УДК 621.383
DOI: 10.21122/2309-4923-2022-2-62-65

*А. М. ТИМОФЕЕВ*

# ОЦЕНКА ВЛИЯНИЯ ВЕРОЯТНОСТИ СТИРАНИЯ ДВОИЧНЫХ СИМВОЛОВ «0» НА ВЕРОЯТНОСТЬ ОШИБОЧНОЙ РЕГИСТРАЦИИ ДАННЫХ В КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ

*Белорусский государственный университет информатики и радиоэлектроники*

*Получено выражение для оценки отношения вероятности стирания двоичных символов «0» P(–/0) к вероятности ошибочной этих символов $P_{ош0}$ применительно к асинхронному квантово-криптографическому каналу связи, в котором в качестве приемного модуля используется счетчик фотонов с мертвым временем продлевающегося типа. По результатам математического моделирования установлены зависимости отношения P(–/0) / $P_{ош0}$ от средней скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» $n_{s0}$ для различной средней длительности мертвого времени продлевающегося типа $\tau_d$. Выполненные исследования показали, что с ростом $n_{s0}$ эти зависимости вначале практически не изменяются и имеют значения, близкие к единице, однако затем спадают вплоть до наименьших значений и переходят в насыщение, что имеет место как при отсутствии мертвого времени продлевающегося типа, так и при его наличии.*

***Ключевые слова:*** *счетчик фотонов; мертвое время; квантово-криптографический канал связи.*

## Введение

В настоящее время одной из основных задач при создании инфокоммуникационных систем и каналов связи различного назначения является обеспечение их информационной безопасности [1]. Для этого применяют, как правило, комплекс мер, включая криптографические и криптоподобные преобразования передаваемой информации [2]. Важно отметить также, что применение квантово-криптографических каналов связи позволяет обеспечить абсолютную скрытность и конфиденциальность данных. Это является безусловным преимуществом использованием этих каналов связи, в сравнении с другими [2]. Однако при создании квантово-криптографических каналов связи существует ряд проблем практического характера. В частности, одной из проблем является значительно ме́ньшая пропускная способность, чем для стандартных инфокоммуникационных каналов связи. Связано это с трудностью не только формирования и передачи маломощных оптических импульсов, используемых в квантово-криптографических каналах связи, но и их регистрацией [2, 3].

Под маломощными оптическими импульсами будем понимать оптические импульсы, среднее число фотонов в которых не превышает десяти на каждый передаваемый бит (или символ).

Для регистрации маломощных оптических импульсов целесообразно использовать высокочувствительные приемные модули, такие, как счетчики фотонов [4]. Однако счетчики фотонов характеризуются ненулевым мертвым временем, что является одной из причин возникновения ошибок в квантово-криптографическом канале связи и приводит к потерям передаваемой информации, в результате снижая его пропускную способность.

Мертвое время – это время, в течение которого счетчик фотонов не чувствителен к падающему на него оптическому излучению [4].

Одной из составляющих вероятности ошибок является вероятность стирания двоичных символов [5].

Поскольку до настоящего времени оценка влияния вероятности стирания двоичных символов на вероятность ошибочной регистрации данных в квантово-криптографическом канале связи не выполнялась, то это являлось целью данной работы.

Объектом исследования являлся асинхронный квантово-криптографический канал связи, в котором в качестве приемного модуля использовался счетчик фотонов с мертвым временем продлевающегося типа. Мертвым временем продлевающегося типа характеризуются счетчики фотонов на базе лавинных фотоприемников, включенные по схеме пассивного гашения лавины [2 – 5].

Предметом исследования является установление влияния вероятности стирания двоичных символов «0» на вероятность ошибочной регистрации данных.

## Математическая модель канала связи

В начале получим выражение для оценки влияния вероятности стирания двоичных символов «0» на вероятность ошибочной регистрации данных в квантово-криптографическом канале связи, содержащем в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа. Дальнейшие рассуждения будут основаны на том, что исследуемый канал связи построен на базе приемо-передающего оборудования [6], в котором данные передаются двоичными символами «0» в течение длительности времени $\tau_b$. Для передачи этих символов используются оптические сигналы, содержащие не более десяти фотонов на каждый бит (символ). Причем трансляция этих сигналов в канал связи осуществляется в течение длительности времени однофотонной передачи $\Delta t = \tau_b /2$. Следовательно, в течение времени $t_з = \tau_b /2$ данные в канал связи не передаются, т.е. между каждой парой символов находится так называемый «защитный» временной интервал. Всеми потерями информации, за исключением потерь в счетчике фотонов, пренебрегаем.

В этом случае вероятность ошибочной регистрации данных квантово-криптографического канала связи равна [5]:

$$P_{iø\ 0} = 1 + \sum_{N=0}^{N_1-1} P_{st0}(N) - \sum_{N=0}^{N_2} P_{st0}(N) = P(-/0) + P(1/0), \quad (1)$$

где $P_{st0}(N)$ – статистическое распределение смеси числа темновых и сигнальных импульсов на выходе

счетчика фотонов при регистрации двоичных символов «0», $P(-/0)$ – вероятность стирания двоичных символов «0», $P(1/0)$ – вероятность регистрации на выходе канала связи символов «1» при наличии на входе канала связи символов «0», $N_1$ и $N_2$ – нижний и верхний пороговые уровни регистрации соответственно.

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, ме́ньшем, чем $N_1$, принимается решение, что символ отсутствует [5, 6].

Для оценки влияния вероятности стирания двоичных символов «0» на вероятность ошибочной регистрации данных воспользуемся отношением:

$$\frac{P(-/0)}{P_{i\phi\ 0}} = \frac{\sum_{N=0}^{N_1-1} \frac{[(n_t+n_{s0})(\Delta t-\tau_d)]^N \exp[-(n_t+n_{s0})(\Delta t-\tau_d)]}{N!}}{1-\sum_{N=N_1}^{N_2} \frac{[(n_t+n_{s0})(\Delta t-\tau_d)]^N \exp[-(n_t+n_{s0})(\Delta t-\tau_d)]}{N!}}, \quad (2)$$

где $n_t$ – средняя скорость счета темновых импульсов на выходе счетчика фотонов, $n_{s0}$ – средняя скорость счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0», $\Delta t$ – среднее время однофотонной передачи, $\tau_d$ – средняя длительность мертвого времени продлевающегося типа.

Темновые и сигнальные – это импульсы, которые появляются на выходе счетчика фотонов соответственно в отсутствии оптического сигнала и в результате воздействия фотонов регистрируемого излучения [2, 4].

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

Выражение (2) получено на основе (1) и формул статистических распределений смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации двоичных символов «0» [7] применительно к асинхронному однородному квантово-криптографическому канала связи без памяти и со стиранием, исходя из следующих соображений. Вероятность стирания двоичных символов «0» $P(-/0)$ определяется вероятностью того, что при наличии на входе канала связи символов «0» на его выходе не будет зарегистрировано ни символа «0», ни символа «1». Следовательно, число зарегистрированных на выходе счетчика фотонов импульсов будет находиться в диапазоне $[0, N_1 - 1]$.

Таким образом, наибольший вклад вероятности стирания двоичных символов «0» $P(-/0)$ в величину вероятности ошибочной регистрации данных $P_{ou0}$ будет иметь место при выполнении условия

$$\frac{P(-/0)}{P_{i\phi\ 0}} \geq 0{,}5. \quad (3)$$

## Результаты математического моделирования и их обсуждение

Отношение $P(-/0) / P_{ou0}$ вычислялось для каналов связи, содержащих в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа при различных значениях $\tau_d$ и $n_{s0}$.

На рис. 1 представлены зависимости отношения $P(-/0) / P_{ou0}$ от средней скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» для различной средней длительности мертвого времени продлевающегося типа.

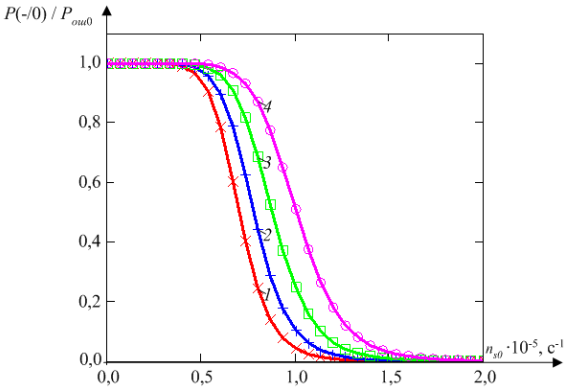


Рис. 1. – Зависимость отношения $P(-/0) / P_{ou0}$ от средней скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0»: $N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, $\tau_b = 100$ мкс; средняя длительность мертвого времени: 1 – × $\tau_d = 0$, 2 – + $\tau_d = 5$ мкс, 3 – □ $\tau_d = 10$ мкс, 4 – ○ $\tau_d = 15$ мкс

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 отметить, что пороговые уровни регистрации можно выбирать и другими, отличными от 1 и 7, но при сравнении зависимостей $P(-/0) / P_{ou0}$ от $n_{s0}$ 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) $\tau_b$. При этом важно учитывать, что $\tau_d$ не может превышать $\Delta t$, которое, в свою очередь, должно быть меньше средней длительности передачи одного бита (символа) $\tau_b$ на величину защитного временного интервала (см. работу [6]); в противном случае использование счетчиков фотонов для регистрации данных становится невозможным. Отметим, что при других значениях $N_1$ и $N_2$, и отношениях $\tau_d/\Delta t$ и $n_t/n_{s0}$ проявление эффекта мертвого времени продлевающегося типа для рассматриваемого канала связи аналогично представленному на рис. 1.

Как видно из полученных результатов, с увеличением средней скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» $n_{s0}$ отношение $P(-/0) / P_{ou0}$ вначале практически не меняется и имеет значения, близкие к единице. Однако при дальнейшем росте $n_{s0}$ наблюдается спад зависимо-

стей $P(-/0)$ / $P_{ош0}$ от $n_{s0}$ вплоть до наименьших значений. Это имеет место как при отсутствии мертвого времени продлевающегося типа (см. рис. 1, кривая 1), так и при его наличии (см. рис. 1, кривые 2 ÷ 4). Это объясняется следующим.

При $n_{s0} = 0$ максимум распределения $P_{st0}(N)$ соответствует значению $N = 0$ [7]. Следовательно, вероятность того, что при наличии на входе канала связи символов «0» на его выходе не будет зарегистрировано ни символа «0», ни символа «1», равна единице. Таким образом, $P(-/0) = P_{ош0}$, следовательно, $P(-/0) / P_{ош0} = 1$.

С увеличением $n_{s0}$ вероятность регистрации импульсов в количестве $N_1 \div N_2$ растет за счет сдвига $P_{st0}(N)$ в сторону бóльших значений $N$ [7]. При этом вероятность регистрации на выходе счетчика фотонов импульсов в количестве, превышающем верхний пороговый уровень регистрации $N_2$, остается весьма малой, поэтому вероятность $P(1/0) \approx 0$. В результате вероятность ошибочной регистрации данных $P_{ош0}$ исследуемого канала связи уменьшается приблизительно на ту же величину, что и вероятность стирания двоичных символов «0» $P(-/0)$. Таким образом, в указанном диапазоне значений средних скоростей счета сигнальных импульсов $n_{s0}$ вероятности $P(-/0) \approx P_{ош0}$, поэтому отношение $P(-/0) / P_{ош0}$ практически не меняется и имеет значения, близкие к единице (см. рис. 1).

При дальнейшем росте $n_{s0}$ максимум распределения $P_{st0}(N)$ продолжает смещаться в сторону еще бóльших значений $N$, достигая и затем превышая верхний пороговый уровень регистрации $N_2$. Это увеличивает вероятность того, что на выходе счетчика фотонов будет зарегистрировано импульсов больше, чем верхний пороговый уровень регистрации $N_2$. Вместе с тем, вероятность $P(-/0)$, продолжая уменьшаться, достигает значения, близкого к нулю, после чего переходит в насыщение. Однако вероятность $P(1/0)$ начинает расти вплоть до своего наибольшего значения, также переходя в насыщение. В результате в таком диапазоне значений $n_{s0}$ вероятность ошибочной регистрации данных $P_{ош0}$ исследуемого канала связи растет приблизительно на ту же величину, на которую увеличивается вероятность регистрации на выходе канала связи символов «1» при наличии на входе канала связи символов «0» $P(1/0)$, поэтому отношение $P(-/0) / P_{ош}$ уменьшается и, достигнув своего минимального значения, тоже переходит в насыщение.

Из полученных результатов также видно, что при других прочих равных параметрах приема рост средней длительности мертвого времени продлевающегося типа приводит к увеличению средних скоростей счета сигнальных импульсов $n_{s0}$, при которых зависимости $P(-/0) / P_{ош0}$ от $n_{s0}$ начинают спадать и при которых эти зависимости переходят в насыщение (см. рис. 1). Так, например, уменьшение зависимостей $P(-/0) / P_{ош0}$ от $n_{s0}$ вплоть до насыщения, определяемое по 95%-ному и 5%-ному отклонению отношения $P(-/0) / P_{ош0}$ от его максимального значения для соответствующего мертвого времени продлевающегося типа, наблюдалось при $0{,}49 \times 10^{-5}$ с$^{-1} \le n_{s0} \le 0{,}99 \times 10^{-5}$ с$^{-1}$ для $\tau_d = 0$; при $0{,}55 \times 10^{-5}$ с$^{-1} \le n_{s0} \le 1{,}10 \times 10^{-5}$ с$^{-1}$ для $\tau_d = 5$ мкс; при $0{,}62 \times 10^{-5}$ с$^{-1} \le n_{s0} \le 1{,}23 \times 10^{-5}$ с$^{-1}$ для $\tau_d = 10$ мкс; при $0{,}71 \times 10^{-5}$ с$^{-1} \le n_{s0} \le 1{,}41 \times 10^{-5}$ с$^{-1}$ для $\tau_d = 15$ мкс. Объясняется это тем, что при увеличении $\tau_d$ максимумы статистических распределений $P_{st0}(N)$ сдвигаются в сторону меньших значений $N$ [7]. Это приводит к уменьшению вероятности стирания двоичных символов «0» $P(-/0)$, поэтому рост средней длительности мертвого времени продлевающегося типа приводит к увеличению средних скоростей счета сигнальных импульсов $n_{s0}$, при которых указные спады зависимостей $P(-/0) / P_{ош0}$ от $n_{s0}$ не только начинают проявляться, но при которых эти зависимости переходят в насыщения. По этим же причинам при других равных параметрах приема в диапазонах средних скоростей счета сигнальных импульсов $n_{s0}$, на которых зависимости отношений $P(-/0) / P_{ош0}$ от $n_{s0}$ спадают, рост средней длительности мертвого времени продлевающегося типа приводит к увеличению отношения $P(-/0) / P_{ош0}$. Так, например, при $n_{s0} = 0{,}80 \times 10^{-5}$ с$^{-1}$ отношение $P(-/0) / P_{ош0}$ составляет при 0,24 для $\tau_d = 0$; при 0,44 для $\tau_d = 5$ мкс; при 0,69 для $\tau_d = 10$ мкс; при 0,87 для $\tau_d = 15$ мкс.

Также важно отметить, что для исследуемого канала связи наибольший вклад вероятности стирания двоичных символов «0» $P(-/0)$ в величину вероятности ошибочной регистрации данных $P_{ош0}$, определяемый при выполнении условия (3), имел место при $n_{s0} \le 0{,}70 \times 10^{-5}$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} \le 0{,}78 \times 10^{-5}$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s0} \le 0{,}88 \times \times 10^{-5}$ с$^{-1}$ для $\tau_d = 10$ мкс; при $n_{s0} \le 1{,}00 \times 10^{-5}$ с$^{-1}$ для $\tau_d =$ 15 мкс.

## Заключение

Получено выражение для оценки влияния вероятности стирания двоичных символов «0» $P(-/0)$ на вероятность ошибочной этих символов $P_{ош0}$ применительно к асинхронному квантово-криптографическому каналу связи, в котором в качестве приемного модуля используется счетчик фотонов с мертвым временем продлевающегося типа.

Установлены зависимости отношения $P(-/0) / P_{ош0}$ от средней скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» $n_{s0}$ для различной средней длительности мертвого времени продлевающегося типа $\tau_d$. Выполненные исследования показали, что для исследуемого канала связи наибольший вклад вероятности стирания двоичных символов «0» $P(-/0)$ в величину вероятности ошибочной регистрации данных $P_{ош0}$, определяемый при выполнении условия $P(-/0) / P_{ош0} \ge 0{,}5$, имел место при $n_{s0} \le 0{,}70 \times 10^{-5}$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} \le 0{,}78 \times 10^{-5}$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s0} \le 0{,}88 \times \times 10^{-5}$ с$^{-1}$ для $\tau_d = 10$ мкс; при $n_{s0} \le 1{,}00 \times 10^{-5}$ с$^{-1}$ для $\tau_d =$ 15 мкс.

## 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. **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. **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.

4. **Гулаков, И. Р., Зеневич А.О.** Фотоприемники квантовых систем: монография / И.Р. Гулаков, А.О. Зеневич. – Минск: УО ВГКС, 2012. – 276 с.

5. **Тимофеев, А. М.** Методика снижения потерь информации в асинхронном двоичном однофотонном канале связи с приемником на основе счетчика фотонов / А.М. Тимофеев // Приборы и методы измерений. – 2020. – т. 11. – № 1. – С. 70–81.

6. **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.

7. **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.

## REFERENCES

1. **Scheglov A. Yu.** [Analysis and design of information systems protection. Control of access to computer resources: methods, models, technical solutions]. *Analiz i proektirovanie zaschityi informatsionnyih sistem. Kontrol dostupa k kompyuternyim resursam: metodyi, modeli, tehnicheskie resheniya*. – St. Petersburg: Professional literature, 2017, 416 p. (in Russian).

2. **Kilin S. Ya.** [Quantum cryptography: ideas and practices]. *Kvantovaya kriptografiya: idei i praktika*. – Minsk: Belarus. Sci, 2007, 391 p. (in Russian).

3. T**imofeev A. M.** [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]. *Trudyi BGTU* [Proceedings of BSTU], 2019, no 2. – P. 79–86 (in Russian).

4. **Gulakov I. R., Zenevich A. O.** [Photodetectors of quantum systems: monograph]. *Fotopriemniki kvantovyih sistem: monografiya*. – Minsk: EI HSCC, 2012, 276 p. (in Russian).

5. **Timofeev A. M.** [Method of Achieving the Least Loss of Information in an Asynchronous Binary Single-Photon Communication Channel with a Receiver Based on a Photon Counter]. *Priboryi i metodyi izmereniy* [Devices and methods of measurements], 2020. – Vol. 11, no 1. – P. 70–81 (in Russian).

6. **Timofeev A. M.** [Device for binary data transmitting and receiving over a fiber-optic communication channel]. *Priboryi i metodyi izmereniy* [Devices and methods of measurements], 2018. – Vol. 9. – № 1, pp. 17–27 (in Russian).

7. **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. – P. 90–98 (in Russian).

*A.M. TIMOFEEV*

# EVALUATION OF THE INFLUENCE OF THE PROBABILITY OF ERASING BINARY SYMBOLS “0” ON THE PROBABILITY OF ERRONEOUS DATA REGISTRATION IN A QUANTUM-CRYPTOGRAPHIC COMMUNICATION CHANNEL

*Belarusian State University of Informatics and Radioelectronics*

*An asynchronous quantum-cryptographic communication channel with a receiving module based on a pho-ton counter with a dead time of an extending type was investigated. An expression for estimating the ratio of the probability of erasing binary symbols “0” P(–/0) to the probability of these symbols being erroneous Perr0 has been obtained. Based on the results of mathematical modeling, the dependences of the ratio P(–/0) / Perr0 on the average count rate of signal pulses at the output of the photon counter during the transmission of symbols “0” ns0 for vari-ous average duration of dead time of the extended type τd were established. The performed studies have shown that with an increase in ns0, these dependences at first practically do not change and have values close to unity, but then they drop down to the lowest values and go into saturation. This takes place both in the absence of a dead time of the prolonging type, and in its presence.*

***Keywords:*** *photon counter; dead time; quantum cryptographic communication channel.*

**Тимофеев Александр Михайлович,** кандидат технических наук, доцент, доцент кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники, г. Минск, Республика Беларусь.

**Timofeev A. M.,** Candidate of Technical Sciences, Associate Professor, Associate Professor of the Information Security Department of the Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus.