26. *Kornienko V.T.* Ispol'zovanie virtual'nykh priborov LabVIEW v uchebnom protsesse dlya skremblirovaniya tsifrovogo potoka dannykh [Application of labview virtual devices in educational process for scrambling of digital data flow*], Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 11 (148), pp. 182-186.
27. *Kornienko V.T.* Otsenka koeffitsienta szhatiya kodera Khaffmana v virtual'nom laboratornom eksperimente LabVIEW [Evaluation of the compression ratio of the Huffman encoder in the virtual laboratory experiment LabVIEW], *Sbornik nauchnykh trudov po itogam mezhdunarodnoy nauchno-prakticheskoy konferentsii «Novye tekhnologii i problemy tekhnicheskikh nauk»* [Proceedings of the international scientific-practical conference "New technologies and problems of technical Sciences"]. Krasnoyarsk, 2014, pp. 107-110.
28. *Kornienko V.T.* Povyshenie effektivnosti peredachi dannykh v sistemakh s interfeysom Wiegand [Improving the efficiency of data transmission in systems with Wiegand interface], *Sbornik nauchnykh trudov po itogam Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Tekhnicheskie nauki v mire: ot teorii k praktike»* [Proceedings of the International scientific-practical conference "Technical Sciences in the world: from theory to practice"]. Rostov-on-Don, 2014, pp. 67-69.

Статью рекомендовал к опубликованию д.пед.н. И.А. Стеценко.

Корниенко Владимир Тимофеевич – Южный федеральный университет; e-mail: vtkornienko@sfedu.ru; г. Таганрог, ул. Дзержинского, 170, кв. 53; тел.:+79515271225; кафедра РТС ИРТСиУ; к.т.н.; доцент.

Kornienko Vladimir Timofeevich – Southern Federal University; e-mail: vtkornienko@sfedu.ru; 170, Dzerginsky street, fl. 53, Taganrog, Russia; phone: +79515271225; the department RTS IRTS&C; cand. of eng. sc.; associate professor.

УДК 621.396.624

К.Е. Румянцев, А.П. Плёнкин

БЕЗОПАСНОСТЬ РЕЖИМА СИНХРОНИЗАЦИИ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ*

Исследования посвящены двухпроходной системе квантового распределения ключа (СКРК) с фазовым кодированием состояний фотонов в режиме вхождения в связь. Сигналы синхронизации представляют собой периодическую последовательность оптических импульсов. Формирование фотонных импульсов и применение однофотонных фотодетекторов обеспечивает повышенную защищённость от несанкционированного доступа режима синхронизации. Считаются известными период следования и длительность фотонного импульса. Временной кадр, равный периоду следования оптических импульсов, разбивается на ряд временных окон. Каждое окно опрашивается несколько раз, определяя объём выборки. При каждом опросе временного окна фиксируется число принимаемых фотоэлектронов (ФЭ) и/или импульсов темнового тока (ИТТ). В процессе синхронизации окно, в котором зарегистрировано максимальное число ФЭ и/или ИТТ, принимается за сигнальное окно. При анализе алгоритма синхронизации считается, что момент появления фотонного импульса случаен. Учитывается, что фотонный импульс может одновременно принадлежать двум соседним окнам. Случайные процессы в шумовых и сигнальных временных окнах описываются законом Пуассона. Моделированием процесса синхронизации определены границы применимости аналитических выражений для расчёта вероятности обнаружения сигнального временного окна в режиме синхронизации СКРК для двух крайних случаев момента появления фотонного импульса: фотонный импульс полностью располагается внутри анализируемого временного окна или распределяется между двумя соседними окна-

* Работа выполнена в рамках государственного задания Министерства образования и науки РФ высшим учебным заведениям в части проведения научно-исследовательских работ. Тема № 213.01-11/2014-9.

ми. Дана оценка влияния числа временных окон и отношения длительности окна к длительности импульса на вероятность правильного обнаружения с учётом случайного момента появления фотонного импульса. Показано, что для уменьшения временной неопределённости длительность временного окна должна в 4 раза превышать длительность фотонного импульса при длительности фотонного импульса 1 нс, периоде следования 1024 нс, частоте появления импульсов темнового тока 400 Гц, среднем числе фотоэлектронов за длительность фотонного импульса 0,01 и объёме выборки отсчётов регистрируемых импульсов в каждом временном окне 200.

Системы квантового распределение ключа; фотонный импульс; синхронизация.

K.Y. Rumyantsev, A.P. Pljonkin

SECURITY OF SYNCHRONIZATION MODE OF QUANTUM KEYS DISTRIBUTION SYSTEM

Investigations related to the two-pass autocompensation quantum key distribution system (QKDS) of phase-encoded states of photons in the connecting mode. The synchronization signals are of a periodic sequence of optical pulses. Using photonic pulses and single-photon photodetectors provides enhanced protected from unauthorized access synchronization mode. Length of photon pulse and repetition period are assumed to be known. The time frame (period of following the optical pulses) are division to the many periods (a time windows). Each window is queried several times, determining sample size. Each time window survey fixed number of received photoelectrons and / or dark counts. The window in which recorded the maximum number of photoelectrons and dark counts is taken as a signal window. When analyzing the synchronization algorithm it is considered that the time of occurrence of the photon pulse is random. Taken into account that the photon pulse can simultaneously belong to two neighboring windows. Random processes in noise and signal time windows described by the Poisson law. Simulation of the synchronization process defined the limits of applicability of analytical expressions to calculate the probability of detecting the signal of the time window in sync QKDS for the two extreme cases, the appearance of the photon momentum: the photon momentum is completely within the analyzed time window or distributed between two adjacent windows. The estimation of the impact of the number of time windows and the relationship of the duration of the pulse to width of the time window on the detection probability in view of the appearance of a random photon pulse. It is shown that in order to reduce the time of uncertainty the duration of the time window should be 4 times the length of the photon momentum in the photon pulse duration of 1 ns, the repetition period of 1024 ns, the frequency of occurrence of dark counts pulses of 400 Hz, the average number of photoelectrons per photon pulse duration of 0.01 and a volume sample counts of registered pulses in each time window 200.

Quantum key distribution systems; the photon pulse synchronization.

Предисловие. Защита классических криптографических систем предполагает трудность взлома сообщений из-за ограниченных вычислительных мощностей. Защищённость систем при квантовом распределении ключей (КРК) опирается на фундаментальные законы квантовой физики и принципиально исключает возможность несанкционированного перехвата передаваемых сообщений [1−6].

Одной из важнейших составляющих эффективной работы систем КРК (СКРК) является синхронизация, задача которой сводится к фиксации момента приёма фотонного импульса однофотонными фотодетекторами. Для обеспечения синхронизации с высокой точностью измеряется общая длина пути распространения оптического импульса как в волоконно-оптической линии связи (ВОЛС), так и во всех функциональных компонентах внутри станций СКРК.

Обзор методов [7−9], применяемых для временной синхронизации, показал, что в силу квантовой природы для СКРК наиболее подходящей формой синхронизирующего сигнала является периодическая последовательность узких оптических импульсов. Временными маркерами здесь являются сами импульсы, а синхронизация достигается измерением момента прихода оптических сигналов [10−12].

Проведённые в [13−20] исследования подтверждают, что процессы формирования и распределения квантовых ключей в системе с фазовым кодированием проходят в однофотонном режиме, причём среднее число фотоэлектронов на импульс не превышает 0,1. Однако установлено [21, 22], что процесс синхронизации реализуется в многофотонном режиме, где среднее число фотоэлектронов на импульс порядка 1000. Это потенциально упрощает злоумышленнику организацию несанкционированного доступа к информации.

В [23−26] описан процесс вхождения в синхронизм СКРК с фазовым кодированием состояний фотонов и предложен алгоритм поиска фотонного импульса, обеспечивающий повышенную защищённость режима синхронизации от несанкционированного съёма информации. Полученные аналитические выражения позволяют оценить влияние параметров фотонного импульса и аппаратуры поиска на вероятность правильного обнаружения сигнального временного окна. В дальнейшем в [27] оценено влияние параметров фотонного импульса, однофотонных фотодетекторов и поисковой аппаратуры на вероятностные характеристики СКРК в режиме синхронизации.

Проведённый в [23] анализ с использованием разработанного программного обеспечения для ЭВМ [28, 29] 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. Это требует анализа режима синхронизации с учётом двух факторов. Во-первых, момент появления фотонного импульса случаен, а во-вторых, фотонный импульс может одновременно принадлежать двум соседним временным окнам.

В [30] исследованы два крайних случая временного момента появления фотонного импульса: фотонный импульс полностью располагается внутри анализируемого временного окна или распределяется поровну между двумя соседними окнами. Аналитические выражения доказывают, что в случае деления поровну фотонного импульса между двумя соседними временными окнами вероятность синхронизации системы КРК низка.

Цель исследований состоит с учётом возможности принадлежности синхронизирующего сигнала двум временным окнам из-за априорной неопределённости в отношении момента приёма фотонного импульса определить границы применимости аналитических выражений для расчёта вероятности обнаружения сигнального временного окна в режиме синхронизации СКРК для двух крайних случаев: фотонный импульс полностью располагается внутри анализируемого временного окна или поровну распределяется между двумя соседними окнами.

В процессе исследований предполагается оценить границы применимости аналитических выражений для вероятности обнаружения сигнального временного окна в режиме синхронизации СКРК для крайних случаев временного момента появления фотонного импульса.

Алгоритм синхронизации двухпроходных автокомпенсационных систем с фазовым кодированием состояний фотонов. Пусть в качестве счётчика фотоэлектронов (ФЭ) используется устройство, регистрирующее все принятые ФЭ за фиксированное время наблюдения. Считаются известными период следования T_s и длительность τ_s фотонного импульса, причём предполагается их абсолютная стабильность ΔT_s=0 и $\Delta \tau_s$=0.

Фиксируется момент t=0 начала поиска временного окна. Временной кадр, равный периоду следования оптических импульсов T_s, разбивается на N_w временных окон с длительностью τ_w, причём

$$T_s = N_w \tau_w. \quad (1)$$

Каждое временное окно опрашивается N раз, определяя объём выборки. Последнее эквивалентно опросу j-го окна во временных интервалах

$$t \in \left[(i-1)T_s + (j-1)\tau_w ; (i-1)T_s + j\tau_w \right], \; i = \overline{1, N}; \;\; j = \overline{1, N_w}. \quad (2)$$

При каждом опросе временного окна фиксируется количество принимаемых ФЭ и/или импульсов темнового тока (ИТТ). Случай отсутствия фотонного импульса в обследуемом временном окне подразумевает регистрацию только ИТТ. Такое временное окно считаем «шумовым».

В процессе синхронизации временное окно, в котором зарегистрировано максимальное число срабатываний, принимается за сигнальное временное окно.

Модель процессов в шумовом временном окне. Пусть известна частота появления ИТТ ξ_d. Тогда за длительность τ_w одного временного окна среднее число зарегистрированных ИТТ равно

$$\overline{n_{d.w}} = \xi_d \tau_w. \quad (3)$$

За выборку объёмом N среднее число регистрируемых ИТТ составит

$$\overline{n_{d.N}} = N \cdot \overline{n_{d.w}}. \quad (4)$$

Поскольку среднее число регистрируемых ИТТ за длительность шумового временного окна в СКРК крайне мало, то для описания статистических свойств потока ИТТ за выборку объёмом N используется закон Пуассона [31]

$$Pos\left\{ n_{d.N} \left| \overline{n_{d.N}} \right. \right\} = \frac{\left(\overline{n_{d.N}} \right)^{n_{d.N}}}{n_{d.N}!} \exp\left(-\overline{n_{d.N}} \right). \quad (5)$$

Модель процессов в сигнальном временном окне. Пусть $\overline{n_s}$ – среднее число ФЭ, принимаемых за длительность фотонного импульса. Считается, что момент появления t_1 фотонного импульса принадлежит первому временному окну. Данное утверждение не является критическим и принимается только для упрощения математических выкладок.

Если момент появления t_1 фотонного импульса принадлежит интервалу $\left[0, \tau_w - \tau_s\right]$ в первом временном кадре, то фотонный импульс полностью располагается внутри анализируемого окна. В этом случае за длительность τ_w сигнального временного окна будут регистрироваться как ФЭ, так и ИТТ. Причём их среднее количество равно

$$\overline{n_w} = \overline{n_{d.w}} + \overline{n_s} = \xi_d \tau_w + \overline{n_s}. \quad (6)$$

За выборку объёмом N среднее число регистрируемых ФЭ и ИТТ в сигнальном временном окне составит

$$\overline{n_{w.N}} = N \cdot \overline{n_w} = \overline{n_{d.N}} + \overline{n_{s.N}}, \quad (7)$$

где

$$\overline{n_{s.N}} = N \cdot \overline{n_s} \quad (8)$$

− среднее число регистрируемых ФЭ за выборку объёмом N.

Поскольку среднее число регистрируемых ФЭ и ИТТ за длительность сигнального временного окна по-прежнему мало, то для описания статистических свойств потока ФЭ и ИТТ за выборку объёмом N также используется закон Пуассона

$$Pos\left\{n_{w.N}\left|\overline{n_{w.N}}\right.\right\}=\frac{\left(\overline{n_{w.N}}\right)^{n_{w.N}}}{n_{w.N}!}\exp\left(-\overline{n_{w.N}}\right). \quad (9)$$

Напротив, если момент появления t_1 фотонного импульса принадлежит интервалу $\left[\tau_w-\tau_s,\,\tau_w\right]$ 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:

$$\overline{n_{w1}}=\overline{n_{d.w}}+\overline{n_{s1}}=\xi_d\tau_w+\overline{n_s}\left(\frac{\tau_w\,t_1}{\tau_s}\right). \quad (10)$$

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

$$\overline{n_{w2}}=\overline{n_{d.w}}+\left(\overline{n_s}-\overline{n_{s1}}\right)=\xi_d\tau_w+\left(\overline{n_s}-\overline{n_{s1}}\right). \quad (11)$$

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

$$\begin{aligned}\overline{n_{w1.N}}&=N\cdot\overline{n_{w1}}=\overline{n_{d.N}}+\overline{n_{s1.N}};\\ \overline{n_{w2.N}}&=N\cdot\overline{n_{w2}}=\overline{n_{d.N}}+\overline{n_{s2.N}},\end{aligned} \quad (12)$$

где

$$\begin{aligned}\overline{n_{s1.N}}&=N\cdot\overline{n_{s1}};\\ \overline{n_{s2.N}}&=N\cdot\overline{n_{s2}}\end{aligned} \quad (13)$$

− средние числа регистрируемых ФЭ за выборку объёмом N соответственно в первом и втором сигнальных временных окнах.

Поскольку среднее число регистрируемых ФЭ и ИТТ за длительность сигнального временного окна по-прежнему мало, то для описания статистических свойств потока ФЭ и ИТТ за выборку объёмом N также используется закон Пуассона

$$Pos\left\{n_{w.i.N}\left|\overline{n_{w.i.N}}\right.\right\}=\frac{\left(\overline{n_{w.i.N}}\right)^{n_{w.i.N}}}{n_{w.i.N}!}\exp\left(-\overline{n_{w.i.N}}\right),\ i=1;2. \quad (14)$$

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

$$\left\{n_{w.N}(j),\ j=\overline{1,N_w}\right\}=\left\{n_{w.N}(1),\,n_{w.N}(2),\,...,\,n_{w.N}(j),\,...,\,n_{w.N}(N_w)\right\}. \quad (15)$$

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 (5) с параметрами (3) и (4), а в сигнальном (первом) временном окне число $n_{w.N}(1)$ − законом (9) с параметрами (6)–(8).

Напротив, если момент появления t_1 фотонного импульса принадлежит интервалу $\left[\tau_w - \tau_s, \tau_w\right]$ в первом временном кадре, то фотонный импульс располагается одновременно в первом и втором временных окнах. Причём оба окна выступают в роли сигнальных. При этом в (15) значения чисел $n_{w.N}(3), ..., n_{w.N}(j), ..., n_{w.N}(N_w)$ в $N_w - 2$ шумовых временных окнах описываются законом Пуассона (5) с параметрами (3) и (4). В сигнальных временных окнах числа $n_{w.N}(1)$ и $n_{w.N}(2)$ – законом (14) с параметрами (10)–(13).

За сигнальное окно принимается временное окно, в котором зарегистрировано максимальное число срабатываний.

Случай принадлежности фотонного импульса одному временному окну. При нахождении импульса только в одном временном окне правильное обнаружение возможно только тогда, когда

$$\begin{cases} n_{w.N}(1) > 1; \\ n_{w.N}(1) > \left\{ n_{w.N}(2), ..., n_{w.N}(j), ..., n_{w.N}(N_w) \right\}. \end{cases} \quad (16)$$

Первое неравенство в (16) показывает, что для принятия правильного решения в сигнальном временном окне за время анализа должен быть зарегистрирован хотя бы один ФЭ или ИТТ. Второе условие в (16) определяет, что в каждом из оставшихся шумовых окнах число зарегистрированных ИТТ должно быть строго меньше зарегистрированных импульсов в сигнальном временном окне. С точки зрения анализа вероятностных характеристик положение временного окна, в которое попадает фотонный импульс, не имеет значения.

Предположим, что в сигнальном временном окне за выборку объёмом N зарегистрировано $n_{w.N}(1) = n_{w.N}$ ФЭ и ИТТ. Тогда с учётом (5) условная вероятность правильного обнаружения сигнального временного окна в первом анализируемом случае будет равна

$$P_{1d.N}\left\{n_{w.N}\right\} = \prod_{j=2}^{N_w} \left(\sum_{n_{w.N}(j)=0}^{n_{w.N}-1} \left(Pos\left\{ n_{d.N}(j) \middle| \overline{n_{d.N}} \right\} \right) \right).$$

Поскольку математические ожидания числа ИТТ за выборку объёмом N во всех шумовых временных окнах неизменны $\overline{n_{d.N}}$, то

$$P_{1d.N}\{n_{w.N}\} = exp[-(N_w - 1) \cdot \overline{n_{d.N}}] \cdot \left(\sum_{n_{d.N}=0}^{n_{w.N}-1} \frac{\overline{n_{d.N}}^{n_{d.N}}}{n_{d.N}!} \right)^{N_w - 1}. \quad (17)$$

Заметим, что расчёт по формуле (17) справедлив при одновременном выполнении двух условий. Во-первых, число регистрируемых ФЭ и ИТТ в сигнальном временном окне должно равняться $n_{w.N}(1) = n_{w.N}$. А во-вторых, момент появления фотонного импульса в первом временном кадре должен находиться внутри временного интервала $t_1 \in \left[0; \tau_w - \tau_s\right]$. Кроме того, из формулы (17) следует, что если фотонный импульс полностью располагается внутри анализируемого временного окна, то условная вероятность не зависит от момента его появления t_1.

Вероятность правильного обнаружения сигнального временного окна может быть найдена усреднением вероятности (17) по возможным значениям числа регистрируемых ФЭ и ИТТ за выборку объёмом N в сигнальном временном окне.

С учётом (9) находим вероятность правильного обнаружения сигнального временного окна при условии, что фотонный импульс полностью располагается внутри анализируемого окна,

$$P_{\mathrm{D1}} = \sum_{n_{w.N}=1}^{\infty} \frac{(\overline{n_{w.N}})^{n_{w.N}}}{n_{w.N}!} \cdot exp[-\overline{n_{w.N}}] \cdot P_{1d.N}\{n_{w.N}\}. \quad (18)$$

Вычисления по формуле (18) представляют определённые трудности из-за суммирования бесконечного числа слагаемых. Однако расчёты показывают, что при ограничении верхнего предела суммирования в формуле (18) числом, равным объёму выборки ($n_{w.N} = N$), гарантируется ничтожно малая погрешность вычисления вероятности правильного обнаружения сигнального временного окна, а ограничение числа слагаемых числом $(2{,}5 \ldots 3) \cdot N \cdot \overline{n_s}$ является достаточным для расчёта вероятности с погрешностью не хуже 0,02 %.

Для доказательства возможности использования формул (17) и (18) проведено имитационное моделирование процесса синхронизации. В качестве исходных данных при моделировании выступали: длительность фотонного импульса τ_s=1 нс; период следования T_s=1024 нс; частота появления импульсов темнового тока 400 Гц; среднее число ФЭ $\overline{n}_s$=0,01, принимаемых за длительность фотонного импульса; объём выборки отсчётов регистрируемых импульсов в каждом временном окне N=200.

Число статистических испытаний принималось равным 1000.

Выбор отношения длительности временного окна (τ_w=256 нс) к длительности фотонного импульса (τ_s=1 нс) равным 256 гарантирует, что фотонный импульс с вероятностью $p = 1 - \tau_s/\tau_w = 0{,}9960$ (99,6 %) принадлежит только одному временному окну. При этом количество временных окон составляет N_w=4.

Вероятность правильного обнаружения сигнального временного окна, полученная в результате моделирования, составляет 84,90 %. Сравнение со значением 85,13 %, полученным в результате расчётов по формулам (16)−(18), показывает их расхождение не более чем на 0,3 %.

Даже при числе временных окон N_w=256 и длительности временного окна τ_w=4 нс расхождение между результатами моделирования 0,829 и расчётами 0,8435 по формулам (16)−(18) не превышает 2 %. Хотя в последнем случае фотонный импульс принадлежит только одному временному окну лишь с вероятностью 75 %.

Таким образом, числовые результаты доказывают возможности использования аналитических выражений (16)−(18) для расчёта вероятности правильного обнаружения сигнального временного окна.

Случай деления фотонного импульса поровну между двумя соседними временными окнами. Рассмотрим частный случай взаимного временного расположения момента начала временного окна и момента появления в нём фотонного импульса. Случай предусматривает появление фотонного импульса в момент $t_1 = \tau_w - \tau_s/2$. При этом ровно половина фотонного импульса принадлежит первому временному окну, а его вторая половина – второму окну.

Тогда $\tau_w - t_1 = \tau_s - \tau_w + t_1$, $\overline{n_{s.N1}} = \overline{n_{s.N2}} = 0{,}5 \cdot \overline{n_{s.N}} = \overline{n_{s.h}}$ и $\overline{n_{w.N1}} = \overline{n_{w.N2}} = \overline{n_{d.N}} + \overline{n_{s.h}} = \overline{n_{w.h}}$. Соответственно вероятности принадлежности фотонного импульса первому и второму временным окнам будут равны $P_{D2} = P_{D3} = P_{Dh}$. Как следствие,

$$P_{D.h} = \sum_{n_{w.h}=1}^{\infty} \langle (pos\{n_{w.h}|\overline{n_{w.h}}\}) \cdot \left(\sum_{g=0}^{n_{w.h}-1} pos\{g|\overline{n_{w.h}}\} \right) \cdot P_{d.h}\{n_{w.h}\} \rangle \quad (19)$$

и

$$P_{2d.N}\{n_{w.N1}\} = P_{3d.N}\{n_{w.N2}\} = P_{d.h} = \left(\sum_{n_{d.h}=0}^{n_{w.h}-1} pos\{n_{d.h}|\overline{n_{d.N}}\} \right)^{N_w-2}. \quad (20)$$

Вероятность правильного обнаружения сигнального временного окна при появлении фотонного импульса в момент $t_1 = \tau_w - 0,5 \cdot \tau_s$ составит

$$P_{обн.h} = 2 \cdot P_{D.h}. \quad (21)$$

Расчёты показывают, что при ограничении верхнего предела суммирования в формуле (19) числом $n_{w.h} = N$ гарантируется ничтожно малая погрешность вычисления вероятности правильного обнаружения сигнального временного окна, а ограничение числа слагаемых числом $(2,5 \ldots 3) \cdot N \cdot \overline{n_s}$ является достаточным для расчёта вероятности с погрешностью 0,02 %.

Для доказательства возможности использования формул (19)–(21) проведено имитационное моделирование процесса синхронизации. В качестве исходных данных при моделировании выступали длительность 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 принимается равным 2 000.

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.

Для случая деления фотонного импульса поровну между двумя соседними временными окнами на рис. 1 сплошной линией представлен график зависимости вероятности правильного обнаружения сигнального временного окна от числа временных окон.

Из графика видно, что, несмотря на значительное изменение (в 512 раз) числа временных окон N_w (а, следовательно, и длительности временного окна с 512 до 1 нс), вероятность правильного обнаружения сигнального временного окна сохраняет практически постоянное значение. Так, например, при изменении числа временных окон N_w с 2 до 1024 вероятность при моделировании меняется от 71,95 до 66,75 %. Заметим, что аналитические выражения дают изменения в пределах от 69,89 до 67,03 %, причём с плавным падением с ростом числа временных окон.

Причина столь слабой зависимости вероятности правильного обнаружения от числа временных окон становится ясна при анализе поведения средних чисел ФЭ и ИТТ. Действительно, при изменении числа временных окон N_w с 2 до 1024, регистрируемое среднее число ИТТ во временном окне меняется в 512 раз, снижаясь до $8 \cdot 10^{-5}$. Среднее же число ФЭ, регистрируемое одним из двух сигнальных окон, в анализируемом случае остаётся постоянным и равным 1,0. Как следствие, среднее суммарное число ФЭ и ИТТ в сигнальных окнах изменяется от 1,04 до 1,00, т. е. не более чем на 4 %.

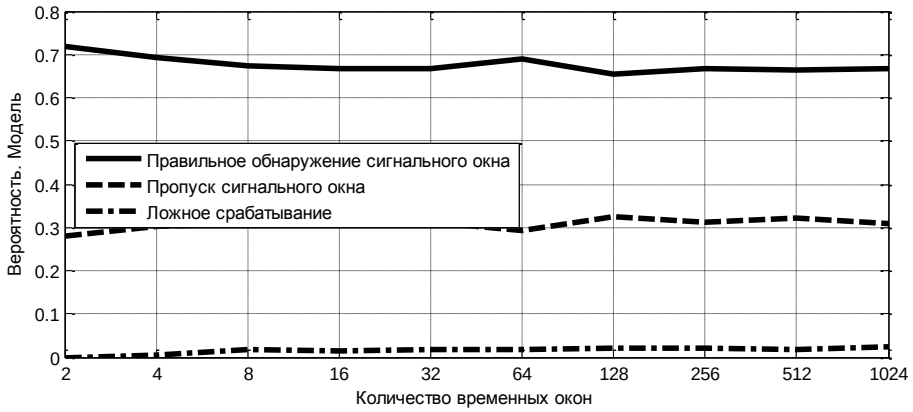

Рис. 1. Зависимость вероятностей правильного обнаружения (сплошная), пропуска (штриховая) и ложного срабатывания (штрихпунктирная линия) от числа окон для случая деления фотонного импульса поровну между окнами

Отметим, что в модели частота появления импульсов темнового тока принимается равной 400 Гц. Применяемые же в СКРК однофотонные лавинные фотодиоды id230 [32] гарантируют частоту появления ИТТ не более 100 Гц, а при охлаждении до минус 90 градусов по Цельсию – менее 25 Гц. Естественно, что в этих условиях вероятность правильного обнаружения практически не зависит от количества временных окон.

Следует обратить внимание на тот факт, что вероятность принятия ошибочного решения довольно велика (в районе 30 %). И это при том, что даже при двух временных окнах (длительность временного окна τ_w равна половине периода следования оптических импульсов T_s =1024 нс) различие между средними числами ФЭ и ИТТ $\overline{n_{s.N1}} = \overline{n_{s.N2}} = 1{,}04$ в сигнальных и ИТТ $\overline{n_{d.N}}$=0,041 в шумовых окнах за выборку объёмом 200 и достигает 25,4 раза. Различие возрастает до 12 500 раз при максимальном числе временных окон 1024, когда длительность окна τ_w равна длительности фотонного импульса τ_s=1 нс.

Причина высокой вероятности принятия ошибочного решения связана с делением энергии (фотоэлектронов) фотонного импульса поровну между соседними окнами. Напомним, что случай равенства количества регистрируемых импульсов в любых временных окнах (включая и соседние сигнальные окна) рассматривается аппаратурой синхронизации как ложное срабатывание.

На рис. 1 штриховой линией представлена полученная в результате моделирования зависимость вероятности регистрации равного количества импульсов в двух соседних временных окнах Pr_{eq} (вероятности пропуска сигнального окна), между которыми поровну разделён фотонный импульс. Видно, что эта вероятность составляет порядка 30 % и является определяющей в вероятности принятия ошибочного решения.

Это подтверждает график штрихпунктирной линией на рис. 1, где представлена зависимость от количества временных окон вероятности $P_{err\text{ИТТ}} = 1 - P_{\text{обн}.h} - -Preq$, которая определяет вероятность принятия ошибочного решения из-за превышения числа накопленных ИТТ с одного из шумовых окон над количеством импульсов с сигнальных окон (вероятность ложного срабатывания). Значения вероятности не превышает 3 % во всем диапазоне изменений количества временных окон.

Отметим, что значения вероятности регистрации равного количества импульсов в двух соседних сигнальных временных окнах Pr_{eq} хорошо согласуются с расчётами по формуле

$$Pr_{eq.th} = \sum_{i\geq 0} \frac{\overline{n_{s.N1}}^{2i}}{(i!)^2} \cdot exp(-2 \cdot \overline{n_{s.N1}}) .$$

Различие расчётов по формуле с результатами моделирования не превышают 1 %.

На рис. 2 показаны зависимости от числа временных окон вероятностей правильного обнаружения для случая деления фотонного импульса поровну между соседними окнами, полученные в результате моделирования (сплошная линия) или посредством расчётов (штриховая линия) по формулам (19)−(21). Здесь же штрихпунктирной линией представлены результаты моделирования случая принадлежности фотонного импульса только одному временному окну, рассчитанные по формулам (17)−(18).

Сравнение двух первых графиков показывает практически их полное совпадение во всём диапазоне изменений числа временных окон. Расхождения между теоретическими результатами и данными моделирования не превышают 1 %. Это доказывает возможность использования аналитических выражений (19)−(21) для расчёта вероятности правильного обнаружения сигнального временного окна для случая деления фотонного импульса поровну между соседними окнами.

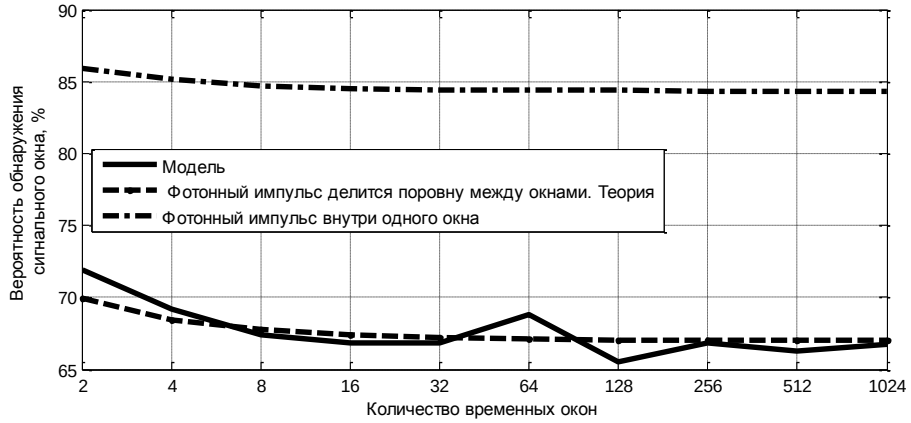

Рис. 2. Зависимость вероятности правильного обнаружения от числа окон для случая деления фотонного импульса поровну между соседними окнами

Сравнение трёх графиков на рис. 2 показывает, что частный случай принадлежности фотонного импульса в равной степени двум временным окнам определяет нижний предел вероятности правильного обнаружения. Из-за случайного момента появления фотонного импульса внутри временного окна график зависимости безусловной вероятности правильного обнаружения сигнального временного окна от числа временных окон будет располагаться между графиками, изображёнными штриховой и штрихпунктирной линиями. Причём он будет тяготиться к штрихпунктирной линии с уменьшением числа временных окон.

Оценка влияния отношения длительности временного окна к длительности импульса на вероятность правильного обнаружения с учетом случайного момента появления фотонного импульса во временном окне. Результаты имитационного моделирования процесса вхождения в синхронизм с учётом случайного момента появления фотонного импульса в первом временном окне представлены сплошной линией на рис. 3. В качестве исходных данных при моделиро-

вании выступали ранее описанные параметры фотонного импульса, однофотонного фотоприёмника и аппаратуры вхождения в синхронизм. Число статистических испытаний равно 5000.

Зависимость, рассчитанная по формулам (17)−(18) и представленная штриховой линией, предполагает принадлежность фотонного импульса только одному временному окну. Зависимость, рассчитанная по формулам (19)−(21) и представленная штрихпунктирной линией, иллюстрирует частный случай, при котором импульс распределяется поровну между двумя соседними окнами.

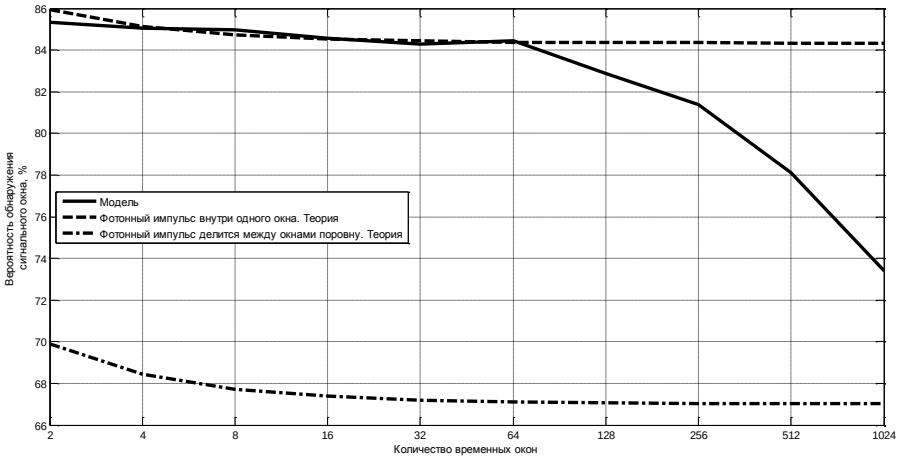

Рис. 3. Зависимость вероятности правильного обнаружения от числа временных окон с учётом случайного момента появления фотонного импульса

Заметим, что результаты моделирования, как и предсказывалось ранее, располагаются внутри границ, очерченных двумя другими графиками. Причём в границах от 2 до 256 окон различие между результатами моделирования и рассчитанными по формулам (17)−(18) не превышает 2 %. И это при том, что при N_w=256 (при отношении длительности временного окна 4 нс к длительности фотонного импульса 1 нс, равном 4) вероятность принадлежности фотонного импульса двум окнам при моделировании составляет 25,7 % (теоретически 25 %). Даже при N_w=512 (отношение длительности временного окна 2 нс к длительности фотонного импульса 1 нс равно 2) различие между результатами моделирования и расчётов по формулам (17)−(18) не превышает 8 %.

Лишь в предельном случае, когда отношение длительности временного окна равно длительности фотонного импульса 1 нс (N_w=1024), результат моделирования 73,38 % ниже вероятности 84,34 %, получаемой при ориентации на случай принадлежности фотонного импульса только одному временному окну. Хотя и здесь различие не превышает 13 %.

Поскольку в предельном случае (N_w=1024) фотонный импульс всегда распределяется между двумя соседними окнами, то результат моделирования выше, чем для случая деления фотонного импульса поровну между двумя соседними временными окнами 67,03 % (различие и здесь не превышает 11 %).

Особое внимание обратим на результаты моделирования при другом предельном случае N_w=1. Здесь решение об обнаружении сигнального временного окна принимается при регистрации хотя бы одного ФЭ или ИТТ. Вероятность такого события равна

$$P_{\mathrm{D1}}\left(\mathrm{N_W}=1\right)=1-exp[-\overline{n_{w.N}}]$$

и теоретически должна составлять 0,8753, что отличается от результатов моделирования 0,8815 всего на 0,7 %.

Следует обратить внимание на парадокс, вытекающий из результатов моделирования. Действительно, как в теории, так и при моделировании, максимальная вероятность правильного обнаружения сигнального временного окна обеспечивается при равенстве длительности временного окна и периода следования оптических импульсов (при одном временном окне N_w=1). Однако при этом сохраняется исходная неопределённость в отношении момента приёма фотонного импульса, поскольку факт присутствия фотонного импульса в анализируемом временном интервале, равном периоду следования оптических синхронизирующих импульсов, априорно известен.

Естественно принять, что для уменьшения временной неопределённости в отношении момента приёма фотонного импульса число временных окон должно превышать два (N_w≥2). Поскольку в диапазоне от 2 до 256 временных окон вероятность правильного обнаружения сигнального временного окна практически постоянна (изменение в диапазоне 85,34…82,88 %), то выбор следует остановить на числе временных окон N_w=256. При этом можно говорить об уменьшении первоначальной временной неопределённости в отношении момента приёма фотонного импульса в 256 раз.

В пользу такого выбора говорит и анализ графиков на рис. 4, полученных в процессе моделирования. Здесь сплошной линией представлена зависимость вероятности правильного обнаружения от числа временных окон с учётом случайного момента появления фотонного импульса. Штриховой линией представлена зависимость от числа временных окон вероятности равенства числа регистрируемых ФЭ и ИТТ в двух сигнальных окон (вероятность пропуска). Наконец, штрихпунктирная линия отображает зависимость от числа окон вероятности принятия ошибочного решения из-за превышения максимального числа зарегистрированных ИТТ среди шумовых окон над максимальным числом зарегистрированных ФЭ и ИТТ среди сигнальных временных окон (вероятность ложного срабатывания).

Из рис. 4 видно, что при числе временных окон между 256 и 512 значения двух составляющих, определяющих вероятности принятия ошибочного решения, сравниваются. Причём, если при отношении длительности временного окна к длительности фотонного импульса, равном 4 вероятности пропуска и ложного срабатывания составляют соответственно 6,10 и 12,5 %, то при отношении 2 уже в обратную сторону 13,28 и 8,62 %. Наконец, при равенстве длительностей временного окна и фотонного импульса вероятность пропуска более чем в 10 раз превышает ложное срабатывание (24,52 % против 2,10 %).

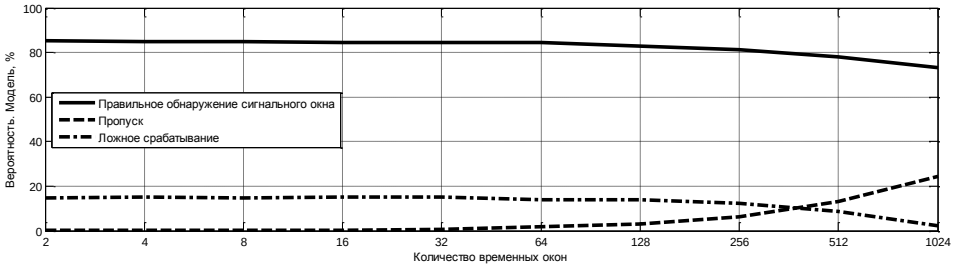

Рис. 4. Результаты моделирования процесса вхождения в синхронизм

Можно говорить о выборе числа временных окон таким образом, чтобы длительность временного окна в 4 раза превышала длительность фотонного импульса.

Выводы. Проанализирован предварительный этап синхронизации двухпроходной СКРК, предполагающий разбиение периода посылки синхросигналов на временные окна и обнаружение сигнального окна с фотонным импульсом. Особенность исследуемого алгоритма синхронизации состоит в том, что он реализуется в однофотонном режиме, затрудняя злоумышленнику использовать часть энергии сигнального импульса и тем самым повышая безопасность СКРК.

Исследования позволили посредством статистического моделирования определить границы применимости аналитических выражений для расчёта вероятности обнаружения сигнального временного окна в режиме синхронизации СКРК для двух крайних случаев: фотонный импульс полностью располагается внутри анализируемого временного окна или распределяется между двумя соседними окнами. Дана оценка влияния числа временных окон и отношения длительности окна к длительности импульса на вероятность правильного обнаружения с учётом случайного момента появления фотонного импульса. Показано, что для уменьшения временной неопределённости длительность временного окна в 4 раза должна превышать длительность фотонного импульса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, № 1. – P. 145-195.
2. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / Под ред. Д. Боумейстера, А. Экерта, А. Цайлингера: Пер. с англ. С.П. Кулика, Е.А. Шапиро. – М.: Постмаркет, 2002. – 376 с.
3. Квантовая криптография: идеи и практика / Под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. – Минск: Беларуская навука, 2008. – 392 с.
4. *Румянцев К.Е.* Системы квантового распределения ключа: монография. − Таганрог: Изд-во ТТИ ЮФУ, 2011. − 264 с.
5. *Kilin S.Y.* Diamond-based quantum information technologies // Physics, chemistry and application of nanostructures / Ed. by V. Borisenko, S. Gaponenko, V. Gurin. – Singapore: World Scientific, 2007. – P. 3-14.
6. *Румянцев К.Е.* Квантовая коммуникация: теория, эксперименты, приложения. В кн. «Информационно-телекоммуникационные и компьютерные технологии, устройства и системы в Южном федеральном университете. – Ростов-на-Дону: Изд-во ЮФУ, 2010. – С. 213-247.
7. *Румянцев К.Е., Розова Я.С.* Патентно-лицензионная ситуация в области квантовой криптографии // Электротехнические и информационные комплексы и системы. – 2011. – Т. 7, № 1. – С. 3-10.
8. *Румянцев К.Е., Голубчиков Д.М., Розова Я.С.* Квантовая криптография: теория, эксперименты, приложения. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – 156 с.
9. *Голубчиков Д.М., Румянцев К.Е.* Квантовая криптография: принципы, протоколы, системы // Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению "Информационно-телекоммуникационные системы". – 2008. – 37 с.
10. *Гальярди Р.М., Карп Ш.* Оптическая связь: Пер. с англ. / Под ред. А.Г. Шереметьева. − М.: Связь, 1978. – 424 с.
11. *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.
12. *Golubchikov D.M., Rumiantsev K.E.* The probabilistic model of keys generation of QKD systems // The 4-th world congress in the XXI-st century. 21–23 september 2010. – Kiev: 2010. − P. 17.51-17.53.

13. *Румянцев К.Е., Плёнкин А.П.* Стенд для научных исследований квантово-криптографической системы // Современные тенденции в образовании и науке: сборник научных трудов по материалам Международной научно-практической конференции 31 октября 2013 г.: в 26 частях. Ч. 2. − Тамбов: Изд-во ТРОО «Бизнес–Наука–Общество», 2013. – С. 108-111.
14. *Rumyantsev K.E., Golubchikov D.M.* Modeling of Quantum Key Distribution System for Secure Information Transfer: Chapter 15. In the book «Integrated Models for Information Communication Systems and Networks: Design and Development». − IGI Global (USA), 2013. − P. 314-342.
15. *Румянцев К.Е., Плёнкин А.П.* Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей // Телекоммуникации. – 2014. – № 10. – С. 11-16.
16. *Плёнкин А.П.* Использование квантовых ключей в сетевой информационной безопасности // Наука и сучасність: виклики XXI століття. Ч. II (технічні науки, історичні науки): Міжнародна конференція, м. Київ, 31 січня 2014 р. Центр наукових публікацій. – С. 98-100.
17. *Румянцев К.Е., Плёнкин А.П.* Натурные испытания коммерческой системы квантового распределения ключей // Доклады VI Пленума СибРОУМО по образованию в области информационной безопасности и XV конференции: Томск–Иркутск, 9–13 июня 2014 г. – Томск: В-Спектр, 2014. – С. 120-125.
18. *Плёнкин А.П.* Квантово-криптографическая сеть на основе системы квантового распределения ключей // Информационная безопасность и защита персональных данных: Проблемы и пути их решения: Материалы VI Межрегиональной научно-практической конференции. – Брянск: БГТУ, 2014. – С. 103-106.
19. *Розова Я.С., Румянцев К.Е.* Исследование влияния характеристик узлов системы квантовой криптографии на процесс формирования ключевых последовательностей // Сборник VII Всероссийской НПК «Молодёжь и современные информационные технологии». Томск. 25–27.02.2009. Ч. 1. – Томск: Изд-во СПБ “График С”. – С. 57-58.
20. *Плёнкин А.П.* Использование квантовых ключей для шифрования сетевого соединения // Десятая ежегодная научная конференция студентов и аспирантов базовых кафедр Южного научного центра РАН: Тезисы докладов (г. Ростов-на-Дону, 14−29 апреля 2014 г.). – Ростов-на-Дону: Изд-во ЮНЦ РАН, 2014. – С. 81-82.
21. *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.
22. *Плёнкин А.П.* Повышение защищённости процесса вхождения в синхронизм системы квантового распределения ключей // Сборник научных трудов. IV Международная конференция по фотонике и информационной оптике. Москва, 28−30 января 2015 г. – М.: НИЯУ МИФИ. – С. 212-213.
23. *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.
24. *Плёнкин А.П.* Защищённость режима синхронизации системы квантового распределения ключей // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: Сборник статей I Всероссийской научно-технической конференции молодых ученых, аспирантов и студентов. – Таганрог: Изд-во ЮФУ, 2015. – С. 240-243.
25. *Плёнкин А.П.* Повышение защищенности режима синхронизации системы квантового распределения ключей // Сборник материалов международной научно-практической конференции «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації»: Зб. наук. праць науково-практичної конференції; м. Київ, 25–28 лютого 2015р., Європейський університет. – Киів: Вид-во Європейського університету, 2015. – С. 85-87.
26. *Плёнкин А.П. Румянцев К.Е.* Однофотонный режим синхронизации системы квантового распределения ключей // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Ч. I. – Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ, 2015. – С. 498-501.

27. *Плёнкин А.П.* Исследование режима вхождения в синхронизм при использовании фотонных импульсов системы квантового распределения ключа // ES-ФМ-2014-011. Физико-математические методы и информационные технологии в естествознании, технике и гуманитарных науках: сборник материалов международного научного е-симпозиума. Россия, г. Москва, 27–28 декабря 2014 г. [Электронный ресурс]. – Киров: МЦНИП, 2015. – С. 101-113.
28. *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 № 2015613500 РФ. Правообладатель: ФГАОУВО «Южный федеральный университет», г. Ростов-на-Дону (RU). – Заявка 2014660503 от 16.10.2014. Дата регистрации 17.03.2015.
29. *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: ФГАОУВО «Южный федеральный университет», г. Ростов-на-Дону (RU). – Заявка 2014661772 от 20.11.2014. Дата регистрации 20.01.2015.
30. *Плёнкин А.П. Румянцев К.Е.* Зависимость вероятности обнаружения фотонного импульса в режиме синхронизации системы квантового распределения ключей от длительности временного окна // ES-Т-ФМ-2015-011. Технические и естественные науки: теория и практика: сборник материалов международного научного е-симпозиума, г. Москва, 27−28 марта 2015 г. [Электронный ресурс]. – Киров: МЦНИП, 2015. – С. 59-72.
31. *Шереметьев А.Г.* Статистическая теория лазерной связи. – М.: Связь, 1971. – 264 с.
32. http://www.idquantique.com/wordpress/wp-content/uploads/id230-specs.pdf.

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. Fizika kvantovoy informatsii: Kvantovaya kriptografiya. Kvantovaya teleportatsiya. Kvantovye vychisleniya [Physics of quantum information: Quantum cryptography. Quantum teleportation. Quantum computing], Under ed. D. Boumeystera, A. Ekerta, A. Tsaylingera: Translation from English S.P. Kulika, E.A. Shapiro. Moscow: Postmarket, 2002, 376 p.
3. Kvantovaya kriptografiya: idei i praktika [Quantum cryptography: concepts and practices], Under ed. S.Ya. Kilina, D.B. Khoroshko, A.P. Nizovtseva. Minsk: Belaruskaya navuka, 2008, 392 p.
4. *Rumyantsev K.E.* Sistemy kvantovogo raspredeleniya klyucha: Monografiya [System of quantum key distribution: a Monograph]. Taganrog: Izd-vo TTI YuFU, 2011, 264 p.
5. *Kilin S.Y.* Diamond-based quantum information technologies, *Physics, chemistry and application of nanostructures*, Ed. by V. Borisenko, S. Gaponenko, V. Gurin. Singapore: World Scientific, 2007, pp. 3-14.
6. *Rumyantsev K.E.* Kvantovaya kommunikatsiya: teoriya, eksperimenty, prilozheniya. V kn. «Informatsionno–telekommunikatsionnye i komp'yuternye tekhnologii, ustroystva i sistemy v Yuzhnom federal'nom universitete [Quantum communication: theory, experiments, applications. In the book "Information and telecommunication and computer technologies, devices and systems at southern Federal University]. Rostov-on-Don: Izd-vo YuFU, 2010, pp. 213-247.
7. *Rumyantsev K.E., Rozova Ya.S.* Patentno–litsenzionnaya situatsiya v oblasti kvantovoy kriptografii [Patent and licensing situation in the field of quantum cryptography], *Elektrotekhnicheskie i informatsionnye kompleksy i sistemy* [Electrical and data processing facilities and systems], 2011, Vol. 7, No. 1, pp. 3-10.
8. *Rumyantsev K.E., Golubchikov D.M., Rozova Ya.S.* Kvantovaya kriptografiya: teoriya, eksperimenty, prilozheniya [Quantum cryptography: theory, experiments, applications]. Taganrog: Izd-vo TTI YuFU, 2010, 156 p.
9. *Golubchikov D.M., Rumyantsev K.E.* Kvantovaya kriptografiya: printsipy, protokoly, sistemy [Quantum cryptography: principles, protocols, systems], *Vserossiyskiy konkursnyy otbor obzorno-analiticheskikh statey po prioritetnomu napravleniyu "Informatsionno-telekommunikatsionnye sistemy"* [Nationwide competitive selection survey and analytical articles on priority area "Information-telecommunication systems"], 2008, 37 p.

10. *Gal'yardi R.M., Karp Sh.* Opticheskaya svyaz' [Optical communications]: Translation from English, Ed. by A.G. Sheremet'eva. Moscow: Svyaz', 1978, 424 p.
11. *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 phase coding of States of photons], *Izvestiya vuzov Rossii. Radioelektronika* [Izvestiia VUZov. Radioelektronika], 2011, No. 6, pp. 26-38.
12. *Golubchikov D.M., Rumiantsev K.E.* The probabilistic model of keys generation of QKD systems, *The 4-th world congress in the XXI–st century. 21–23 september 2010*. Kiev: 2010, pp. 17.51-17.53.
13. *Rumyantsev K.E., Plenkin A.P.* Stend dlya nauchnykh issledovaniy kvantovo-kriptograficheskoy sistemy [Stand for research of quantum cryptographic systems], *Sovremennye tendentsii v obrazovanii i nauke: sbornik nauchnykh trudov po materialam Mezhdunarodnoy nauchno–prakticheskoy konferentsii 31 oktyabrya 2013 g*. [Modern trends in science and education: collection of scientific works on materials of the International scientific–practical conference on 31 October 2013]: In 26 parts. Parte. 2. Tambov: Izd-vo TROO «Biznes–Nauka–Obshchestvo», 2013, pp. 108-111.
14. *Rumyantsev K.E., Golubchikov D.M.* Modeling of Quantum Key Distribution System for Secure Information Transfer: Chapter 15. In the book «Integrated Models for Information Communication Systems and Networks: Design and Development». IGI Global (USA), 2013, pp. 314-342.
15. *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.
16. *Plenkin A.P.* Ispol'zovanie kvantovykh klyuchey v setevoy informatsionnoy bezopasnosti [The use of quantum keys in network information security], *Nauka i suchasnist': vikliki XXI stolittya. Chastina II (tekhnichni nauki, istorichni nauki): Mizhnarodna konferentsiya, m. Kiiv, 31 sichnya 2014 r. Tsentr naukovikh publikatsiy* [Science and modernity: challenges of the XXI century. – Part II (technical Sciences, historical Sciences): international conference, Kiev, January 31, 2014 Center for scientific publications], pp. 98-100.
17. *Rumyantsev K.E., Plenkin A.P.* Naturnye ispytaniya kommercheskoy sistemy kvantovogo raspredeleniya klyuchey [Field tests of a commercial system for quantum key distribution], *Doklady VI Plenuma SibROUMO po obrazovaniyu v oblasti informatsionnoy bezopasnosti i XV konferentsii: Tomsk–Irkutsk, 9–13 iyunya 2014 g* [Reports of the VI Plenum of Dibromo education in the field of information security and XV conference: Tomsk–Irkutsk, 9-13 June 2014]. Tomsk: V-Spektr, 2014, pp. 120-125.
18. *Plenkin A.P.* Kvantovo-kriptograficheskaya set' na osnove sistemy kvantovogo raspredeleniya klyuchey [Quantum cryptographic network based on the system of quantum key distribution], *Informatsionnaya bezopasnost' i zashchita personal'nykh dannykh: Problemy i puti ikh resheniya: Materialy VI Mezhregional'noy nauchno-prakticheskoy konferentsii* [Information security and personal data protection: Problems and their solutions: proceedings of the VI inter-regional scientific-practical conference]. Bryansk: BGTU, 2014, pp. 103-106.
19. *Rozova Ya.S., Rumyantsev K.E.* Issledovanie vliyaniya kharakteristik uzlov sistemy kvantovoy kriptografii na protsess formirovaniya klyuchevykh posledovatel'nostey [Study of the influence of the characteristics of the nodes of a quantum cryptography system on the formation of key sequences], Sbornik VII Vserossiyskoy NPK «Molodezh' i sovremennye informatsionnye tekhnologii». Tomsk. 25–27.02.2009 [The VII all-Russian collection of NPK "Youth and modern information technologies". Tomsk. 25-27.02.2009]. Part 1. Tomsk: Izd-vo SPB Grafik S, pp. 57-58.
20. *Plenkin A.P.* Ispol'zovanie kvantovykh klyuchey dlya shifrovaniya setevogo soedineniya [The use of quantum keys for encryption of the network connection], *Desyataya ezhegodnaya nauchnaya konferentsiya studentov i aspirantov bazovykh kafedr Yuzhnogo nauchnogo tsentra RAN: Tezisy dokladov (g. Rostov-na-Donu, 14−29 aprelya 2014 g.)* [Tenth annual scientific conference of students and postgraduates of basic departments of the Southern scientific center of Russian Academy of Sciences: Abstracts (Rostov-on-don, 14-29 April 2014).]. Rostov-on-Don: Izd-vo YuNTs RAN, 2014, pp. 81-82.

21. *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, № 5, pp. 54-66.
22. *Plenkin A.P.* Povyshenie zashchishchennosti protsessa vkhozhdeniya v sinkhronizm sistemy kvantovogo raspredeleniya klyuchey [Improving the security of the process of entering into synchronism system of quantum key distribution], *Sbornik nauchnykh trudov. IV Mezhdunarodnaya konferentsiya po fotonike i informatsionnoy optike. Moskva, 28−30 yanvarya 2015 g* [Collection of scientific works. IV international conference on Photonics and information optics. Moscow, 28-30 January 2015]. Moscow: NIYaU MIFI, pp. 212-213.
23. *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.
24. *Plenkin A.P.* Zashchishchennost' rezhima sinkhronizatsii sistemy kvantovogo raspredeleniya klyuchey [Security mode synchronization system of quantum key distribution], *Fundamental'nye i prikladnye aspekty komp'yuternykh tekhnologiy i informatsionnoy bezopasnosti: Sbornik statey I Vserossiyskoy nauchno-tekhnicheskoy konferentsii molodykh uchenykh, aspirantov i studentov* [Fundamental and applied aspects of computer technology and information security: a Collection of articles I all-Russian scientific-technical conference of young scientists, postgraduates and students]. Taganrog: Izd-vo YuFU, 2015, pp. 240-243.
25. *Plenkin A.P.* Povyshenie zashchishchennosti rezhima sinkhronizatsii sistemy kvantovogo raspredeleniya klyuchey [Improving the security mode synchronization system of quantum key distribution], Sbornik materialov mezhdunarodnoy nauchno-prakticheskoy konferentsii «Aktual'ni pitannya zabezpechennya kibernetichnoï bezpeki ta zakhistu informatsiï»: Zb. nauk. prats' naukovo-praktichnoï konferentsiï; m. Kiïv, 25-28 lyutogo 2015r., Єvropeys'kiy universitet [Proceedings of the international scientific-practical conference "Topical issues of cyber security and information protection": Sat. Sciences. proceedings of scientific-practical conference, Kiev, 25-28 February 2015, The European University]. Kiev: Vid-vo Єvropeys'kogo universitetu, 2015, pp. 85-87.
26. *Plenkin A.P. Rumyantsev K.E.* Odnofotonnyy rezhim sinkhronizatsii sistemy kvantovogo raspredeleniya klyuchey [Single-photon mode synchronization system of quantum key distribution], *Trudy Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta svyazi i informatiki* [Proceedings of Severo-Kavkazskiy branch of Moscow technical University of communications and Informatics]. Part I. Rostov-on-Don: PTs «Universitet» SKF MTUSI, 2015, pp. 498-501.
27. *Plenkin A.P.* Issledovanie rezhima vkhozhdeniya v sinkhronizm pri ispol'zovanii fotonnykh impul'sov sistemy kvantovogo raspredeleniya klyucha [Study of the mode of entering into synchronism when using photon pulses of a system of quantum key distribution], *ES-FM-2014-011. Fiziko-matematicheskie metody i informatsionnye tekhnologii v estestvoznanii, tekhnike i gumanitarnykh naukakh: Sbornik materialov Mezhdunarodnogo nauchnogo e-simpoziuma. Rossiya, g. Moskva, 27-28 dekabrya 2014 g*. [ES-FM-2014-011. Physico-mathematical methods and informational technologies in science, technology and the Humanities: proceedings of the International scientific e-Symposium. Russia, Moscow, 27-28 December 2014], [Electronic resource]. Kirov: MTsNIP, 2015, pp. 101-113.
28. *Rumyantsev K.E., Plenkin A.P.* Modelirovanie protsessa sinkhronizatsii sistemy kvantovogo raspredeleniya klyucha pri ispol'zovanii fotonnykh impul'sov dlya povysheniya zashchishchennosti [Modeling of process synchronization system of quantum key distribution using photon pulses to make it more secure], Svidetel'stvo ob ofitsial'noy registratsii programmnogo produkta dlya EVM № 2015613500 RF. Pravoobladatel': FGAOUVO «Yuzhnyy federal'nyy universitet», g. Rostov-na-Donu (RU) [The certificate of official registration of software for computers No. 2015613500 of the Russian Federation. Holder: GAOWO "southern Federal University", Rostov-on-don (RU)]. Application 2014660503 dated 16.10.2014. Registration date: 17.03.2015.

29. *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 system of quantum key distribution using for the registration of photon pulses single-photon avalanche photo-detector to make it more secure], *Svidetel'stvo ob ofitsial'noy registratsii programmnogo produkta dlya EVM № 2015610876 RF. Pravoobladatel': FGAOUVO «Yuzhnyy federal'nyy universitet», g. Rostov-na-Donu (RU)* [The certificate of official registration of software for computers No. 2015610876 of the Russian Federation. Holder: GAOWO "southern Federal University", Rostov-on-Don (RU)]. Application 2014661772 dated 20.11.2014. Registration date: 20.01.2015.
30. *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 synchronization mode of the system of quantum key distribution on the duration of the time window], *ES-T-FM-2015-011. Tekhnicheskie i estestvennye nauki: teoriya i praktika: Sbornik materialov Mezhdunarodnogo nauchnogo e-simpoziuma, g. Moskva, 27–28 marta 2015 g.* [ES-T-FM-2015-011. Technical and natural Sciences: theory and practice: proceedings of the International scientific e-Symposium, Moscow, 27-28 March 2015]. [Electronic resource]. Kirov: MTsNIP, 2015, pp. 59-72.
31. *Sheremet'ev A.G.* Statisticheskaya teoriya lazernoy svyazi [Statistical theory of laser communication]. Moscow: Svyaz', 1971, 264 p.
32. Available at: http://www.idquantique.com/wordpress/wp-content/uploads/id230-specs.pdf.

Статью рекомендовал к опубликованию д.т.н., профессор О.И. Шелухин.

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.