсов при передаче двоичных символов «1».

Получено, что с ростом средней скорости счета сигнальных импульсов при передаче двоичных символов «1» пропускная способность канала связи увеличивается вплоть до насыщения, что наблюдается как при наличии мертвого времени продлевающегося типа, так и при его отсутствии. Причем при прочих равных параметрах приема 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 $n_{s1} \geq 43{,}7 \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс.

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. 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.
2. 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. – 391 с.
3. Гулаков, И.Р. Фотоприемники квантовых систем: монография / И.Р. Гулаков, А.О. Зеневич. – Минск: УО ВГКС, 2012. – 276 с.
4. 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.
5. 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.
6. 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.
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.