УДК 621.383.92
DOI: 10.17277/vestnik.2019.01.pp.036-046

# ВЛИЯНИЕ ВРЕМЕНИ ОДНОФОТОННОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ВЕРОЯТНОСТЬ ОШИБОЧНОЙ РЕГИСТРАЦИИ ДАННЫХ АСИНХРОННЫХ КВАНТОВО-КРИПТОГРАФИЧЕСКИХ КАНАЛОВ СВЯЗИ

**А. М. Тимофеев**

*Кафедра защиты информации, УО «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь; tamvks@mail.ru*

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

**Аннотация:** Определены выражения для оценки вероятностей ошибочной регистрации двоичных данных квантово-криптографического канала связи, содержащего счетчик фотонов с мертвым временем продлевающегося типа. По результатам математического моделирования установлены зависимости вероятностей ошибочной регистрации данных на выходе канала связи от среднего времени однофотонной передачи символов «0» и «1», на основе которых обоснован выбор наименьшего среднего времени передачи одного бита (символа), обеспечивающего наименьшие потери передаваемой информации. Полученные результаты позволяют повысить достоверность определения несанкционированного доступа к информации, передаваемой по дискретному двоичному асинхронному однородному квантово-криптографическому каналу связи без памяти и со стиранием.

## Введение

В последнее время широкое применение находят квантово-криптографические системы связи, которые обеспечивают абсолютную конфиденциальность передаваемой информации за счет использования маломощных оптических импульсов. Среднее число фотонов в каждом таком импульсе составляет не более десяти [1 – 3]. Однако современные квантово-криптографические системы связи не позволяют достигать высоких скоростей передачи данных вследствие достаточно большого числа ошибок при регистрации маломощных оптических импульсов [4]. Одной из причин этого является то, что для достижения высокой скорости передачи информации необходимо сокращать среднее время передачи одного бита (символа), а оно ограничено снизу, в частности, быстродействием приемного оборудования, в качестве которого достаточно часто применяют наиболее чувствительные приемные модули – счетчики фотонов [1, 3 – 7]. 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 [8, 9]. На сегодняшний момент оценка влияния времени однофотонной передачи информации на вероятность ошибочной регистрации данных квантово-криптографических каналов связи, содержащих в качестве приемного модуля счетчик фотонов с мертвым временем, не выполнялась, это являлось целью данной работы.

Объект исследования – дискретный двоичный асинхронный однородный квантово-криптографический канал связи без памяти и со стиранием, 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 [1]. Мертвым временем продлевающегося типа характеризуются счетчики фотонов на базе лавинных фотоприемников, включенных по схеме пассивного гашения лавины [10].

В проводимых исследованиях необходимо установить влияние среднего времени однофотонной передачи информации на потери передаваемой информации и вероятность ошибочной регистрации данных квантово-криптографических каналов связи.

## Оценка вероятностей ошибочной регистрации данных

Вначале получим выражения для расчета вероятностей ошибочной регистрации символов «0» и «1», передаваемых по квантово-криптографическим каналам связи. Дальнейшие рассуждения будут основаны на том, что передача информации осуществляется с использованием дискретного двоичного асинхронного однородного квантово-криптографического канала связи без памяти и со стиранием, математическая модель которого может быть получена по методике, показанной в работе [11]. Всеми потерями информации, за исключением потерь в счетчике фотонов, пренебрегаем.

На основании выражений для оценки вероятности ошибочной регистрации данных и статистических распределений, полученных в работах [10 – 14], применительно к счетчикам фотонов с рассматриваемым типом мертвого времени запишем выражения для вероятностей ошибочной регистрации символов «0» и «1» соответственно:

$$P_{\text{ош}0} = 1 - \sum_{N=N_1}^{N_2} \frac{\left[(n_t + n_{s0})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s0})(\Delta t - \tau_d)\right]}{N!}; \quad (1)$$

$$P_{\text{ош}1} = \sum_{N=0}^{N_2} \frac{\left[(n_t + n_{s1})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s1})(\Delta t - \tau_d)\right]}{N!}, \quad (2)$$

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; $\Delta t$ – среднее время однофотонной передачи; $\tau_d$ – 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 [10].

Темновые и сигнальные импульсы появляются на выходе счетчика фотонов соответственно в отсутствии оптического сигнала и в результате воздействия фотонов регистрируемого излучения [10, 11].

Нижний и верхний пороговые уровни регистрации – 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», при регистрации импульсов в количестве, меньшем, чем $N_1$, принимается решение, что символ отсутствует.

Выражения (1) и (2) получены из следующих соображений. При подаче на вход счетчика фотонов регистрируемого излучения на его выходе формируется смесь темновых и сигнальных импульсов. Статистические распределения этих импульсов при наличии на входе счетчика фотонов ослабленного оптического излучения соответствуют распределению Пуассона [10, 11] и определяют выбор нижнего и верхнего пороговых уровней регистрации $N_1$ и $N_2$, по аналогии с выбором порогового уровня, приведенного в [14, 15]. Причем для рассматриваемого канала связи при передаче символов «0» и «1» используются оптические сигналы мощностью $P_1$ и $P_2$ ($P_1 < P_2$), которые транслируются в течение длительности времени $\Delta t$. Поскольку символы «0» и «1» передаются импульсами различной мощности, то на выходе счетчика фотонов за время $\Delta t$ формируется различное число электрических импульсов, прямо пропорциональное мощности оптического излучения. Поэтому число импульсов, соответствующее символу «0», будет меньше, чем число импульсов, соответствующее символу «1».

Каждая из вероятностей $P_{\text{ош}0}$ и $P_{\text{ош}1}$ имеет две составляющие. Первая определяет вероятность того, что при приеме оптического излучения счетчиком фотонов будет зарегистрировано импульсов меньше, чем нижний пороговый уровень, а вторая составляющая для $P_{\text{ош}0}$ и $P_{\text{ош}1}$ соответственно – вероятность того, что при наличии на входе счетчика фотонов оптических сигналов мощностью $P_1$ и $P_2$ на его выходе будет зарегистрировано импульсов больше, чем верхний пороговый уровень, и в диапазоне $N_1$ … $N_2$. Вероятности регистрации символов «0» и «1» при наличии на входе канала связи символов «0» и «1» равны соответственно $(1 - P_{\text{ош}0})$ и $(1 - P_{\text{ош}1})$.

На основании представленных рассуждений можно сделать вывод, что выражения (1) и (2) пригодны для определения вероятностей ошибочной регистрации двоичных данных для рассматриваемого квантово-криптографического канала связи при соблюдении указанных выше ограничений.

## Результаты моделирования и их обсуждение

Вычисления вероятностей ошибочной регистрации двоичных символов выполнялись для каналов связи, содержащих в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа при различных значениях $\tau_d$, $n_{s0}$ и $n_{s1}$.

На рисунке 1 представлены зависимости вероятностей ошибочной регистрации двоичных символов от среднего времени однофотонной передачи для различной средней длительности мертвого времени продлевающегося типа. 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 среднем времени передачи одного бита (символа) $\tau_b = 100$ мкс как при исследовании зависимости $P_{\text{ош}0}(\Delta t)$, так и при исследовании зависимости $P_{\text{ош}1}(\Delta t)$. Необходимо отметить, что пороговые уровни регистрации можно выбирать и другими, отличными от 1 и 7, но при сравнении значений $P_{\text{ош}0}(\Delta t)$ и $P_{\text{ош}1}(\Delta t)$ 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) $\tau_b$. Диапазон значений $\Delta t$, на котором исследованы зависимости $P_{\text{ош}0}(\Delta t)$ и $P_{\text{ош}1}(\Delta t)$, выбирался от $\tau_d$ до $\tau_b/2$. Это объясняется тем, 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 временно́го интервала (см. [1]); в противном случае использование счетчиков фотонов для регистрации данных становится невозможным.

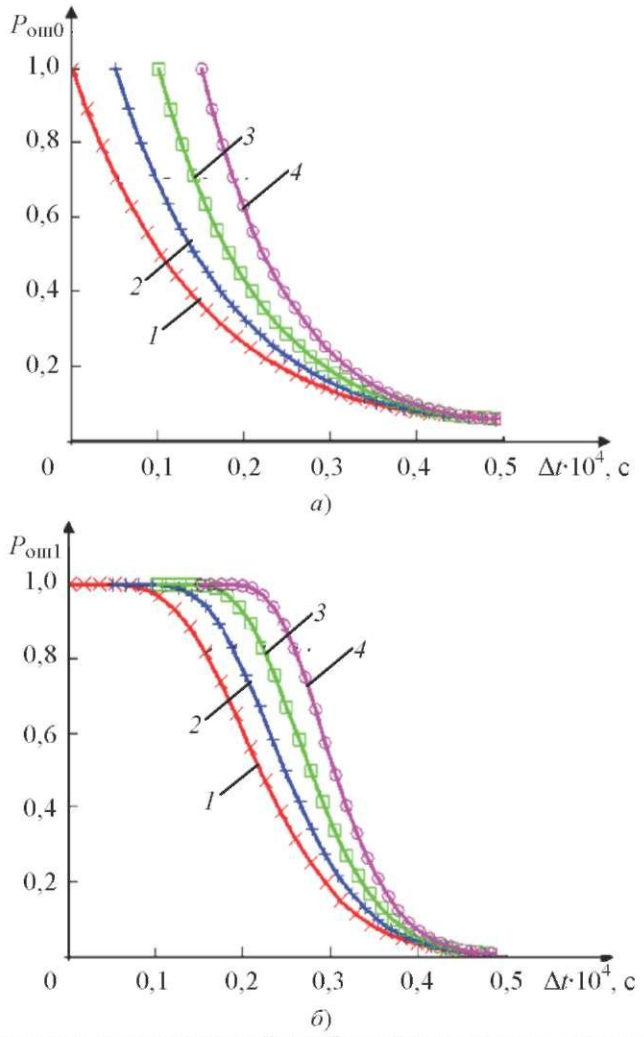


**Рис. 1. Зависимости вероятностей ошибочной регистрации символов «0» (*а*) и «1» (*б*) от среднего времени однофотонной передачи при средней длительности мертвого времени $\tau_d$:**
*1* – 0 мкс; *2* – 5 мкс; *3* – 10 мкс; *4* – 15 мкс

Следует отметить, что при расчете зависимостей, показанных на рис. 1, выбирались оптимальные скорости счета сигнальных импульсов $n_{s0}$ и $n_{s1}$ из диапазона $0…0{,}5 \cdot 10^6$ с$^{-1}$; критерий оптимальности – наименьшее значение скорости счета, при которой вероятность ошибочной регистрации двоичного символа минимальна. Указанный диапазон значений скоростей счета сигнальных импульсов выбран исходя из экспериментальных данных, полученных в работе [10]. При других значениях $N_1$ и $N_2$ и отношениях $\tau_d/\Delta t$, $n_t/n_{s0}$ и $n_t/n_{s1}$ проявление эффекта мертвого времени продлевающегося типа для рассматриваемого канала связи аналогично представленному на рис. 1.

Как видно из рис. 1, с увеличением среднего времени однофотонной передачи вероятность ошибочной регистрации символов «0» $P_{ош0}$ уменьшается во всем исследуемом диапазоне значений $\Delta t$, в то время как для зависимостей $P_{ош1}(\Delta t)$ такой спад наблюдается при $\Delta t \geq 6{,}90$ мкс для $\tau_d = 0$; при $\Delta t \geq 11{,}21$ мкс для

$\tau_d$ = 5 мкс; при $\Delta t \geq 15{,}53$ мкс для $\tau_d$ = 10 мкс; при $\Delta t \geq 19{,}84$ мкс для $\tau_d$ = 15 мкс. Причем рост средней длительности мертвого времени счетчика фотонов при прочих равных параметрах приема приводит к увеличению вероятностей ошибочной регистрации символов «0» и «1» в диапазоне значений $\Delta t$, на котором проявляется спад зависимостей $P_{\text{ош}0}(\Delta t)$ и $P_{\text{ош}1}(\Delta t)$. Указанные особенности поведения зависимостей $P_{\text{ош}0}(\Delta t)$ и $P_{\text{ош}1}(\Delta t)$ объясняются смещением статистических распределений смеси числа темновых и сигнальных импульсов $P_{st0}(N)$ и $P_{st1}(N)$ при передаче символов «0» и «1» соответственно с изменением среднего времени однофотонной передачи и средней длительности мертвого времени продлевающегося типа. Такие распределения могут быть получены на основе соответствующих выражений (1) и (2) по методике, приведенной в [16]. Поскольку для рассматриваемого канала связи проявление эффекта мертвого времени продлевающегося типа и влияние среднего времени однофотонной передачи аналогично как для распределений $P_{st0}(N)$, так и $P_{st1}(N)$, на рис. 2 приведены только статистические распределения смеси числа темновых и сигнальных импульсов при передаче символов «0» $P_{st0}(N)$.

Расчет статистических распределений $P_{st0}(N)$ выполнен для $n_t = 10^3\,\text{с}^{-1}$ и $n_{s0} = 85{,}3 \cdot 10^3\,\text{с}^{-1}$ исходя из тех же соображений, что и при построении рис. 1.

Важно отметить, что представленные на рис. 2 статистические распределения $P_{st0}(N)$ имеют схожий вид с распределениями смеси числа темновых и сигнальных импульсов, экспериментально полученными в работе [11]. Из рисунка 2 видно, что статистические распределения $P_{st0}(N)$ имеют явно выраженный максимум, свойственный для распределения Пуассона, который с увеличением среднего времени однофотонной передачи $\Delta t$ сдвигается в сторону больших значений $N$ как при наличии мертвого времени продлевающегося типа (см. рис. 2, *б*), так и при его отсутствии (см. рис. 2, *а*).

Для рассматриваемого канала связи вероятности приема поступающих на вход счетчика фотонов символов «0» и «1» определяются соответственно вероятностями регистрации импульсов в диапазоне от нижнего до верхнего пороговых уровней и в количестве, превышающем верхний пороговый уровень $N_2$, что видно из формул (1) и (2).

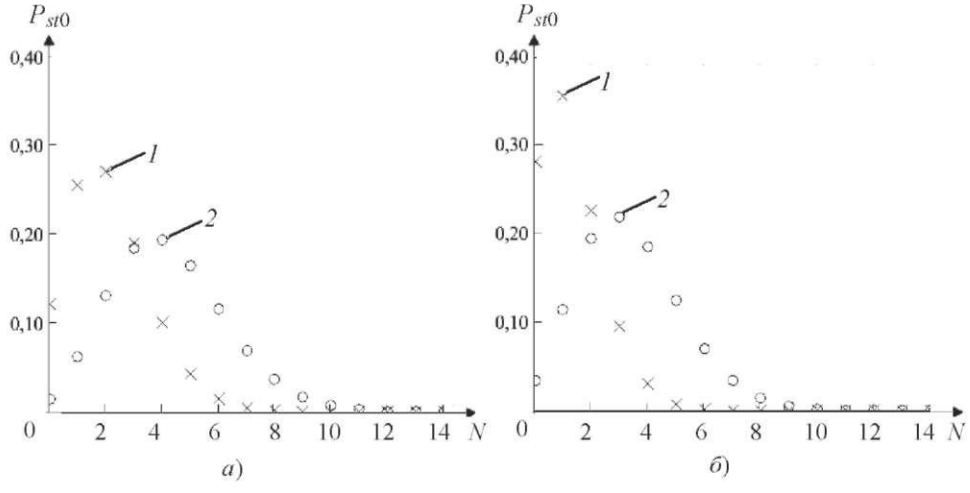


**Рис. 2. Статистические распределения смеси числа темновых и сигнальных импульсов при передаче символов «0» для $\tau_d$ = 0 (*а*) и $\tau_d$ = 10 мкс (*б*) при среднем времени однофотонной передачи $\Delta t$:**
*1* – 25 мкс; *2* – 50 мкс

При $\Delta t = \tau_d$ максимум распределения $P_{st0}(N)$ соответствует значению $N = 0$, то есть вероятность отсутствия импульсов на выходе счетчика фотонов достаточно большая, поэтому $P_{\text{ош}0} = 1$ (см. рис. 1, *а*). Аналогичная ситуация наблюдается и при $\Delta t = \tau_d$ для распределения $P_{st1}(N)$: максимум этого распределения соответствует значению $N = 0$, следовательно, вероятность отсутствия импульсов на выходе счетчика фотонов достаточно большая, поэтому $P_{\text{ош}1} = 1$ (см. рис. 1, *б*).

С увеличением $\Delta t$ вероятность регистрации импульсов в количестве $N_1, \ldots, N_2$ растет за счет сдвига $P_{st0}(N)$ в сторону больших значений $N$ (см. рис. 2), поэтому вероятность ошибочной регистрации символов «0» уменьшается, и на всем исследуемом диапазоне значений $\Delta t$ происходит спад зависимостей $P_{\text{ош}0}(\Delta t)$ (см. рис. 1, *а*). Аналогичный спад с ростом $\Delta t$ имеет место и для вероятности $P_{\text{ош}1}$, который, однако, происходит при более высоких значениях среднего времени однофотонной передачи $\Delta t$, чем для вероятности $P_{\text{ош}0}$. Это объясняется следующим: при приеме символа «1» необходимо зарегистрировать импульсы в количестве, превышающем верхний пороговый уровень $N_2$, что при прочих равных параметрах приема требует большего среднего времени однофотонной передачи, чем в случае регистрации символа «0». По этой причине спад зависимости $P_{\text{ош}1}(\Delta t)$ наблюдается при $\Delta t \geq 6{,}90$ мкс для $\tau_d = 0$; при $\Delta t \geq 11{,}21$ мкс для $\tau_d = 5$ мкс; при $\Delta t \geq 15{,}53$ мкс для $\tau_d = 10$ мкс; при $\Delta t \geq 19{,}84$ мкс для $\tau_d = 15$ мкс (см. рис. 1, *б*).

С ростом мертвого времени продлевающегося типа сокращается среднее время регистрации оптического излучения на величину $\tau_d$, как видно из выражений (1) и (2), поэтому с увеличением $\tau_d$ максимум статистического распределения смеси числа темновых и сигнальных импульсов при передаче символов «0» $P_{st0}(N)$ сдвигается в сторону меньших значений $N$ (см. рис. 2), как и максимум $P_{st1}(N)$ сдвигается в сторону меньших значений $N$. Следовательно, при прочих равных параметрах приема с ростом средней длительности мертвого времени продлевающегося типа вероятности регистрации импульсов на выходе счетчика фотонов в количестве $N_1, \ldots, N_2$ и в количестве, превышающем верхний пороговый уровень, уменьшаются соответственно при передаче символов «0» и символов «1», и $P_{\text{ош}0}$ и $P_{\text{ош}1}$ растут. Так, например, при $\Delta t = 35$ мкс $P_{\text{ош}0}$ и $P_{\text{ош}1}$ равны соответственно $9{,}69 \cdot 10^{-2}$ и $7{,}78 \cdot 10^{-2}$ для $\tau_d = 0$; $10{,}74 \cdot 10^{-2}$ и $10{,}35 \cdot 10^{-2}$ для $\tau_d = 5$ мкс; $12{,}25 \cdot 10^{-2}$ и $14{,}65 \cdot 10^{-2}$ для $\tau_d = 10$ мкс; $14{,}57 \cdot 10^{-2}$ и $21{,}84 \cdot 10^{-2}$ для $\tau_d = 15$ мкс.

В качестве критериев оценки отклонений вероятностей ошибочной регистрации символов «0» и «1», полученных с учетом мертвого времени продлевающегося типа и без него, будем использовать параметры:

$$\sigma_{\text{ош}0} = \sqrt{\frac{\sum_{\Delta t}\left(P_{\text{ош}0} - P'_{\text{ош}0}\right)^2}{N_{\Delta t}}}; \qquad \sigma_{\text{ош}1} = \sqrt{\frac{\sum_{\Delta t}\left(P_{\text{ош}1} - P'_{\text{ош}1}\right)^2}{N_{\Delta t}}}, \tag{3}$$

где $P_{\text{ош}0}$ и $P'_{\text{ош}0}$ – вероятности ошибочной регистрации символов «0», рассчитанные соответственно с учетом мертвого времени продлевающегося типа и без его учета; $P_{\text{ош}1}$ и $P'_{\text{ош}1}$ – вероятности ошибочной регистрации символов «1», рассчитанные соответственно с учетом мертвого времени продлевающегося типа и без его учета; $N_{\Delta t}$ – общее число временны́х интервалов $\Delta t$, по которым выполнялось сравнение вероятностей $P_{\text{ош}0}$ и $P'_{\text{ош}0}$ или $P_{\text{ош}1}$ и $P'_{\text{ош}1}$.

Для сопоставления отклонений вероятностей ошибочной регистрации символов «0» и «1» на рис. 3 представлены зависимости $\sigma_{ош0}/\Delta t$ и $\sigma_{ош1}/\Delta t$ от средней длительности мертвого времени продлевающегося типа при средней длительности передачи одного бита (символа) $\tau_b = 100$ мкс.

Исследования проводились при постоянном значении $N_{\Delta t}$. Из представленных результатов видно, что во всем диапазоне значений средней длительности мертвого времени наблюдается рост как $\sigma_{ош0}/\Delta t$, так и $\sigma_{ош1}/\Delta t$. Причем $\sigma_{ош0}/\Delta t \approx \sigma_{ош1}/\Delta t$ при $0 \le \tau_d \le 3$ мкс (см. рис. 3, кривые *1* и *2*), однако при $\tau_d > 3$ мкс рост проявляется в большей мере для величины $\sigma_{ош1}/\Delta t$, чем для $\sigma_{ош0}/\Delta t$. Для оценки величины отклонения $\sigma_{ош0}/\Delta t$ от $\sigma_{ош1}/\Delta t$ использовался параметр $\Delta\sigma_{ош01} = |\sigma_{ош0}/\Delta t - \sigma_{ош1}/\Delta t|$.

Указанное поведение зависимостей $\sigma_{ош0}/\Delta t$ и $\sigma_{ош1}/\Delta t$ с увеличением средней длительности мертвого времени продлевающегося типа объясняется следующими причинами.

Число импульсов, незарегистрированных счетчиком фотонов из-за наличия мертвого времени (число просчетов) в случае приема символов «0» и «1» определяется соответственно как $(n_t + n_{s0})\,\tau_d$ и $(n_t + n_{s1})\,\tau_d$. Следовательно, при $\tau_d = 0$ число таких просчетов равно 0, поэтому $\sigma_{ош0}/\Delta t = \sigma_{ош1}/\Delta t = 0$. Однако при повышении средней длительности мертвого времени отклонения $P_{ош0}$ от $P'_{ош0}$ и $P_{ош1}$ от $P'_{ош1}$ растут за счет сдвига соответствующих распределений $P_{st0}(N)$ и $P_{st1}(N)$ в сторону меньших значений $N$, что объяснялось ранее. В результате с увеличением $\tau_d$ параметры $\sigma_{ош0}/\Delta t$ и $\sigma_{ош1}/\Delta t$ также растут.

При $\tau_d > 3$ мкс число просчетов в случае приема символов «1» оказывается больше, чем при регистрации символов «0», и вместе с тем такая тенденция проявляется тем больше, чем выше $\tau_d$ (см. рис. 3). Это объясняется тем, что для рассматриваемого канала связи критерием выбора $n_{s0}$ и $n_{s1}$ являются минимальные значения соответствующих вероятностей $P_{ош0}$ и $P_{ош1}$, обеспечиваемые при $n_{s1} > n_{s0}$. С увеличением $\tau_d$ средние скорости счета сигнальных импульсов $n_{s0}$ и $n_{s1}$,при которых соответствующие вероятности $P_{ош0}$ и $P_{ош1}$ минимальны, также растут, причем такой рост имеет более выраженный характер для $n_{s1}$, чем для $n_{s0}$.

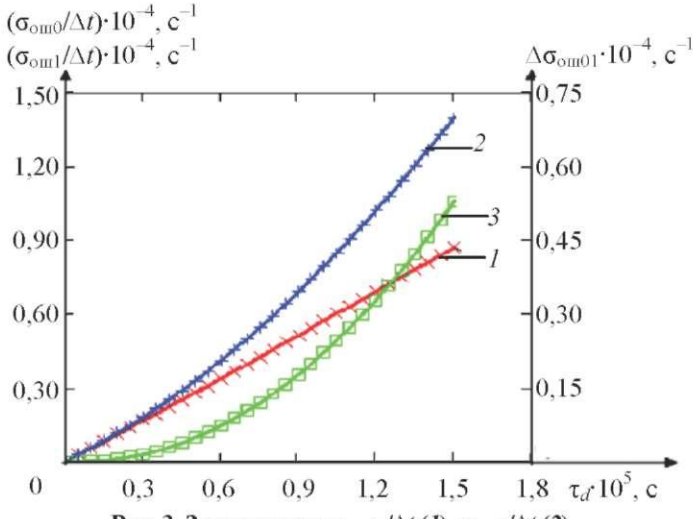


**Рис. 3. Зависимости $\sigma_{ош0}/\Delta t$ (*1*), $\sigma_{ош1}/\Delta t$ (*2*) и $\Delta\sigma_{ош01}$ (*3*) от средней длительности мертвого времени**

Например, наименьшие значения $P_{\text{ош}0} = 0{,}06$ и $P_{\text{ош}1} = 0{,}00$ достигаются соответственно при $n_{s0} = 74{,}1 \cdot 10^3$ с$^{-1}$ и $n_{s1} = 38{,}9 \cdot 10^4$ с$^{-1}$ для $\tau_d = 5$ мкс; при $n_{s0} = 83{,}5 \cdot 10^3$ с$^{-1}$ и $n_{s1} = 43{,}7 \cdot 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс.

## Заключение

Получены выражения для оценки вероятностей ошибочной регистрации данных, передаваемых по дискретному двоичному асинхронному однородному квантово-криптографическому каналу связи без памяти и со стиранием, в котором в качестве приемного модуля использовался счетчик фотонов с мертвым временем продлевающегося типа.

Установлено, что с увеличением среднего времени однофотонной передачи информации вероятность ошибочной регистрации символов «0» $P_{\text{ош}0}$ уменьшается во всем исследуемом диапазоне значений $\Delta t$, в то время, как для зависимостей $P_{\text{ош}1}(\Delta t)$ такой спад наблюдается при $\Delta t \geq 6{,}90$ мкс для $\tau_d = 0$; при $\Delta t \geq 11{,}21$ мкс для $\tau_d = 5$ мкс; при $\Delta t \geq 15{,}53$ мкс для $\tau_d = 10$ мкс; при $\Delta t \geq 19{,}84$ мкс для $\tau_d = 15$ мкс.

Определено, что в диапазонах значений $\Delta t$, на которых имеет место спад зависимостей $P_{\text{ош}0}(\Delta t)$ и $P_{\text{ош}1}(\Delta t)$, увеличение мертвого времени продлевающегося типа приводит к росту вероятностей ошибочной регистрации как символов «0», так и символов «1».

Результаты, полученные в данной работе, могут быть использованы при создании систем квантово-криптографической связи, функционирующих в асинхронном режиме передачи и приема двоичных данных и позволяющих обнаруживать несанкционированный доступ к информации за счет контроля числа ошибок в канале связи. Так, например, в случае реализации системы связи на базе приемопередающих устройств [1], результаты представленных в настоящей работе исследований позволяют обосновать выбор наименьшего времени однофотонной передачи информации, при котором вероятности ошибочной регистрации символов «0» и «1» минимальны, что повысит достоверность определения подлинности передаваемой информации и их источника и увеличит скорость передачи информации. Учитывая весьма низкие скорости передачи информации для указанных каналов связи, перспективным является проведение их оптимизации, используя в качестве критерия оптимальности величину наибольшей пропускной способности, что планируется выполнить в ходе дальнейших исследований.

*Список литературы*

1. 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. doi: 10.21122/2220-9506-2018-9-1-17-27

2. Калачев, А. А. Элементная база дальнодействующей квантовой связи. Часть 1 / А. А. Калачев // Фотоника. – 2017. – № 1. – С. 88 – 98. doi: 10.22184/1993-7296.2017.61.1.88.98

3. Single-Photon Counters in the Telecom Wavelength Region of 1550 nm for Quantum Information Processing / M. Bourennane [et al.] // Journal of Modern Optics. – 2001. – Vol. 48, No. 13. – P. 1983 – 1995. doi: 10.1080/09500340110075131

4. Килин, С. Я. Квантовая криптография: идеи и практика / С. Я. Килин, Д. Б. Хорошко, А. П. Низовцев. – Минск : Белорус. наука, 2007. – 391 с.

5. Cova, S. D. Single-Photon Counting Detectors / S. D. Cova, M. Ghioni // IEEE Photonics Journal. – 2011. – Vol. 3, No. 2. – P. 274 – 277. doi: 10.1109/JPHOT.2011.2130518

6. Single-Photon Experiments at Telecommunication Wavelengths Using Nanowire Superconducting Detectors / C. Zinoni [et al.] // Applied Physics Letters. – 2007. – Vol. 91. – P. 031106-1 – 031106-3. doi: 10.1063/1.2752108

7. Advances in InGaAs/InP Single-Photon Detector Systems for Quantum Communication / J. Zhang [et al.] // Light: Science & Applications. – 2015. – Vol. 4. – P. 1 – 13. doi: 10.1038/lsa.2015.59

8. 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

9. Stipčević, M. Characterization of a Novel Avalanche Photodiode for Single Photon Detection in VIS-NIR Range / M. Stipčević, H. Skenderovic, D. Gracin // Optics Express. – 2010. – Vol. 18, No. 16. – P. 17448 – 17459. doi: 10.1364/OE.18.017448

10. Исследование пропускной способности асинхронного оптического канала связи с приемником на основе счетчика фотонов / И. Р. Гулаков [и др.] // Приборы и методы измерений. – 2013. – № 2 (7). – С. 80 – 87.

11. Гулаков, И. Р. Исследование скорости передачи информации по оптическому каналу связи с приемником на основе счетчика фотонов / И. Р. Гулаков, А. О. Зеневич, А. М. Тимофеев // Автометрия. – 2011. – Т. 47, № 4. – С. 31 – 40.

12. Абед, А. Х. А. Метод шифрования передаваемой информации по случайному закону / А. Х. А. Абед // Вестн. Тамб. гос. техн. ун-та. – 2016. – Т. 22, № 2. – С. 233 – 237. doi: 10.17277/vestnik.2016.02.pp.233-237

13. Беспроводной канал передачи информации со скоростью 40 Гбит/с / А. А. Боев [и др.] // Вестн. Рязанского гос. радиотехн. ун-та. – 2017. – № 62. – С. 44 – 48. doi: 10.21667/1995-4565-2017-62-4-44-48

14. 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.

15. 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 (147). – С. 56 – 62.

16. Гольданский, В. И. Статистика отсчетов при регистрации ядерных частиц / В. И. Гольданский, А. В. Куценко, М. И. Подгорецкий. – М. : Гос. изд-во физико-математической литературы, 1959. – 411 с.

## The Effect of Single Photon Transmission Time on the Probability of Erroneous Registration of Asynchronous Data of Quantum Cryptographic Communication Channels

**A. M. Timofeev**

*Department of Information Security, Belarusian State University of Informatics and Radio Electronics, Minsk, Republic of Belarus; tamvks@mail.ru*

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

**Abstract:** Expressions are determined to estimate the probabilities of erroneous recording of binary data of a quantum-cryptographic communication channel containing a photon counter with an extending dead time.

According to the results of mathematical modeling, the dependences of the probabilities of erroneous data recording at the output of the communication channel are established on the average single-photon transmission time of the characters "0" and "1", on the basis of which the choice of the smallest average transmission time per bit (character), providing the smallest loss of information transmitted, is justified.

The obtained results make it possible to increase the accuracy of determining unauthorized access to information transmitted over a discrete binary asynchronous homogeneous quantum-cryptographic communication channel without memory and with erasure.

*References*


1. 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, no. 1, pp. 17-27, doi: 10.21122/2220-9506-2018-9-1-17-27 (In Russ., abstract in Eng.)

2. Kalachev A.A. [Elemental base of long-range quantum coupling. Part 1], *Fotonika* [Photonics], 2017, no. 1, pp. 88-98, doi: 10.22184/1993-7296.2017.61.1.88.98 (In Russ., abstract in Eng.)

3. Bourennane M., Karlsson A., Ciscar J.P., Mathes M. Single-photon counters in the telecom wavelength region of 1550 nm for quantum information processing, *Journal of modern optics*, 2001, vol. 48, no. 13, pp. 1983-1995, doi: 10.1080/09500340110075131

4. Kilin S.Ya. [Ed.], Khoroshko D.B., Nizovtsev A.P. *Kvantovaya kriptografiya: idei i praktika* [Quantum cryptography: ideas and practice], Minsk: Belorusskaya nauka, 2007, 391 p. (In Russ.)

5. Cova S.D., Ghioni M. Single-photon counting detectors, *IEEE Photonics Journal*, 2011, vol. 3, no. 2, pp. 274-277, doi: 10.1109/JPHOT.2011.2130518

6. Zinoni C., Alloing B., Li L.H., Marsili F., Fiore A. Single-photon experiments at telecommunication wavelengths using nanowire superconducting detectors, *Applied Physics Letters*, 2007, vol. 91, pp. 031106-1-031106-3, doi: 10.1063/1.2752108

7. Zhang J., Itzler M.A., Zbinden H., Pan J.-W. Advances in InGaAs/InP single-photon detector systems for quantum communication, *Light: Science & Applications*, 2015, vol. 4, pp. 1-13, doi: 10.1038/lsa.2015.59

8. 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

9. Stipčević M., Skenderovic H., Gracin D. Characterization of a novel avalanche photodiode for single photon detection in VIS-NIR range, *Optics Express*, 2010, vol. 18, no. 16, pp. 17448-17459, doi: 10.1364/OE.18.017448

10. Gulakov I.R., Zenevich A.O., Timofeyev A.M., Kosari A.G. [Investigation of the throughput capacity of an asynchronous optic communication channel with a receiver based on a photon counter], *Pribory i metody izmereniy* [Instruments and measurement methods], 2013, no. 2 (7), pp. 80-87. (In Russ., abstract in Eng.)

11. Gulakov I.R., Zenevich A.O., Timofeyev A.M. [Investigation of the information transfer rate over an optical communication channel with a receiver based on a photon counter], *Avtometriya* [Avtometriya], 2011, vol. 47, no. 4, pp. 31-40. (In Russ.)

12. Abed A.Kh.A. [The method of encryption of transmitted information by random law], *Transactions of the Tambov State Technical University*, 2016, vol. 22, no. 2, pp. 233-237, doi: 10.17277/vestnik.2016.02.pp.233-237 (In Russ., abstract in Eng.)

13. Boyev A.A., Kernosov M.Yu., Kuznetsov S.N., Ognev B.I., Parshin A.A. [Wireless data transmission channel with a speed of 40 Gbit], *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta* [Bulletin of the Ryazan State Radio Engineering University], 2017, no. 62, pp. 44-48, doi: 10.21667/1995-4565-2017-62-4-44-48 (In Russ., abstract in Eng.)

14. 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], *Aktualnyie problemyi nauki XXI veka* [Current issues of science in the 21st century], 2018, vol. 7, pp. 5-10. (In Russ., abstract in Eng.)

15. 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 (147), pp. 56-62. (In Russ., abstract in Eng.)

16. Gol'danskiy V.I., Kutsenko A.V., Podgoretskiy M.I. *Statistika otschetov pri registratsii yadernykh chastits* [Statistics of counts in the registration of nuclear particles], Moscow: Gosudarstvennoye izdatel'stvo fiziko-matematicheskoy literatury, 1959, 411 p. (In Russ.)

## Der Einfluss der Einzelphotonenübertragungszeit der Information auf die Wahrscheinlichkeit einer fehlerhaften Registrierung asynchroner Daten der quantenkryptographischen Kommunikationskanäle

**Zusammenfassung:** Es sind die Ausdrücke zum Schätzen der Wahrscheinlichkeiten einer fehlerhaften Registrierung binärer Daten eines quantenkryptographischen Kommunikationskanals bestimmt, der einen Photonenzähler mit einer Totzeit eines verlängerten Typs enthält. Den Ergebnissen der mathematischen Modellierung nach sind die Abhängigkeiten der Wahrscheinlichkeiten einer fehlerhaften Datenaufzeichnung am Ausgang des Kommunikationskanals von der durchschnittlichen Einzelphotonen-Übertragungszeit der Zeichen "0" und "1" festgelegt, auf deren Grundlage die Wahl der kleinsten durchschnittlichen Übertragungszeit pro Bit (Zeichen) begründet ist, die den geringsten Verlust der übertragenen Information gewährleistet. Die erhaltenen Ergebnisse ermöglichen es, die Zuverlässigkeit des Bestimmens eines nicht autorisierten Zugriffs auf Informationen zu erhöhen, die über einen diskreten binären asynchronen homogenen quantenkryptographischen Kommunikationskanal ohne Speicher und mit Löschung übertragen werden.

## Influence du temps de la transmission monophotonique d'informations sur la probabilité de l'enregistrement erroné des données des canaux de la communication asynchrones quantiques-cryptographiques

**Résumé**: Sont définies des expressions pour évaluer les probabilités d'enregistrement erroné des données binaires d'un canal de la communication quantique-cryptographique contenant un compteur de photons avec un temps mort du type prolongé. Les résultats de la simulation mathématique montrent que les données sont probablement enregistrées de manière erronée à la sortie du canal de communication à partir du temps moyen du transfert monophotonique des caractères "0" et "1", à la base duquel il est justifié de choisir le temps moyen du transfert d'un bit (symbole), ce qui garantit la perte la plus faible de l'information transmise. Les résultats obtenus permettent d'améliorer la fiabilité de la définition de l'accès non autorisé aux informations transmises par un canal de la communication binaire asynchrone homogène quantique-cryptographique discret sans mémoire et avec effacement.

**Автор:** ***Тимофеев Александр Михайлович*** – кандидат технических наук, доцент кафедры защиты информации, УО «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь.

**Рецензент:** ***Жарин Анатолий Лаврентьевич*** – доктор технических наук, профессор кафедры информационно-измерительной техники и технологии, Белорусский национальный технический университет, г. Минск, Республика Беларусь.