Раздел I. Информационная безопасность

УДК 621.396.624

К.Е. Румянцев, А.П. Плёнкин

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ АЛГОРИТМА ВХОЖДЕНИЯ В СИНХРОНИЗМ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ*

Исследована двухпроходная система квантового распределения ключа (СКРК) с фазовым кодированием состояний фотонов в режиме вхождения в синхронизм. Сигналы синхронизации представляют периодическую последовательность фотонных импульсов для защиты от несанкционированного доступа. Предложен алгоритм синхронизации двухпроходной автокомпенсационной СКРК с фазовым кодированием состояний фотонов, предполагающий деление периода следования оптических импульсов на временные окна и обнаружение сигнального окна. Особенность исследуемого алгоритма синхронизации состоит в том, что он реализуется в однофотонном режиме с регистрацией фотонов, повышая безопасность режима синхронизации СКРК. Вторая особенность алгоритма состоит в том, что при равенстве числа накопленных импульсов в двух соседних временных окнах принимается решение о приёме фотонного импульса любым из этих окон, если количество накопленных импульсов в нём превышает число зарегистрированных импульсов в остальных окнах. В известном алгоритме в таком случае оба окна принимались шумовыми, что являлось причиной пропуска сигнального окна. Для доказательства эффективности предлагаемого алгоритма синхронизации системы квантового распределения ключей проведено имитационное моделирование процесса синхронизации. Исходными данными при моделировании выступают длительность фотонного импульса 1 нс, период следования оптических импульсов 1024 нс, частота появления импульсов темнового тока 400 Гц, среднее число ФЭ, принимаемых за длительность фотонного импульса 0,01, объём выборки отсчётов регистрируемых импульсов в каждом временном окне 200. Число статистических испытаний принято равным 5 000. В процессе моделирования отношение длительности временного окна к длительности фотонного импульса принимает 10 дискретных значений 1; 2; 4; 8; 16; 32; 64; 128; 256 и 512. Установлено, что при изменении числа временных окон с 2 до 1024, разность предельных значений вероятности не превышает 3,34 %. Причём, наибольшее значение вероятности правильного обнаружения наблюдается при числе временных окон равном 2, где отношение длительности временного окна к длительности фотонного импульса равно 512. Предлагаемый алгоритм уменьшает вероятность принятия ошибочного решения при равенства числа накопленных импульсов в соседних сигнальных временных окнах при распределении между ними энергии фотонных импульсов. Выигрыш предлагаемого алгоритма очевиден при количестве окон более 512, когда вероятность принадлежности фотонного импульса двум окнам превышает 49 %. Снижение более чем в 4 раза вероятности принятия ошибочного решения достигается при числе окон 1024, т.е. когда длительность временного окна равна длительности фотонного импульса. Получено аналитическое выражение для инженерных расчётов вероятности правильного обнаружения. Максимальное отклонение результатов моделирования предложенного алгоритма и расчётов не превышает 1,5 %. Это доказывает возможность использования аналитических соотноше-

* Работа выполнена при поддержке «ИнфоТеКС Академия 2015–2016».

ний для расчёта вероятности правильного обнаружения момента приёма фотонного импульса в предложенном алгоритме вхождения в синхронизм автокомпенсационной системы квантового распределения ключей.

Система квантового распределение ключа; фотонный импульс; синхронизация; алгоритм; эффективность вхождения в синхронизм.

K.E. Rumyantsev, A.P. Pljonkin

IMPROVING EFFICIENT OF SYNCHRONIZATION ALGORITHM OF QUANTUM KEY DISTRIBUTION SYSTEM

The two-pass quantum key distribution system (QKDS) with phase-encoded states of photons in the synchronization mode are studies. The synchronization signals are periodic sequence of photon pulses to protect against unauthorized access. An algorithm for synchronizing two pass autocompensation QKDS phase-encoded states of photons, involving the division of the repetition period of the optical pulses in the time window and the detection of the signal window. Feature of investigated the synchronization algorithm is that it is implemented in the single-photon mode detection, improving security of QKDS synchronization mode. The second feature of the algorithm is that for equal numbers of accumulated pulses in two adjacent time windows is decided reception photon pulse in any of these windows, if the number of accumulated pulses in it exceeds the number of detected pulses in the other windows. In a certain algorithm in this case, both windows were "noise" that was the reason for skip the signal box. To prove the effectiveness of the proposed synchronization algorithm for quantum key distribution system conducted simulation of the synchronization process. Initial data for modeling are the photon pulse duration of 1 ns, the repetition period optical pulse of 1024 ns , the pulse frequency of the dark count of 400 Hz, the average number of photoelectrons taken for the duration of the photon momentum 0.01, the counts for each time window 200. The number of statistical tests assumed to be 5 000. In the process of modeling the ratio of the length of the time window to the photon pulse duration takes 10 discrete values 1; 2; 4; 8; 16; 32; 64; 128; 256 and 512. It is found that when the number of time windows from 2 to 1024, the difference of the limiting values of the probability does not exceed 3.34 %. Moreover, the greatest value of the likelihood of correct detection occurs when the number of time windows equal to 2. The proposed algorithm reduces the probability of making a wrong decision in the equal number of accumulated pulses in adjacent time windows when the energy of the photon pulses signal distribution between the windows . Winning the proposed algorithm with the number of windows to 512, when the probability of belonging to two windows photon pulse exceeds 49%. Reduced more than 4 times the probability of making a wrong decision is reached when the number of windows 1024, when the duration of the time window is equal to the duration of the photon pulse. An analytical expression for engineering calculations of probability of correct detection. The maximum deviation of the simulation results of the proposed algorithm and calculations does not exceed 1.5 %. This demonstrates the ability to use analytical expressions to calculate the probability of correct detection of the reception of the photon momentum in the proposed algorithm of synchronization quantum key distribution system.

Quantum key distribution system; photon pulse; synchronization; algorithm; efficiency and probability of synchronization mode.

Введение. Среди успешно реализованных коммерческих СКРК выделяются двухпроходные автокомпенсационные волоконно-оптические системы с фазовым кодированием состояний фотонов, которые отличаются устойчивой работоспособностью [1−4]. Распределение квантовых ключей в этих системах проходит в однофотонном режиме, где среднее число фотонов на импульс не превышает 0,1.

Важнейшей составляющей эффективной работы СКРК является регистрация момента приёма фотонного импульса однофотонными фотодетекторами (процесс синхронизации). Для СКРК наиболее подходящей формой сигнала синхронизации является периодическая последовательность оптических импульсов [5, 6]. Вре-

менными маркерами здесь выступают сами импульсы, а синхронизация достигается измерением с высокой точностью общей длины распространения фотонов в волоконно-оптической линии связи (ВОЛС) и в функциональных компонентах внутри станций СКРК.

В [7–9] описан стенд и результаты натурных испытаний квантово-криптографической сети на базе системы квантового распределения ключей Clavis2 фирмы idQuantique (Швейцария). Показано, что процесс синхронизации реализуется в многофотонном режиме, где среднее число фотонов на импульс измеряется сотнями и тысячами. Это согласуется с результатами исследований в [10], где показано, что в процессе синхронизации фотодетекторы работают в линейном режиме.

Реализация многофотонного режима в процессе синхронизации потенциально упрощает злоумышленнику организацию несанкционированного доступа к информации. Последнее определяет актуальность нахождения алгоритмов синхронизации в однофотонном режиме, обеспечивающих повышенную защищённость процесса вхождения в связь.

В [11] описан процесс вхождения в синхронизм СКРК с фазовым кодированием состояний фотонов и предложен алгоритм поиска фотонного импульса. Исследуемый процесс синхронизации в системе с фазовым кодированием проходит в однофотонном режиме, причём среднее число фотонов на импульс на обратном пути от кодирующей станции Алиса к приёмопередающей станции Боб не превышает 0,1. Полученные аналитические выражения позволяют оценить влияние параметров фотонного импульса и аппаратуры поиска на вероятность правильного обнаружения сигнального временного окна.

Проведённый анализ предполагает, что фотонный импульс не может принадлежать одновременно двум соседним временным окнам. Последнее справедливо лишь при значительном превышении длительности временного окна над длительностью фотонного импульса. При уменьшении длительности временного окна возрастает вероятность попадания фотонного импульса на границу между двумя соседними временными окнами.

В [12] исследованы два крайних случая временного момента появления фотонного импульса: фотонный импульс полностью располагается внутри анализируемого временного окна или распределяется поровну между двумя соседними окнами. Моделированием процесса определены границы применимости аналитических выражений для расчёта вероятности обнаружения сигнального временного окна в режиме синхронизации СКРК для двух крайних случаев момента появления фотонного импульса. Аналитические выражения доказывают, что в случае деления поровну фотонного импульса между соседними временными окнами, вероятность синхронизации СКРК не велика.

В [11] проведён анализ алгоритма синхронизации с учётом случайного момента появления фотонного импульса во временном окне. Учтено, что фотонный импульс может одновременно принадлежать двум соседним временным окнам. Установлено, что в реализуемом алгоритме синхронизации аппаратура может принимать ошибочные решения из-за пропуска сигнального окна и ложного срабатывания. Пропуск сигнального окна возникает при равенстве накопленного числа фотонов в двух соседних временных окнах из-за распределения между ними энергии фотонных импульсов. Напротив, превышение накопленного числа ИТТ хотя бы в одном из шумовых окон над суммарным числом фотонов и ИТТ в сигнальных окнах приводит к тому, что аппаратурой за сигнальное принимается шумовое окно (ложное срабатывание).

Исключение или, хотя бы, уменьшение вероятности пропуска сигнального окна и ложного срабатывания позволит повысить эффективность синхронизации СКРК. Ложное срабатывание напрямую связано с частотой появления ИТТ в применяемых однофотонных фотодетекторах [13–16]. Так, например, в однофотонных лавинных фотодиодах [17, 18] снизить частоту появления ИТТ до уровня 50 Гц удаётся за счёт охлаждения фотодиода. Однако полное исключение ложных срабатываний за счёт охлаждения не гарантируется.

Цель исследований состоит в повышении вероятности вхождения в синхронизм СКРК путём разработки алгоритма, уменьшающего принятие ошибочного решения при равенстве числа накопленных импульсов в соседних сигнальных временных окнах, между которыми распределена энергия фотонного импульса.

Алгоритм поиска оптического сигнала в СКРК. В процессе вхождения в синхронизм временной кадр, равный периоду следования оптических импульсов T_s, разбивается на N_w временных окон с длительностью τ_w, причём $T_s = N_w \tau_w$.

Каждое временное окно опрашивается N раз, определяя объём выборки. Последнее эквивалентно опросу j-го временного окна во временных интервалах $t \in \left[(i-1)T_s + (j-1)\tau_w ; (i-1)T_s + j\tau_w\right], i = \overline{1,N};\ j = \overline{1,N_w}$.

Объём выборки для обеспечения заданной вероятности обнаружения сигнального временного окна в режиме синхронизации определяется средним числом фотоэлектронов (ФЭ) в импульсе и частотой появления ИТТ в однофотонном фотодетекторе. Здесь под фотоэлектроном понимается генерируемый первичный электрон в результате взаимодействия фотона с фоточувствительной поверхностью однофотонного фотодетектора.

Имитационное моделирование в [11, 19, 20] при длительности фотонного импульса τ_s=1 нс, периоде следования оптических импульсов T_s=1024 нс, частоте появления ИТТ 400 Гц, среднем числе принимаемых ФЭ в фотонном импульсе $\overline{n_s}$=0,01 и длительности временного окна τ_w=128 нс показало, что для вхождения в синхронизм с вероятностью 85 % потребует опросить 200 раз каждое временное окно. Требуемый объём выборки при той же вероятности вхождения в синхронизм возрастает с увеличением дальности ВОЛС (уменьшением среднего числа принимаемых ФЭ за длительность фотонного импульса).

Пусть в качестве счётчика фотонов используется идеальное устройство, регистрирующее все принятые ФЭ за фиксированное время наблюдения (в нашем случае за длительность временного окна τ_w).

Предполагается абсолютная стабильность периода следования ΔT_s и длительности $\Delta\tau_s$ фотонного импульса. Отметим, что выбор значения периода следования T_s (временного кадра) определяется протяжённостью ВОЛС и рассчитывается исходя из скорости распространения оптического импульса в волокне.

При каждом опросе временного окна фиксируется число принятых ФЭ и/или ИТТ. Случай отсутствия фотонного импульса в обследуемом шумовом временном окне подразумевает регистрацию только ИТТ.

Модель процессов в шумовом временном окне. Пусть известна частота появления ИТТ ξ_d. Тогда за длительность τ_w одного временного окна среднее число регистрируемых ИТТ равно $\overline{n_{d.w}} = \xi_d \tau_w$. За выборку объёмом N среднее число регистрируемых ИТТ составит $\overline{n_{d.N}} = N \cdot \overline{n_{d.w}} = N \cdot \xi_d \tau_w$.

Поскольку среднее число регистрируемых ИТТ за длительность шумового временного окна в СКРК крайне мало (в модели даже при 2-х временных окнах не превышает 0,041 [11]), то для описания статистических свойств потока ИТТ за выборку объёмом N используется закон Пуассона [21].

Модель процессов в сигнальных временных окнах. Пусть $\overline{n_s}$ – среднее число ФЭ, регистрируемых за длительность фотонного импульса. Принимается, что момент появления t_1 фотонного импульса принадлежит первому временному окну. Для случая расположения фотонного импульса полностью внутри анализируемого окна момент его появления t_1 должен располагаться внутри интервала $[0, \tau_w - \tau_s]$ в первом временном кадре. В этом случае за длительность τ_w сигнального временного окна будут регистрироваться как ФЭ, так и ИТТ, причём их среднее число равно $\overline{n_w} = \overline{n_{d.w}} + \overline{n_s} = \xi_d \tau_w + \overline{n_s}$. За выборку объёмом N количество регистрируемых импульсов в сигнальном временном окне составит в среднем $\overline{n_{w.N}} = N \cdot \overline{n_w} = \overline{n_{d.N}} + \overline{n_{s.N}}$, где $\overline{n_{s.N}} = N \cdot \overline{n_s}$ – среднее число регистрируемых ФЭ за выборку объёмом N.

Напротив, если момент появления t_1 фотонного импульса принадлежит интервалу $[\tau_w - \tau_s, \tau_w]$ в первом временном кадре, то фотонный импульс располагается на границе первого и второго временных окон. В этом случае за длительность τ_w в первом временном окне будет регистрироваться в среднем следующее количество ФЭ и ИТТ

$$\overline{n_{w1}} = \overline{n_{d.w}} + \overline{n_{s1}} = x_d t_w + \overline{n_s}\left(\frac{t_w - t_1}{t_s}\right).$$

Среднее число регистрируемых ФЭ и ИТТ во втором временном окне при этом составит

$$\overline{n_{w2}} = \overline{n_{d.w}} + \left(\overline{n_s} - \overline{n_{s1}}\right) = \xi_d \tau_w + \overline{n_s} - \overline{n_{s1}}.$$

За выборку объёмом N в среднем количество регистрируемых ФЭ и ИТТ в сигнальных временных окнах равно

$$\overline{n_{w1.N}} = N \cdot \overline{n_{w1}} = \overline{n_{d.N}} + \overline{n_{s1.N}} \quad \text{и} \quad \overline{n_{w2.N}} = N \cdot \overline{n_{w2}} = \overline{n_{d.N}} + \overline{n_{s2.N}},$$

где $\overline{n_{s1.N}} = N \cdot \overline{n_{s1}}$ и $\overline{n_{s2.N}} = N \cdot \overline{n_{s2}}$ – средние числа регистрируемых ФЭ за выборку объёмом N соответственно в первом и втором окнах.

Поскольку среднее число регистрируемых ФЭ за длительность фотонного импульса мало (0,001 … 0,1), то для описания статистических свойств потока ФЭ и ИТТ также используется закон Пуассона.

Набор статистик для обнаружения сигнального временного окна. После опроса всех N_w временных окон формируется массив значений зарегистрированных ФЭ и/или ИТТ

$$\left\{n_{w.N}(j),\ j = \overline{1, N_w}\right\} = \left\{n_{w.N}(1), n_{w.N}(2), ..., n_{w.N}(j), ..., n_{w.N}(N_w)\right\}.$$

Если фотонный импульс полностью располагается внутри первого временного окна, то значения чисел $n_{w.N}(2), ..., n_{w.N}(j), ..., n_{w.N}(N_w)$ в $N_w - 1$ шумовых временных окнах описываются законом Пуассона

$$\mathrm{Pos}\left\{n_{d.N}\middle|\overline{n_{d.N}}\right\}=\frac{\left(\overline{n_{d.N}}\right)^{n_{d.N}}}{n_{d.N}!}\exp\left(-\overline{n_{d.N}}\right)$$

с параметром $\overline{n_{d.N}}=N\cdot\xi_d\cdot\tau_w$, а в первом сигнальном временном окне число $n_{w.N}(1)$ – законом

$$\mathrm{Pos}\left\{n_{w.N}\middle|\overline{n_{w.N}}\right\}=\frac{\left(\overline{n_{w.N}}\right)^{n_{w.N}}}{n_{w.N}!}\exp\left(-\overline{n_{w.N}}\right)$$

с параметром $\overline{n_{w.N}}=N\cdot\xi_d\cdot\tau_w+N\cdot\overline{n_s}$.

Напротив, если момент появления t_1 фотонного импульса принадлежит интервалу $[\tau_w-\tau_s,\tau_w]$ в первом временном кадре, то фотонный импульс располагается одновременно в первом и втором временных окнах. Причём оба окна выступают в роли сигнальных. При этом случайные величины $n_{w.N}(3),\ldots,n_{w.N}(j),\ldots,n_{w.N}(N_w)$ в N_w-2 шумовых временных окнах описываются законом Пуассона с параметром $\overline{n_{d.N}}=N\cdot\xi_d\cdot\tau_w$, а в сигнальных временных окнах числа $n_{w.N}(1)$ и $n_{w.N}(2)$ – законом

$$\mathrm{Pos}\left\{n_{w.i.N}\middle|\overline{n_{w.i.N}}\right\}=\frac{\left(\overline{n_{w.i.N}}\right)^{n_{w.i.N}}}{n_{w.i.N}!}\exp\left(-\overline{n_{w.i.N}}\right);\quad i=1;2,$$

где $\overline{n_{w1.N}}=N\cdot\overline{n_{w1}}$ и $\overline{n_{w2.N}}=N\cdot\overline{n_{w2}}$.

Условия синхронизации СКРК. При нахождении момента появления фотонного импульса в 1-м временном окне правильное обнаружение возможно только при выполнении ряда условий.

Во-первых, в 1-м сигнальном временном окне за время анализа должен быть зарегистрирован хотя бы один ФЭ или ИТТ. При распределении фотонного импульса между двумя соседними окнами это условие трансформируется: зарегистрировать хотя бы один ФЭ или ИТТ в одном из двух окон, содержащих фотонный импульс.

Во-вторых, в 1-м сигнальном временном окне число зарегистрированных импульсов строго превышает число зарегистрированных импульсов во 2-м окне и сгенерированных ИТТ в каждом шумовом окне.

В-третьих, во 2-м окне, содержащем часть фотонного импульса, число зарегистрированных импульсов строго превышает число зарегистрированных импульсов в 1-м сигнальном окне и сгенерированных ИТТ в каждом из шумовых окнах.

Наконец, при равенстве числа накопленных импульсов в двух соседних временных окнах принимается решение о приёме фотонного импульса любым из этих окон, если количество накопленных импульсов в нём превышает число зарегистрированных импульсов в остальных окнах. Заметим, что в ранее описанных алгоритмах [11, 12] в таком случае оба окна принимались шумовыми, что являлось причиной пропуска сигнального окна.

С точки зрения анализа вероятностных характеристик положение временного окна, в которое попадает момент появления фотонного импульса, не имеет значения.

Моделирование алгоритма вхождения в синхронизм с учётом случайного момента появления оптического импульса во временном окне. Для доказательства эффективности предлагаемого алгоритма синхронизации системы квантового распределения ключей проведено имитационное моделирование процесса синхронизации. Исходными данными при моделировании выступают длитель-

ность фотонного импульса τ_s=1 нс, период следования оптических импульсов T_S=1024 нс, частота появления импульсов темнового тока 400 Гц, среднее число ФЭ, принимаемых за длительность фотонного импульса $\overline{n_S}$=0,01, объём выборки отсчётов регистрируемых импульсов в каждом временном окне N=200. Число статистических испытаний принято равным 5 000.

В процессе моделирования отношение длительности временного окна τ_w к длительности фотонного импульса τ_s принимает 10 дискретных значений 1; 2; 4; 8; 16; 32; 64; 128; 256 и 512. Последнее эквивалентно выбору числа временных окон N_W соответственно 1024; 512; 256; 128; 64; 32; 16; 8; 4 и 2.

Результаты моделирования алгоритма вхождения в синхронизм. На рис. 1 представлены графические зависимости вероятности правильного обнаружения от количества временных окон.

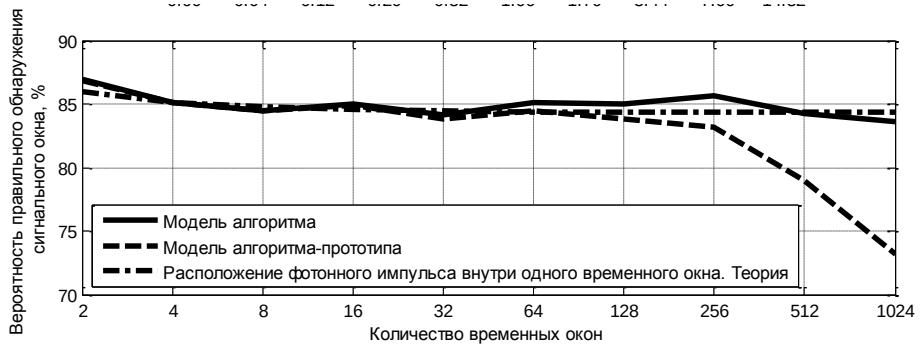

Рис. 1. Зависимость вероятности правильного обнаружения от количества временных окон

Зависимость, представленная сплошной линией, демонстрирует результаты моделирования предложенного алгоритма поиска временного окна с учётом двух факторов. Во-первых, учитывается, что момент появления оптического импульса во временном окне случаен. Во-вторых, случай, при котором регистрируется равное число ФЭ в двух соседних временных окнах, не рассматривается аппаратурой поиска как пропуск сигнала.

Из графика видно, что при изменении числа временных окон с 2 до 1024, разность предельных значений вероятности не превышает 3,34 % (83,56–86,90 %). Причём, наибольшее значение вероятности правильного обнаружения наблюдается при числе временных окон равном 2. При этом отношение длительности временного окна к длительности фотонного импульса равно 512.

Следует помнить, что при делении временного кадра всего на 2 временных окна временная неопределённость в отношении момента появления фотонного импульса максимальна. При уменьшении в 2 раза временной неопределённости (до 4-х окон) вероятность правильного обнаружения упадёт на 1,76 %. Последующее же увеличение числа временных окон до 1024 приведёт к снижению вероятности всего на 1,58 % при сокращении временной неопределённости в отношении момента появления фотонного импульса в 256 раз.

На рис. 1 штриховой линией (модель-прототип) представлена зависимость вероятности правильного обнаружения от количества временных окон для алгоритма-прототипа, построенная по результатам имитационного моделирования. В прототипе ошибочные решения могут возникать из-за пропуска сигнального окна и ложного срабатывания.

Как и следовало ожидать, при малом количестве временных окон оба алгоритма дают примерно равные результате. Например, при числе окон менее 64 расхождение вероятностей не превышает 1 %, а при 128–1,4 %. Заметим, что в первом случае вероятность принадлежности фотонного импульса двум окнам не превышает 6,5 %, то во втором – 13 %. Выигрыш предлагаемого алгоритма очевиден (84,20 вместо 78,98 %) при количестве окон более 512, когда вероятность принадлежности фотонного импульса двум окнам превышает 49 %. Различие достигает максимального значения в 12,5 % при числе окон 1024, т. е. когда длительность временного окна τ_w равна длительности фотонного импульса τ_s. Последнее эквивалентно снижению более чем в 4 раза вероятности принятия ошибочного решения.

Причина роста вероятности правильного обнаружения в предлагаемом алгоритме по сравнению с прототипом становится ясна при анализе зависимостей на рис. 2, полученных в результате моделирования. Здесь сплошной линией представлен график, устанавливающий связь вероятности правильного обнаружения с числом временных окон. График, представленный штриховой линией, иллюстрирует вероятность равного числа ФЭ и ИТТ в соседних временных окнах, между которыми распределяется фотонный импульс. Наконец график, представленный штрихпунктирной линией, определяет вероятность ложного срабатывания аппаратуры за счёт превышения накопленного числа импульсов в одном из шумовых временных окон над количеством импульсов в двух сигнальных окнах при их равенстве.

В алгоритме-прототипе при равенстве накопленного числа фотонов в двух соседних временных окнах из-за распределения между ними энергии фотонных импульсов принимается решение об отсутствии сигнала. В предлагаемом же алгоритме при равенстве накопленного числа фотонов в двух соседних временных окнах из-за распределения между ними энергии фотонных импульсов за сигнальный будет принят первый из них, но при условии, что накопленное здесь число превышает число ИТТ в каждом шумовом окне. Вероятность этого события представляет при заданном числе окон разность значений графиков, представленных штриховой и штрихпунктирной линиями.

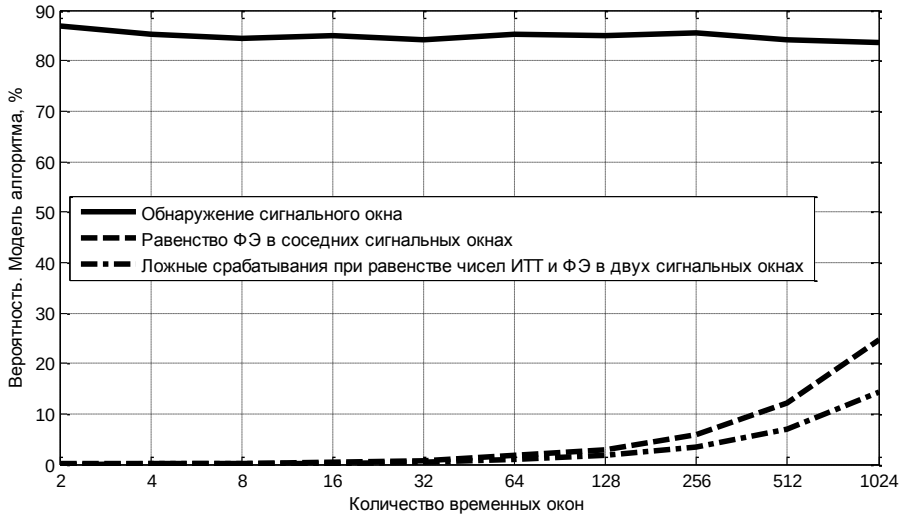

Рис. 2. Зависимость вероятностных характеристик от количества временных окон

Таким образом, предлагаемый алгоритм, уменьшающий принятие ошибочного решения при равенстве числа накопленных импульсов в соседних сигнальных временных окнах при распределении между ними энергии фотонных импульсов гарантирует повышение вероятности вхождения в синхронизм СКРК при малом отношении длительности временного окна к длительности фотонного импульса.

Соотношения для расчёта вероятностных характеристик алгоритма вхождения в синхронизм. На рис. 1 штрихпунктирной линией представлен график теоретической зависимости вероятности правильного обнаружения от количества временных окон при условии, что фотонный импульс полностью располагается внутри одного временного окна. Расчёты вероятности проведены по формуле из [11]

$$P_{\mathrm{D}} = \sum_{n_{w.N}=1}^{\infty} \frac{(\overline{n_{w.N}})^{n_{w.N}}}{n_{w.N}!} \cdot exp[-\overline{n_{w.N}}] \cdot P_{1d.N}\{n_{w.N}\}, \quad (1)$$

где

$$P_{d.N}\{n_{w.N}\} = \left(\sum_{n_{d.N}=0}^{n_{w.N}-1} \frac{\overline{n_{d.N}}^{n_{d.N}}}{n_{d.N}!} \cdot exp(-\overline{n_{d.N}}) \right)^{N_w-1}. \quad (2)$$

Вычисления по формулам (1) и (2) представляют определённые трудности из-за суммирования бесконечного числа слагаемых. Однако, как показано в [11], при ограничении верхнего предела суммирования в формуле (1) числом $(2{,}5 \ldots 3) \cdot N \cdot \overline{n_s}$ гарантируется погрешность вычисления не хуже 0,02 %.

Отметим, что максимальное отклонение двух графиков, соответствующих результатам моделирования предложенного алгоритма (сплошная линия) и расчётов (штрихпунктирная линия), не превышает 1,5 % (при числе окон 256). Это доказывает возможность использования аналитических соотношений (1) и (2) для расчёта вероятности правильного обнаружения.

Исследования показывают, что максимальное значение среднего числа ИТТ за выборку в шумовом временном окне $\overline{n_{d.N}}$ не превышает 0,041, причём при разбиении временного кадра всего на два временных окна. При этом вероятность накопления за выборку более одного ИТТ в каждом из шумовых временных окон не превышает 0,08 %.

Среднее число ИТТ за выборку в шумовом временном окне опускается до 0,00008 при увеличении числа окон до 1024. Естественно, что это позволяет производить суммирование в формуле (2) только при 2-х значениях $n_{d.N}$, равных 0 и 1. Тогда

$$P_{\mathrm{D}} = \overline{n_{w.N}} \cdot exp[-\overline{n_{w.N}}] \cdot exp(-\mathrm{N_w}\overline{n_{d.N}} + \overline{n_{d.N}}) + \rightarrow \sum_{n_{w.N}=2}^{\infty} \left[\frac{(\overline{n_{w.N}})^{n_{w.N}}}{n_{w.N}!} exp(-\overline{n_{w.N}}) \cdot (1 + \overline{n_{d.N}})^{\mathrm{N_w}-1} exp(-\mathrm{N_w}\overline{n_{d.N}} + \overline{n_{d.N}}) \right].$$

После преобразования находим

$$P_{\mathrm{D}} = \overline{n_{w.N}} \cdot exp[-\overline{n_{w.N}}] \cdot exp(-\mathrm{N_w} \cdot \overline{n_{d.N}} + \overline{n_{d.N}}) + \rightarrow +(1 + \overline{n_{d.N}})^{\mathrm{N_w}-1} exp(-\mathrm{N_w} \cdot \overline{n_{d.N}} + \overline{n_{d.N}}) \left\{ \sum_{n_{w.N}=2}^{\infty} \left[\frac{(\overline{n_{w.N}})^{n_{w.N}}}{n_{w.N}!} exp(-\overline{n_{w.N}}) \right] \right\}.$$

Поскольку для пуассоновского процесса

$$\sum_{n_{w.N}=0}^{\infty}\left[\frac{(\overline{n_{w.N}})^{n_{w.N}}}{n_{w.N}!}exp(-\overline{n_{w.N}})\right] = exp(-\overline{n_{w.N}}) + \overline{n_{w.N}}\cdot exp(-\overline{n_{w.N}}) + \rightarrow + \sum_{n_{w.N}=2}^{\infty}\left[\frac{(\overline{n_{w.N}})^{n_{w.N}}}{n_{w.N}!}exp(-\overline{n_{w.N}})\right] = 1\ ,$$

то

$$P_{\mathrm{D}} = exp(-\mathrm{N_w}\cdot\overline{n_{d.N}} + \overline{n_{d.N}})\langle\overline{n_{w.N}}\cdot exp(-\overline{n_{w.N}}) + [1 - exp(-\overline{n_{w.N}}) - \overline{n_{w.N}}\cdot exp(-\overline{n_{w.N}})](1 + \overline{n_{d.N}})^{\mathrm{N_w}-1}\rangle. \quad (3)$$

Расхождение результатов расчётов по формулам (1)–(2) и (3) не превышает 0,02 % на всем диапазоне изменений числа временных окнах.

Таким образом, получено аналитическое выражение (3) для проведения инженерных расчётов вероятности правильного обнаружения момента приёма фотонного импульса в предложенном алгоритме вхождения в синхронизм автокомпенсационной системы квантового распределения ключей.

Выводы. Предложен алгоритм синхронизации двухпроходной автокомпенсационной СКРК с фазовым кодированием состояний фотонов, предполагающий деление периода следования оптических импульсов на временные окна и обнаружение сигнального окна. Особенность исследуемого алгоритма синхронизации состоит в том, что он реализуется в однофотонном режиме с регистрацией фотонов, повышая безопасность режима синхронизации СКРК. Вторая особенность алгоритма состоит в том, что при равенстве числа накопленных импульсов в двух соседних временных окнах принимается решение о приёме фотонного импульса любым из этих окон, если количество накопленных импульсов в нём превышает число зарегистрированных импульсов в остальных окнах. В известном алгоритме в таком случае оба окна принимались шумовыми, что являлось причиной пропуска сигнального окна.

Для доказательства эффективности предлагаемого алгоритма синхронизации системы квантового распределения ключей проведено имитационное моделирование процесса синхронизации. Исходными данными при моделировании выступают длительность фотонного импульса 1 нс, период следования оптических импульсов 1024 нс, частота появления импульсов темнового тока 400 Гц, среднее число ФЭ, принимаемых за длительность фотонного импульса 0,01, объём выборки отсчётов регистрируемых импульсов в каждом временном окне 200. Число статистических испытаний принято равным 5 000. В процессе моделирования отношение длительности временного окна к длительности фотонного импульса принимает 10 дискретных значений 1; 2; 4; 8; 16; 32; 64; 128; 256 и 512.

Установлено, что при изменении числа временных окон с 2 до 1024, разность предельных значений вероятности не превышает 3,34 %. Причём, наибольшее значение вероятности правильного обнаружения наблюдается при числе временных окон равном 2, где отношение длительности временного окна к длительности фотонного импульса равно 512.

Предлагаемый алгоритм уменьшает вероятность принятия ошибочного решения при равенстве числа накопленных импульсов в соседних сигнальных временных окнах при распределении между ними энергии фотонных импульсов. Выигрыш предлагаемого алгоритма очевиден при количестве окон более 512, когда вероятность принадлежности фотонного импульса двум окнам превышает 49 %. Снижение более чем в 4 раза вероятности принятия ошибочного решения достигается при числе окон 1024, т.е. когда длительность временного окна равна длительности фотонного импульса.

Получены аналитические выражения (1)−(3) для расчёта вероятности правильного обнаружения. Максимальное отклонение результатов моделирования предложенного алгоритма и расчётов не превышает 1,5 %. Это доказывает возможность использования аналитической формулы (3) для инженерных расчётов эффективности предложенного алгоритма вхождения в синхронизм автокомпенсационной системы квантового распределения ключей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145-195.
2. *Румянцев К.Е.* Системы квантового распределения ключа: Монография. − Таганрог: Издательство ТТИ ЮФУ, 2011. − 264 с.
3. *Голубчиков Д.М., Румянцев К.Е.* Обобщённая структура систем квантового распределения ключей с фазовым кодированием состояний фотонов // Известия вузов России. Радиоэлектроника. – 2011. – № 6. – С. 26-38.
4. Квантовая криптография: идеи и практика / Под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. – Минск: Беларуская навука, 2008. – 392 с.
5. *Гальярди Р.М., Карп Ш.* Оптическая связь: Пер. с англ. / Под ред. А.Г. Шереметьева. – М.: Связь. 1978. – 424 с.
6. *Бычков С.И., Румянцев К.Е.* Поиск и обнаружение оптических сигналов: Монография / Под ред. К.Е. Румянцева. – М.: Радио и связь, 2000. – 282 с.
7. *Румянцев К.Е., Плёнкин А.П.* Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей // Телекоммуникации. – 2014. – № 10. – С. 11-16.
8. *Плёнкин А.П.* Исследование режима вхождения в синхронизм при использовании фотонных импульсов системы квантового распределения ключа // Сборник материалов международного научного е-симпозиума «Физико-математические методы и информационные технологии в естествознании, технике и гуманитарных науках» – Москва, 27-28 декабря 2014 г. – С. 101-113.
9. *Румянцев К.Е., Плёнкин А.П.* Синхронизация системы квантового распределения ключа в режиме однофотонной регистрации импульсов для повышения защищенности // Радиотехника. – 2015. – № 2. – С. 125-134.
10. *Курочкин В.Л., Курочкин Ю.В., Зверев А.В., Рябцев И.И., Неизвестный И.Г.* Экспериментальные исследования в области квантовой криптографии // Фотоника. – 2012. – № 5. – С. 54-66.
11. *Румянцев К.Е., Плёнкин А.П.* Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости // Известия ЮФУ. Технические науки. – 2014. – № 8 (157). – С. 81-96.
12. *Плёнкин А.П. Румянцев К.Е.* Зависимость вероятности обнаружения фотонного импульса в режиме синхронизации системы квантового распределения ключей от длительности временного окна // Сборник материалов международного научного е-симпозиума. Технические и естественные науки: теория и практика. Россия, г. Москва, 27–28 марта 2015 г. / под ред. К.Е. Румянцева. – Киров: МЦНИП, 2015. – С. 59-72.
13. *Scarani Valerio.* Quantum Physics: A First Encounter: Interference, Entanglement, and Reality. Translated by Rachael Thew. **–** Oxford: University Press, Mar 2006. **–** 125 p.
14. Практическая квантовая криптография // Презентационный материал. – 2-я зимняя школа. – 4–17 ноября 2010. – Компания id Quantique (Швейцария).
15. *Bennett Ch.H., Bessette F., Brassard G., Salvail L., Smolin J.* Experimental quantum cryptography // Journal of Cryptology. – 1992. – № 5. – P. 3-28.
16. *Clavis.* Plug & play quantum cryptography // id 3000. Specifications. id Quantique SA. – Ver. 2.1. – January 2005. – 2 p.
17. http://www.idquantique.com/wordpress/wp-content/uploads/id230-specs.pdf.
18. http://www.idquantique.com/photon-counting/photon-counting-modules/id220.

19. *Румянцев К.Е., Плёнкин А.П.* Моделирование процесса вхождения в синхронизм системы квантового распределения ключа при использовании для регистрации фотонных импульсов однофотонного лавинного фотодетектора для повышения защищённости // Свидетельство об официальной регистрации программного продукта для ЭВМ № 2015610876 РФ. Правообладатель: Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет», г. Ростов-на-Дону (RU). – Заявка 2014661772 от 20.11.2014. Дата регистрации 20.01.2015.
20. *Румянцев К.Е., Плёнкин А.П.* Моделирование процесса синхронизации системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости // Свидетельство об официальной регистрации программного продукта для ЭВМ № РФ. Правообладатель: Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет», г. Ростов-на-Дону (RU). – 17 марта 2015. Заявка 2014660503 от 16.10.2014.
21. *Шереметьев А.Г.* Статистическая теория лазерной связи. – М.: Связь, 1971. – 264 с.

REFERENCES

1. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography, *Reviews of Modern Physics*, 2002, Vol. 74, No. 1, pp. 145-195.
2. *Rumyantsev K.E.* Sistemy kvantovogo raspredeleniya klyucha: Monografiya [The system of quantum distribution of keys: the Monograph]. Taganrog: Izdatel'stvo TTI YuFU, 2011, 264 p.
3. *Golubchikov D.M., Rumyantsev K.E.* Obobshchennaya struktura sistem kvantovogo raspredeleniya klyuchey s fazovym kodirovaniem sostoyaniy fotonov [Generalized structure of systems of quantum key distribution with phase coding of States of photons], *Izvestiya vuzov Rossii. Radioelektronika* [Proceedings of the Russian Universities: Radioelectronics], 2011, No. 6, pp. 26-38.
4. Kvantovaya kriptografiya: idei i praktika [Quantum cryptography: ideas and practice], Under ed. S.Ya. Kilina, D.B. Khoroshko, A.P. Nizovtseva. Minsk: Belaruskaya navuka, 2008, 392 p.
5. *Gal'yardi R.M., Karp Sh*. Opticheskaya svyaz' [optical communication]: Translation from English, By ed. A.G. Sheremet'eva. Moscow: Svyaz'. 1978, 424 p.
6. *Bychkov S.I., Rumyantsev K.E.* Poisk i obnaruzhenie opticheskikh signalov: Monografiya [Search and detection of optical signals: a Monograph], By ed. K.E. Rumyantseva. Moscow: Radio i svyaz', 2000, 282 p.
7. *Rumyantsev K.E., Plenkin A.P.* Eksperimental'nye ispytaniya telekommunikatsionnoy seti s integrirovannoy sistemoy kvantovogo raspredeleniya klyuchey [Experimental testing of telecommunication networks with the integrated system of quantum key distribution], *Telekommunikatsii* [Telecommunications], 2014, No. 10, pp. 11-16.
8. *Plenkin A.P.* Issledovanie rezhima vkhozhdeniya v sinkhronizm pri ispol'zovanii fotonnykh impul'sov sistemy kvantovogo raspredeleniya klyucha [Study of mode of entering in synchronism with the pulses using photon system quantum key distribution], *Sbornik materialov mezhdunarodnogo nauchnogo e-simpoziuma «Fiziko-matematicheskie metody i informatsionnye tekhnologii v estestvoznanii, tekhnike i gumanitarnykh naukakh» – Moskva, 27-28 dekabrya 2014 g.* [Proceedings of the international scientific e-conference "Physico-mathematical methods and informational technologies in science, technology and the Humanities" Moscow, 27-28 December 2014], pp. 101-113.
9. *Rumyantsev K.E., Plenkin A.P.* Sinkhronizatsiya sistemy kvantovogo raspredeleniya klyucha v rezhime odnofotonnoy registratsii impul'sov dlya povysheniya zashchishchennosti [Synchronization system of quantum key distribution in the regime of single-photon pulses registering for enhanced protection], *Radiotekhnika* [Radioengineering], 2015, No. 2, pp. 125-134.
10. *Kurochkin V.L., Kurochkin Yu.V., Zverev A.V., Ryabtsev I.I., Neizvestnyy I.G.* Eksperimental'nye issledovaniya v oblasti kvantovoy kriptografii [Experimental research in the field of quantum cryptography], *Fotonika* [Photonika], 2012, No. 5, pp. 54-66.
11. *Rumyantsev K.E., Plenkin A.P.* Sinkhronizatsiya sistemy kvantovogo raspredeleniya klyucha pri ispol'zovanii fotonnykh impul'sov dlya povysheniya zashchishchennosti [Synchronization of quantum key distribution system using photon pulses to improve the security] *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8 (157), pp. 81-96.

12. *Plenkin A.P. Rumyantsev K.E.* Zavisimost' veroyatnosti obnaruzheniya fotonnogo impul'sa v rezhime sinkhronizatsii sistemy kvantovogo raspredeleniya klyuchey ot dlitel'nosti vremennogo okna [The dependence of the probability of detecting a photon pulse in the mode synchronization system of quantum key distribution on the duration of the time window], *Sbornik materialov mezhdunarodnogo nauchnogo e-simpoziuma. Tekhnicheskie i estestvennye nauki: teoriya i praktika. Rossiya, g. Moskva, 27–28 marta 2015 g.* [Proceedings of the international scientific e-Symposium. Technical and natural science: theory and practice. Russia, Moscow, 27-28 March 2015], By ed. K.E. Rumyantseva. Kirov: MTsNIP, 2015, pp. 59-72.
13. *Scarani Valerio.* Quantum Physics: A First Encounter: Interference, Entanglement, and Reality. Translated by Rachael Thew. Oxford: University Press, Mar 2006б 125 p.
14. Prakticheskaya kvantovaya kriptografiya [Practical quantum cryptography], Prezentatsionnyy material. 2-ya zimnyaya shkola. 4-17 noyabrya 2010 [Presentation material. 2nd winter school. 4-17 November 2010]. Kompaniya id Quantique (Switzerland).
15. *Bennett Ch.H., Bessette F., Brassard G., Salvail L., Smolin J.* Experimental quantum cryptography, *Journal of Cryptology*, 1992, No. 5, pp. 3-28.
16. *Clavis.* Plug & play quantum cryptography, id 3000. Specifications, *id Quantique SA*, Ver. 2.1, January 2005, 2 p.
17. Available at: http://www.idquantique.com/wordpress/wp-content/uploads/id230-specs.pdf.
18. Available at: http://www.idquantique.com/photon-counting/photon-counting-modules/id220.
19. *Rumyantsev K.E., Plenkin A.P.* Modelirovanie protsessa vkhozhdeniya v sinkhronizm sistemy kvantovogo raspredeleniya klyucha pri ispol'zovanii dlya registratsii fotonnykh impul'sov odnofotonnogo lavinnogo fotodetektora dlya povysheniya zashchishchennosti [Modeling of the process of entering into synchronism of the system of quantum distribution of the key when used for the registration of photon pulses single-photon avalanche photo-detector to enhance security], *Svidetel'stvo ob ofitsial'noy registratsii programmnogo produkta dlya EVM № 2015610876 RF. Pravoobladatel': FGAOUVO «Yuzhnyy federal'nyy universitet», g. Rostov-na-Donu (RU). Zayavka 2014661772 ot 20.11.2014. Data registratsii 20.01.2015* [Certificate about official registration software for computers No. 2015610876 of the Russian Federation. Holder: Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University", Rostov-on-don (RU). Application 2014661772 from 20.11.2014. Registration date 20.01.2015].
20. *Rumyantsev K.E., Plenkin A.P.* Modelirovanie protsessa sinkhronizatsii sistemy kvantovogo raspredeleniya klyucha pri ispol'zovanii fotonnykh impul'sov dlya povysheniya zashchishchennosti [Modelling the synchronization process of the system of quantum key distribution using photon pulses to enhance security], *Svidetel'stvo ob ofitsial'noy registratsii programmnogo produkta dlya EVM № RF. Pravoobladatel': Federal'noe gosudarstvennoe avtonomnoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovaniya «Yuzhnyy federal'nyy universitet», g. Rostov-na-Donu (RU). 17 marta 2015. Zayavka 2014660503 ot 16.10.2014* [Certificate about official registration software for computers No. of the Russian Federation. Holder: Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University", Rostov-on-don (RU). March 17, 2015. Application 2014660503 from 16.10.2014].
21. *Sheremet'ev A.G.* Statisticheskaya teoriya lazernoy svyazi [Statistical theory laser communication]. Moscow: Svyaz', 1971, 264 p.

Статью рекомендовал к опубликованию д.т.н., профессор Д.А. Безуглов.

Румянцев Константин Евгеньевич – Южный федеральный университет; e-mail: rke2004@mail.ru; 347922, г. Таганрог, ул. Чехова, 2; тел.: 89281827209; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Плёнкин Антон Павлович – e-mail: pljonkin@mail.ru; тел.: 89054592158; кафедра ИБТКС; аспирант.

Rumyantsev Konstantin Evgenievich – Southern Federal University; e-mail: rke2004@mail.ru; 2, Chekhova street, Taganrog, 347922, Russia; phone: +79281827209; the department of information security of telecommunication; head of department; dr. of eng.. sc.; professor.

Pljonkin Anton Pavlovich – e-mail: pljonkin@mail.ru; phone: +79054592158; the department of information security of telecommunication systems; postgraduate student.