УДК 621.383

Методика достижения наименьших потерь информации в квантово-криптографическом канале связи с приемником на основе счетчика фотонов

Получено выражение для оценки вклада вероятности стирания двоичных символов «0» в вероятность ошибочной регистрации этих символов для квантово-криптографического канала связи, содержащего в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа. Применительно к такому каналу связи предложена методика выбора нижнего и верхнего пороговых уровней регистрации и интенсивностей регистрируемых оптических излучений при передаче символов «0» и символов «1», которая позволяет достичь наименьших потерь информации.

А.М. ТИМОФЕЕВ,
доцент кафедры защиты информации,
к. т. н., доцент

Белорусский государственный университет информатики и радиоэлектроники

Ключевые слова:
счетчик фотонов, мертвое время продлевающегося типа, вероятность ошибочной регистрации двоичных данных, канал связи.

Введение. В настоящее время одной из основных задач, решаемых при построении систем инфокоммуникаций, является обеспечение скрытности и конфиденциальности передаваемой информации [1–3]. Для этого целесообразно применять каналы квантово-криптографической связи. Такие каналы связи характеризуются абсолютной скрытностью и конфиденциальность передаваемой информации, что выгодно отличает их от других.

Важно отметить, что исключительно высокий уровень информационной безопасности квантово-криптографических каналов связи достигается за счет использования квантово-механического ресурса при кодировании передаваемых данных [3–5]. При этом передача и прием информации осуществляется посредством предельно слабого оптического излучения со средним числом фотонов не более нескольких десятков в расчете на каждый двоичный бит (символ). Регистрация столь слабого оптического излучения возможна с помощью высокочувствительных приемных модулей [3–7]. В этой связи для регистрации данных, передаваемых в квантово-криптографических каналах связи, достаточно часто используют счетчики фотонов, построенные на базе лавинных фотоприемников. Объясняется это тем, что по большинству своих характеристик и других особенностей создания и практического применения счетчики фотонов на базе лавинных фотоприемников превосходят счетчики фотонов на базе фотоэлектронных умножителей, многоканальных усилителей, горячих электронных болометров, сверхпроводящих переходов Джозефсона, сенсоров граничного перехода и квантовых точек [7]. Однако при регистрации данных в квантово-криптографическом канале связи, содержащем в качестве приемного модуля счетчик фотонов на базе лавинного фотоприемника, могут возникать ошибки. Наличие таких ошибок не только уменьшает скорость передачи данных, но и снижает уровень информационной безопасности системы связи в целом [8]. Одной из причин ошибочной регистрации данных в указанных каналах связи могут быть так называемые «просчеты», которые обусловлены, в частности, ненулевым мертвым временем счетчика фотонов, а также квантовой эффективностью регистрации счетчика фотонов, ме́ньшей единицы.

Мертвое время счетчика фотонов – это время, в течение которого счетчик фотонов нечувствителен к падающему на него оптическому излучению [3, 7].

Квантовая эффективность регистрации счетчика фотонов – это отношение числа фотонов оптического излучения, зарегистрированных счетчиком фотонов, к общему числу поступивших фотонов [3, 7].

Важно также отметить, что применительно к квантово-криптографическим каналам связи вероятность ошибочной регистрации данных определяется двумя составляющими [9]. Первая составляющая – вероятность стирания двоичного символа, а вторая – вероятность регистрации разноименных символов.

Вероятность стирания двоичного символа – это вероятность того, что при передаче двоичного символа («0» или «1») на выходе канала связи не будет зарегистрирован ни символ «0», ни символ «1».

Под вероятностью регистрации разноименных символов в случае передачи двоичного символа «0» будем понимать вероятность регистрации на выходе канала связи символа «1» $P(1/0)$, а в случае передачи двоичного символа «1» – вероятность регистрации на выходе канала связи символа «0» $P(0/1)$.

Первая составляющая вероятности ошибочной регистрации данных (вероятность стирания двоичного символа) зависит как от интенсивности регистрируемого оптического излучения, так и от напряжения питания лавинного фотоприемника, и может иметь место не только в случае передачи двоичного символа «0», но и при передаче двоичного символа «1».

Известные методы оценки показателей надежности [1, 10], учитывающие ошибки при передаче информации, не применимы для квантово-криптографических каналов связи. Также в литературных источниках отсутствует оценка вклада вероятности стирания двоичных данных в общую вероятность их ошибочной регистрации применительно к квантово-криптографическому каналу связи, содержащему в качестве приемного модуля счетчик фотонов на базе на базе лавинного фотоприемника. Кроме того, отсутствует методика, позволяющая уменьшить вероятность ошибочной регистрации двоичных данных за счет снижения вероятности стирания двоичных данных.

Объектом исследования являлся асинхронный двоичный несимметричный однородный квантово-криптографический канал связи без памяти и со стиранием, содержащий в качестве приемного модуля счетчик фотонов на базе лавинного фотоприемника ФД-115Л, включенный по схеме пассивного гашения лавины. Выбор в качестве объекта исследования такого канала связи обусловлен тем, что асинхронный способ передачи и приема информации не требует наличия дополнительных линий связи для передачи и приема синхроимпульсов [11]. Схема пассивного гашения лавины имеет ме́ньшую погрешность измерений регистрируемого излучения благодаря отсутствию принудительного гашения лавинного пробоя, что выгодно ее отличает от других схем – активного гашения и импульсного смещения *p-n*-перехода (со стробированием). Фотоприемники ФД-115Л используются для работы в ближнем ИК-диапазоне и за счет применяемого при их изготовлении кремниевого полупроводникового материала характеризуются ме́ньшими шумами, связанными с умножением носителей, и лучшей пороговой чувствительностью по сравнению с германиевыми и галлиевыми фотоприемниками. Также следует отметить, что кремниевые лавинные фотоприемники позволяют реализовывать режим счета фотонов при комнатных температурах [7].

Предметом исследования являлась разработка методики уменьшения потерь информации при ее регистрации в квантово-криптографическом канале связи, учитывающей интенсивность регистрируемого оптического излучения и напряжение питания лавинного фотоприемника.

Целью данной работы являлось разработка методики, обеспечивающей наименьшие потери информации при ее регистрации в квантово-криптографическом канале связи, содержащем в качестве приемного модуля счетчик фотонов.

Математическая модель однофотонного канала связи. Дальнейшие рассуждения будут основаны на том, что канал связи реализован на базе приемопередающих устройств [12]. Вначале построим математическую модель канала связи. Для этого воспользуемся методиками, описанными 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. При регистрации оптического излучения счетчик фотонов подсчитывает количество импульсов N и принимает решение, какой двоичный символ поступил на его вход, используя для этого нижний N_1 и верхний N_2 пороговые уровни регистрации путем проверки условий [12, 15]:

$$N_1 \le N \le N_2, \quad (1)$$

$$N > N_2. \quad (2)$$

Нижний пороговый уровень регистрации – это наименьшее число зарегистрированных на выходе счетчика фотонов импульсов, при котором делается вывод, что передан символ «0». При регистрации импульсов в количестве, ме́ньшем N_1, принимается решение, что символ отсутствует.

Верхний пороговый уровень регистрации – это 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».

Таким образом, ошибочная регистрация данных фиксировалась в следующих случаях:

– если условия (1) или (2) не выполнялись;
– если условие (1) выполнялось, но при этом на входе канала связи двоичный символ «0» отсутствовал;
– если условие (2) выполнялось, но при этом на входе канала связи двоичный символ «1» отсутствовал.

Стирание двоичного символа «0» фиксировалось, если двоичный символ «0» присутствовал на входе канала связи, однако при регистрации оптического излучения счетчиком фотонов подсчитывалось импульсов меньше, чем N_1.

Для оценки вклада вероятности стирания двоичных символов «0» в вероятность ошибочной регистрации этих символов воспользуемся отношением:

где $P(-/0)$ и $P_{ош0}$ – вероятности стирания и ошибочной регистрации двоичных символов «0» 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 данных, τ_d – средняя длительность мертвого времени продлевающегося типа, $P_{st0}(N)$ – статистическое распределение смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации двоичных символов «0».

Вероятность стирания двоичных символов «0» – это вероятность того, что при передаче двоичного символа «0» на выходе канала связи не будет зарегистрирован ни символ «0», ни символ «1» [11].

Отметим, что для оценки мертвого времени продлевающегося типа используют среднее значение, т. к. его длительность зависит от интенсивности оптического излучения [7].

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

Скорость счета темновых импульсов определяется как число импульсов, формирующихся на выходе приемного модуля в единицу времени, когда регистрируемое оптическое излучение отсутствует [7]. Чем большее число темновых импульсов будет образовываться в единицу времени, тем больше вероятности того, что будет принят символ «0» и символ «1» соответственно при отсутствии двоичного символа «0» и при его наличии на входе канала связи. Скорость счета сигнальных импульсов определяется как число импульсов, формирующихся на выходе приемного модуля в единицу времени при воздействии фотонов излучения. Для оценки скоростей счета темновых и сигнальных импульсов используют их средние значения n_t и n_{s0} соответственно [7].

Отношение (3) получено на основании выражений для оценки вероятности ошибочной регистрации данных [9] и статистических распределений [16] применительно к счетчикам фотонов с рассматриваемым типом мертвого времени.

$$\frac{P(-/0)}{P_{ош0}} = \frac{\sum_{N=0}^{N_1-1} \frac{\left[\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]^N \exp\left[-\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]}{N!}}{1 - \sum_{N=N_1}^{N_2} \frac{\left[\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]^N \exp\left[-\left(n_t + n_{s0}\right)\left(\Delta t - \tau_d\right)\right]}{N!}} = \frac{\sum_{N=0}^{N_1-1} P_{st0}(N)}{1 - \sum_{N=N_1}^{N_2} P_{st0}(N)}, \quad (3)$$

Сущность разработанной методики. Методика содержит пять этапов:

1. Формирование массивов данных статистических распределений смеси числа темновых и сигнальных импульсов $P_{st}(N)$ и интенсивностей оптических сигналов J:

$$P_{st}(N) = \left\{ P_{st}(N)^{(1)}, P_{st}(N)^{(2)}, P_{st}(N)^{(i)}, ..., P_{st}(N)^{(m)} \right\}, \quad (4)$$

$$J = \left\{ J^{(1)}, J^{(2)}, J^{(i)}, ..., J^{(m)} \right\}, \quad (5)$$

где $P_{st}(N)^{(i)}$ – i-е статистическое распределение смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов, соответствующее i-й интенсивности оптического сигнала $J^{(i)}$, $i = 2 \div m$ (m определяется объемом накопленных данных числа импульсов).

Статистические распределения $P_{st}(N)$ и интенсивности J могут быть получены с использованием установки, описанной в [12].

По мере реализации методики итерационно определяют величины i_0, i_1, N_1, N_2 и K_P, а также i_0', i_1', N_1', N_2' и K_P' следующим образом. Вначале устанавливают $i_0 = 1$, $i_1 = 2$, $N_1 = 1$, $K_P' = 10^3$. Затем переходят к этапу 2.

2. Определение интенсивности оптического сигнала для передачи двоичных символов «0». Если $i_0 < m$, то устанавливают $P_{st0}(N) = P_{st}(N)^{(i_0)}$ и переходят к этапу 3; иначе завершают выполнение методики.

3. Определение интенсивности оптического сигнала для передачи двоичных символов «1». Если $i_1 \le m$, то устанавливают $P_{st1}(N) = P_{st}(N)^{(i_1)}$ и переходят к этапу 4; иначе последовательно устанавливают $K_P' = 10^3$, увеличивают на единицу i_0, устанавливают $i_1 = i_0 + 1$ и переходят к этапу 2.

4. Определение нижнего порогового уровня зарегистрированных на выходе счетчика фотонов импульсов N_1, при котором делается вывод, что передан символ «0». Если $N_1 < 10$, то устанавливают $N_2 = N_1 + 1$ и переходят к этапу 5; иначе последовательно устанавливают $N_1 = 1$, увеличивают на единицу i_1 и переходят к этапу 3.

5. Определение верхнего порогового уровня зарегистрированных на выходе счетчика фотонов импульсов N_2, при превышении которого делается вывод, что передан символ «1». Если $N_2 > 10$, то увеличивают на единицу значение N_1 и переходят к этапу 4; иначе последовательно выполняют следующие действия:

– по формуле (5) вычисляют:

$$K_P = \frac{1 - \sum_{N=N_1}^{N_2} P_{st0}(N) + \sum_{N=0}^{N_2} P_{st1}(N)}{1 + \sum_{N=N_1}^{N_2} P_{st0}(N) - \sum_{N=0}^{N_2} P_{st1}(N)}, \quad (6)$$

где $P_{st1}(N)$ – статистическое распределение смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации двоичных символов «1»;

– если $K_P < K_P'$, то последовательно устанавливают K_P', равным K_P, и формируют массив данных, содержащий $i_0' = i_0$, $i_1' = i_1$, $N_1' = N_1$, $N_2' = N_2$, а также величины J_0 и J_1, соответствующие статистическим распределениям $P_{st}(N)^{(i_0)}$ и $P_{st}(N)^{(i_1)}$;

– увеличивают на единицу верхний пороговый уровень зарегистрированных на выходе счетчика фотонов импульсов N_2;

– переходят к началу этапа 5.

По окончании реализации методики из массива сформированных данных i_0', i_1', N_1', N_2', J_0 и J_1 выбирают величины N_1' и N_2', используемые соответственно как нижний и верхний пороговые уровни. Значения i_0' и i_1' определяют статистические распределения смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации двоичных символов «0» $P_{st0}(N)$ и двоичных символов «1» $P_{st1}(N)$, а также интенсивности регистрируемых оптических излучений при передаче этих символов J_0 и J_1, соответствующие $P_{st}(N)^{(i_0')}$, $J^{(i_0')}$ и $P_{st}(N)^{(i_1')}$, $J^{(i_1')}$, которые выбирают из массивов данных (4) и (5). Расчет отношения $P(-/0) / P_{out0}$ выполнялся путем подстановки в (3) статистических распределений $P_{st0}(N)$ при выбранных пороговых уровнях зарегистрированных импульсов $N_1 = N_1'$ и $N_2 = N_2'$.

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 оценки вклада вероятности стирания двоичных символов «0» $P(-/0)$ в вероятность ошибочной регистрации этих символов P_{out0}.

Для исследованного канала связи предложена методика выбора нижнего и верхнего пороговых уровней регистрации и интенсивностей регистрируемых оптических излучений при передаче символов «0» J_0 и символов «1» J_1. Данная методика учитывает статистические распределения смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации двоичных символов «0» $P_{st0}(N)$ и двоичных символов «1» $P_{st1}(N)$, что позволяет достичь наименьших потерь информации в квантово-криптографическом канале связи с приемником на основе счетчика фотонов.

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.

Автору настоящей работы видятся весьма важными экспериментальные исследования, направленные на оценку потерь информации в квантово-криптографическом канале связи с приемником на основе счетчика фотонов с мертвым временем продлевающегося типа. Различные технико-эксплуатационные параметры счетчиков фотонов (интенсивности оптических сигналов, используемых для передачи двоичных символов «0» и «1», напряжения питания лавинных фотоприемников и пр.) влияют, в частности, на длительность мертвого времени счетчиков фотонов, следовательно, и на потери информации. В этой связи особый интерес представляет определить, как эти параметры влияют на вероятности стирания двоичных символов «0» и «1», на вероятности ошибочной регистрации этих символов, а также на достоверность принятых данных в целом, что планируется выполнить в ходе дальнейших комплексных исследований.

ЛИТЕРАТУРА

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. **Vacca, J. R.** Managing Information Security. – 2nd Edition / J.R. Vacca. – Elsevier Inc: Waltham, 2014. – 372 p. – Дата доступа: 10.02.22. – Режим доступа: https://doi.org/10.1016/C2011-0-08782-3.
3. **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.
4. **Yiannopoulos K.**, **Sagias N. C.**, **Boucouvalas A. C.** On the photon counting error probability and its application in optical wireless communications. Physical Communication, 2019, vol. 36, pp. 100756–100764. – Дата доступа: 15.03.22. – Режим доступа: https://doi.org/10.1016/j.phycom.2019.100756.
5. 35.88 attenuation lengths and 3.32 bits/photon underwater optical wireless communication based on photon-counting receiver with 256-PPM / S. Hu [et al.] // Optics Express. – 2018. – Vol. 26, № 17. – P. 21685–21699. – Дата доступа: 15.03.22. – Режим доступа: https://doi.org/10.1364/OE.26.021685.
6. **Cova S. D.**, **Ghioni M.** Single-photon counting detectors. IEEE Photonics Journal, 2011, vol. 3, no. 2, pp. 274–277. Дата доступа: 15.03.22. – Режим доступа: https://doi.org/10.1109/JPHOT.2011.2130518.
7. **Гулаков, И. Р.** Фотоприемники квантовых систем: монография / И. Р. Гулаков, А. О. Зеневич. – Минск: УО ВГКС, 2012. – 276 с.
8. **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.
9. **Тимофеев, А. М.** Оценка влияния продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации данных квантово-криптографических каналов связи / А. М. Тимофеев // Вестник связи. – 2018. – № 1. – С. 56–62.
10. **Дмитриев, С. А.** Волоконно-оптическая техника: современное состояние и новые перспективы / С.А. Дмитриев, Н.Н. Слепов. – 3-е изд. – М.: Техносфера, 2010. – 608 с.
11. **Тимофеев, А. М.** Измерение вероятности стирания двоичного символа «0» в однофотонном асинхронном канале связи с приемником на основе счетчика фотонов / А. М. Тимофеев // Приборы и методы измерений. – 2021. – т. 12. – № 2. – С. 156–165. – Дата доступа: 17.03.22. – Режим доступа: https://doi.org/10.21122/2220-9506-2021-12-2-156-165.
12. **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.
13. **Клюев, Л. Л.** Теория электрической связи: учебник / Л. Л. Клюев. – Минск: Техноперспектива, 2008. – 423 с.
14. **Биккенин, Р. Р.** Теория электрической связи / Р. Р. Биккенин, М. Н. Чесноков. – М.: Издательский цент «Академия», 2010. – 336 с.
15. **Тимофеев, А. М.** Оценка влияния интенсивности оптического сигнала на вероятность ошибочной регистрации данных в однофотонном канале связи / А. М. Тимофеев // Информатика. – 2021. – т. 18. – № 2. – С. 72–82. – Дата доступа: 15.03.22. – Режим доступа: https://doi.org/10.37661/1816-0301-2021-18-2-72-82.
16. **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.

An expression for estimating the contribution of the probability of erasing binary symbols «0» to the probability of erroneous registration of these symbols has been obtained. It can be used for a quantum cryptographic communication channel containing as a receiving module a photon counter with a dead time of an extending type. For such a communication channel, methodology for selecting the lower and upper threshold levels of registration and intensities of detected optical radiation during the transmission of symbols «0» and symbols «1» has been developed. This methodology allows to achieve the least loss of information.

Key words: *photon counter, dead time of the prolonging type, probability of erroneous registration of binary data, communication channel.*

Получено 07.04.2022.