7. *Gruzman I.S., Kirichuk V.S., Kosykh V.P., Peretyagin G.I., Spektor A.A.* Tsifrovaya obra-botka izobrazheniy v informatsionnykh sistemakh [Digital image processing in information systems]: Uchebnoe posobie. Novosibisrk: Izd-vo NGTU, 2002, 352 p.
8. *Akushskiy I.Ya., Yuditskiy D.I.* Mashinnaya arifmetika v ostatochnykh klassakh [Machine arithmetic in residual classes]. Moscow: Sovetskoe radio, 1968, 440 p.
9. *Omondi, Amos R., and Benjamin Premkumar.* Residue number systems theory and implementation. London: Imperial College Press, 2007, 296 p.
10. *Amerbaev V.M.* Teoreticheskie osnovy mashinnoy arifmetiki [Theoretical foundations of computer arithmetic. Alma-Ata: Nauka, 1976, 323 p.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Абасова Анастасия Михайловна – Южный федеральный университет; e-mail: moonriel@yandex.ru; 347928, г. Таганрог, ул. Чехова, 22; тел.:+79615006290; кафедра безопасности информационных технологий; аспирантка.

Abasova Anastasiya Mikhailovna – Southern Federal University; e-mail: moonriel@yandex.ru; 22, Chekhova street, Taganrog, 347928, Russia; phone: +79615006290; the department of security in data processing technologies; postgraduate student.

УДК 621.396.624:621.396.96

К.Е. Румянцев, А.П. Плёнкин

СИНХРОНИЗАЦИЯ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА ПРИ ИСПОЛЬЗОВАНИИ ФОТОННЫХ ИМПУЛЬСОВ ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ*

Исследования посвящены оценке вероятностных характеристик системы квантового распределения ключа (СКРК) в режиме вхождения в синхронизм. Описаны методы синхронизации оптических систем, принцип действия которых основывается на приёме многофотонных и фотонных импульсов. Предложен алгоритм поиска фотонного импульса при использовании идеального счетчика фотоэлектронов, на основе которого разработана программа для ЭВМ, имитирующая алгоритм вхождения в синхронизм системы КРК на предварительном этапе поиска. Получены аналитические выражения для расчёта вероятностных характеристик СКРК на предварительном этапе поиска при использовании фотонных импульсов для повышения защищённости СКРК от несанкционированного съёма информации. Оценено влияние параметров фотонного импульса, однофотонного фотоэмиссионного прибора и аппаратуры поиска при идеальной регистрации фотонов на вероятность правильного обнаружения сигнального временного окна. Определено выражение для расчёта предельно реализуемой вероятности ошибочного обнаружения сигнального временного окна. Обоснован выбор параметров аппаратуры поиска, фотонного импульса, однофотонного детектора. Предложена методика проектирования СКРК в режиме вхождения в синхронизм при идеальной однофотонной регистрации. Квантовое распределение ключа; защищённость, синхронизация; фотонный импульс, вероятность обнаружения.

Квантовое распределение ключа; защищённость, синхронизация; фотонный импульс; вероятность обнаружения.

* 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.

K.Y. Rumyantsev, A.P. Pljonkin

SYNCHRONIZATION OF QUANTUM KEY DISTRIBUTION SYSTEM USING PHOTON PULSES TO IMPROVE THE SECURITY

The research is to assess the probabilistic characteristics of quantum key distribution system (QKDS) in synchronization mode. Synchronization methods of optical systems are described. Algorithm of photon pulse search with ideal photon counting system are proposed. PC program for imitation of first stage QKDS synchronization search algorithm is developed. Expressions for calculation of the probability characteristics QKDS on the first stage searching using photon pulses to enhance security from eavesdropping are obtained. The influence of the photon pulse parameters, the single-photon detector and equipment search with ideal photoelectrons counter by the properly probability are evaluated. Expressions for calculation a limit probability of wrong signal detection. A method for designing QKDS in synchronization mode are proposed.

Quantum keys distribution; security; synchronization; photon pulse; detection probability.

Введение. В основу криптографических систем положен принцип защиты, заключающийся в трудности взлома сообщений из-за ограниченных вычислительных мощностей [1]. В отличие от классических криптосистем, защищённость которых основывается на математических предположениях, защищённость квантовых криптографических систем опирается на фундаментальные законы квантовой механики, что при надлежащей реализации в системах квантового распределения ключа (КРК) принципиально исключает возможность несанкционированного съёма передаваемых сообщений третьими лицами [2–6].

Эффективная работа СКРК возможна только при условии синхронизации, под которой понимается знание временного момента приёма фотонного импульса для подачи стробирующего импульса на однофотонные фотодетекторы. Для обеспечения синхронизации необходимо с высокой точностью определить общую длину оптического пути распространения фотонов как в волоконно-оптической линии связи между двумя станциями, так и во всех функциональных узлах внутри СКРК.

Проблема временной синхронизации исследована для каналов с аддитивными гауссовскими шумами [7]. В силу квантовой природы системы КРК полностью отличаются от традиционных хотя бы различными моделями выходного сигнала фотодетектора.

Для оптических систем наиболее подходящей формой синхросигнала считается периодическая последовательность узких оптических импульсов. Временными маркерами (отметками) в этом случае являются сами импульсы, а синхронизация достигается измерением моментов прихода оптических сигналов. Проблема аналитического исследования процедуры синхронизации периодической последовательностью оптических импульсов формулируется как проблема оценки времени прихода синхронизирующего сигнала. При этом процедура оценки времени прихода периодической последовательности импульсов сводится к выполнению двух операций. Первая операция обеспечивает грубое обнаружение, сводящееся к дискретизации периода посылки синхросигнала на временные интервалы (окна) и обнаружению сигнального окна с оптическим импульсом. Второй операцией, более точной, является измерение дополнительного временного сдвига, составляющей доли интервала дискретизации.

В [7] описаны алгоритмы синхронизации оптических систем, принцип действия которых основывается на многофотонных импульсах.

Известен метод [8], в котором используются два импульса: 1) мощный опорный (многофотонный); 2) слабый фотонный сигнальный. Если импульсы во времени жёстко «связаны» (синхронизированы), то фиксация момента приёма первого импульса однозначно определяет момент появления фотонного импульса. Од-

нако присутствие мощного первого оптического импульса упрощает злоумышленнику процесс вхождения в синхронизм для организации последующего несанкционированного съёма информации.

Среди успешно реализованных коммерческих СКРК отдельно стоит отметить двухпроходные автокомпенсационные волоконно-оптические системы с фазовым кодированием, которые отличаются устойчивой работоспособностью при изменяющихся внешних условиях. Механизм синхронизации в таких системах описан в [2]. Многофотонный импульс лазера, сгенерированный станцией Алиса, разделяется оптическим делителем на два импульса, которые проходят по двум разным волоконно-оптическим «плечам» интерферометра Маха–Цендера и посылается на станцию Боб по волоконно-оптической линии связи (ВОЛС). Здесь происходит их ослабление до фотонного уровня и переотражение от поляризационного зеркала назад в ВОЛС. При обратном распространении через ВОЛС импульса происходит компенсация ранее имевших место поляризационных и фазовых искажений. После интерференции фотонный импульс регистрируется одним из двух однофотонных детекторов станции Алиса. Синхронизация моментов излучения и прихода импульсов осуществляется за счёт отведения части оптической мощности на синхронизирующие генераторы станции Боб.

Процессы генерации и распределения квантовых ключей в системе проходят в фотонном режиме. Считается, что среднее число фотоэлектронов на импульс при этом составляет порядка 0,1. Однако процесс вхождения в синхронизм реализуется в многофотонном режиме, что позволяет злоумышленнику использовать часть энергии для синхронизации своей аппаратуры.

Цель исследований состоит в оценке вероятностных характеристик СКРК в режиме вхождения в синхронизм при использовании фотонных импульсов для повышения защищённости системы от несанкционированного съёма информации.

Вероятностные характеристики СКРК в режиме вхождения в синхронизм (процесс предварительного поиска сигнального временного окна) при идеальной однофотонной регистрации. Пусть в качестве идеального счётчика фотоэлектронов (ФЭ) – первичных электронов с фотокатода однофотонного фотоэмиссионного прибора (ОФЭП) – используется устройство, регистрирующее все принятые ФЭ за фиксированное время наблюдения. В процессе поиска момента прихода оптических сигналов считаются известными период следования T_s и длительность τ_s фотонных импульсов, причём предполагается их абсолютная стабильность ΔT_s=0 и $\Delta \tau_s$=0.

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

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

Каждое временное окно опрашивается N_t раз, определяя размер выборки. Последнее эквивалентно опросу i-го временного окна во временных интервалах

$$t \in \left[(i-1) T_{след}; (i-1) T_s + \tau_w \right], i = \overline{1, N_t}. \qquad (2)$$

При каждом опросе временного окна фиксируется количество принимаемых фотоэлектронов (ФЭ) и/или импульсов темнового тока (ИТТ).

Рассмотрим случай отсутствия оптических импульсов в обследуемом временном окне. В этом случае во время опроса такого шумового временного окна могут регистрироваться только ИТТ.

Пусть известна частота (скорость, интенсивность) появления ИТТ ξ_d. Тогда за длительность τ_w одного временного окна количество зарегистрированных ИТТ составит в среднем

$$\overline{n_{d.w1}} = \xi_d \tau_w. \quad (3)$$

За выборку объёмом N_t количество регистрируемых ИТТ составит в среднем

$$\overline{n_{d.w}} = N_t \overline{n_{d.w1}}. \quad (4)$$

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_t справедливо использовать закон Пуассона [9]

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

Рассмотрим случай присутствия фотонных импульсов в обследуемом сигнальном временном окне. Пусть $\overline{n_s}$ – среднее число сигнальных ФЭ, принимаемых за длительность фотонного импульса.

В этом случае во время опроса сигнального временного окна могут регистрироваться как ФЭ, так и ИТТ. Тогда за длительность τ_w сигнального временного окна будет регистрироваться в среднем следующее количество импульсов:

$$\overline{n_{w1}} = \overline{n_{d.w1}} + \overline{n_s} = \xi_d \tau_w + \overline{n_s}. \quad (6)$$

При анализе предполагается, что длительность временного окна τ_w значительно превышает длительность оптического импульса τ_s. Кроме того, считается, что фотонный импульса не может принадлежать одновременно двум соседним временным окнам.

За выборку объёмом N_t количество регистрируемых ФЭ и ИТТ в сигнальном временном окне составит в среднем

$$\overline{n_w} = N_t \overline{n_{w1}} = \overline{n_{d.w}} + \overline{n_{s.w}}, \quad (7)$$

где

$$\overline{n_{s.w}} = N_t \overline{n_s}, \quad (8)$$

− среднее число регистрируемых ФЭ за выборку объёмом N_t.

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_t также используется закон Пуассона

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

После последовательного (или параллельного) опроса всех N_w временных окон формируется массив значений зарегистрированных ФЭ и/или ИТТ

$$n_w = \{n_w(1), n_w(2), ..., n_w(j), ..., n_w(N_w)\}. \quad (10)$$

В (10) значения чисел в $N_w - 1$ шумовых временных окнах описываются законом Пуассона (5) с параметрами (3) и (4), а в одном сигнальном временном окне – законом (9) с параметрами (6)–(8).

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

Пусть фотонный импульс находится в 1-м временном окне. Тогда правильное обнаружение возможно только тогда, когда

$$\begin{cases} n_w(1) > 1; \\ n_w(1) > \{n_w(2), ..., n_w(j), ..., n_w(N_w)\}. \end{cases} \quad (11)$$

Первое неравенство в (11) показывает, что для правильного принятия решения в сигнальном временном окне за время анализа должен быть зарегистрирован хотя бы один ФЭ или ИТТ. Второе условие в (11) определяет, что в каждом из оставшихся шумовых окон число зарегистрированных ИТТ должно быть строго меньше зарегистрированных импульсов в сигнальном временном окне.

Заметим, что с точки зрения анализа вероятностных характеристик положение временного окна, в которое попадает фотонный импульс, не имеет роли.

Предположим, что в сигнальном временном окне зарегистрировано $n_w(1) = n_w$ ФЭ и ИТТ. Тогда с учётом (5) условная вероятность правильного обнаружения сигнального временного окна будет равна

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

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

$$P_D\{n_w\} = \left(\sum_{n=0}^{n_w-1} Pos\left\{ n \middle| \overline{n_{d.w}} \right\} \right)^{N_w-1}. \quad (12)$$

Вероятность (безусловная) правильного обнаружения сигнального временного окна в режиме предварительного поиска может быть найдена усреднением вероятности (12) по возможным значениям чисел регистрируемых ФЭ и ИТТ за выборку объёмом N_t в сигнальном временном окне. С учётом (9) находим

$$P_D = \sum_{n_w=1}^{\infty} Pos\left\{ n_w \middle| \overline{n_w} \right\} \cdot P_D\{n_w\}. \quad (13)$$

Вероятность (безусловная) ошибочного обнаружения (пропуска) сигнального временного окна в режиме предварительного поиска составит

$$P_E = 1 - P_D. \quad (14)$$

Важность обнаружения сигнального временного окна с наибольшей вероятностью на первом (предварительном) этапе определяется тем, что результирующая вероятность правильной синхронизации при любом количестве последующих этапов не может превышать вероятность правильного обнаружения сигнала на первом этапе.

Полученные аналитические выражения (12)–(14) позволяют оценить влияние параметров фотонного импульса, ОФЭП и аппаратуры поиска на вероятностные характеристики СКРК в режиме вхождения в синхронизм.

Однако сложность такого анализа связана с вычислительными трудностями при расчётах из-за необходимости суммирования бесконечного числа слагаемых в формуле (13). Заметим, что суммируется произведение двух сомножителей, значения которых не превышают единицы. Следовательно, можно утверждать, что всегда будет выполняться неравенство

$$\sum_{n_w=1}^{\infty} Pos\left\{n_w \middle| \overline{n_w}\right\} \geq \sum_{n_w=1}^{\infty} Pos\left\{n_w \middle| \overline{n_w}\right\} P_D\left\{n_w\right\}.$$

Поскольку

$$\sum_{n_w=1}^{\infty} Pos\left\{n_w \middle| \overline{n_w}\right\} = 1 - Pos\left\{n_w = 0 \middle| \overline{n_w}\right\} = 1 - \exp(-\overline{n_w}),$$

то

$$\sum_{n_w=1}^{\infty} Pos\left\{n_w \middle| \overline{n_w}\right\} P_D\left\{n_w\right\} \leq 1 - \exp(-\overline{n_w}). \tag{15}$$

Пусть первоначально (при первой итерации) в формуле (15) выполнено суммирование n_w от 1 до $k = k(1)$:

$$P_{D1} = \sum_{n_w=1}^{k} Pos\left\{n_w \middle| \overline{n_w}\right\} \cdot P_D\left\{n_w\right\}. \tag{16}$$

Разница между истинным P_D и приближённым P_{D1} значениями определяет погрешность расчёта вероятности правильного обнаружения сигнального временного окна ε_D. Естественно, что при этом уже не будут выполняться равенства $\sum_{n_w=1}^{k} Pos\left\{n_w \middle| \overline{n_w}\right\}$ и $1 - \exp(-\overline{n_w})$. Возникшая разница между этими величинами позволяет ввести в рассмотрение ещё одну погрешность $\varepsilon_n = \varepsilon_n(1)$, причём (в процентах)

$$\varepsilon_n = 100\left(1 - \frac{\sum_{n_w=1}^{k} Pos\left\{n_w \middle| \overline{n_w}\right\}}{1 - \exp(-\overline{n_w})}\right), \%. \tag{17}$$

Следовательно, задав значение погрешности $\varepsilon_n = \varepsilon_{n1}$ на первом шаге (итерации) и использовав формулу (17), определяется значение $k = k_1$. Расчёт по формулам (12) и (16) при ограниченном суммировании по $n_w = \overline{1, k_1}$ даёт первое значение вероятности P_{D1}, которое представляет первую грубую оценку снизу вероятности правильного обнаружения сигнального временного окна. Естественно, чтобы обеспечить требуемую погрешность расчёта вероятности правильного обнаружения сигнального временного окна ε_{D0}, необходимо при новом меньшем значении погрешности ε_{n2} на втором шаге (итерации) провести аналогичные расчёты для получения второго значения вероятности P_{D2}. Проводится сравнение двух полученных значений посредством вычисления достигнутой погрешности

$$\varepsilon_{D1} = 100\left(1 - \frac{P_{D1}}{P_{D2}}\right), \%\,. \qquad (18)$$

Если $\varepsilon_{D1} \le \varepsilon_{D0}$, то считается, что значение P_{D2} и есть искомая вероятность правильного обнаружения сигнального окна: $P_D = P_{D2}$.

В противном случае процесс итераций повторяется. При новой m-й итерации выбирается новое (меньшее) значение погрешности $\varepsilon_{n.m}$ и, применяя формулы (12), (16) и (17), рассчитывается новое значение вероятности $P_{D.m}$ и погрешности

$$\varepsilon_{D.(m-1)} = 100\left(1 - \frac{P_{D.(m-1)}}{P_{D.m}}\right), \%. \qquad (19)$$

Если $\varepsilon_{D.(m-1)} \le \varepsilon_{D0}$, то расчёт прекращается, а значение $P_{D.m}$ принимается за искомую вероятность правильного обнаружения сигнального временного окна: $P_D = P_{D.m}$.

Блок-схема алгоритма расчёта вероятности правильного обнаружения сигнального временного окна при синхронизации в СКРК в соответствии с формулами (12), (16)–(19) представлена на рис. 1.

Анализ влияния параметров фотонного импульса, ОФЭП и поисковой аппаратуры на вероятностные характеристики СКРК в режиме вхождения в синхронизм. Полученные аналитические выражения (12)–(14) с учётом упрощений (16)–(19) позволяют провести анализ влияния параметров фотонного импульса, ОФЭП и поисковой аппаратуры на вероятностные характеристики СКРК в режиме вхождения в синхронизм.

На рис. 2 представлены графики зависимостей вероятности ошибочного обнаружения сигнального временного окна на предварительном этапе поиска от значений среднего числа ФЭ за время анализа сигнального временного окна при фиксированных значениях среднего числа ИТТ за время анализа. Общее количество анализируемых временных окон принято считать равным 100. Полагается, что фотонный импульс может присутствовать только в одном временном (сигнальном) окне. Остальные 99 окон выступают в роли шумовых временных окон. Среднее число ФЭ за всё время анализа сигнального временного окна принимает значения в диапазоне от 1 до 15 с шагом 1. Среднее число ИТТ за время анализа шумового временного окна принимает дискретные значения 0,01; 0,02; 0,05 и 0.1.

Из семейства графиков (см. рис. 2) видно, что с увеличением среднего числа ФЭ, например, в 3,5 раза (в пределах от 2 до 7), при среднем числе ИТТ $\overline{n_{d.w}}$ =0,01 за время анализа, вероятность ошибочного обнаружения снижается в 6 раз (с 0,3 до 0,05).

Все графики на рис. 2 строились при заданном значении допустимой погрешности расчёта вероятности правильного обнаружения сигнального окна (ε_{D0} = 0,01 %). Достоверность полученных результатов подтверждается тем, что реально достигнутая погрешность вероятности правильного обнаружения при расчётах не превышала заданную величину. Это подтверждается графиками на рис. 3.

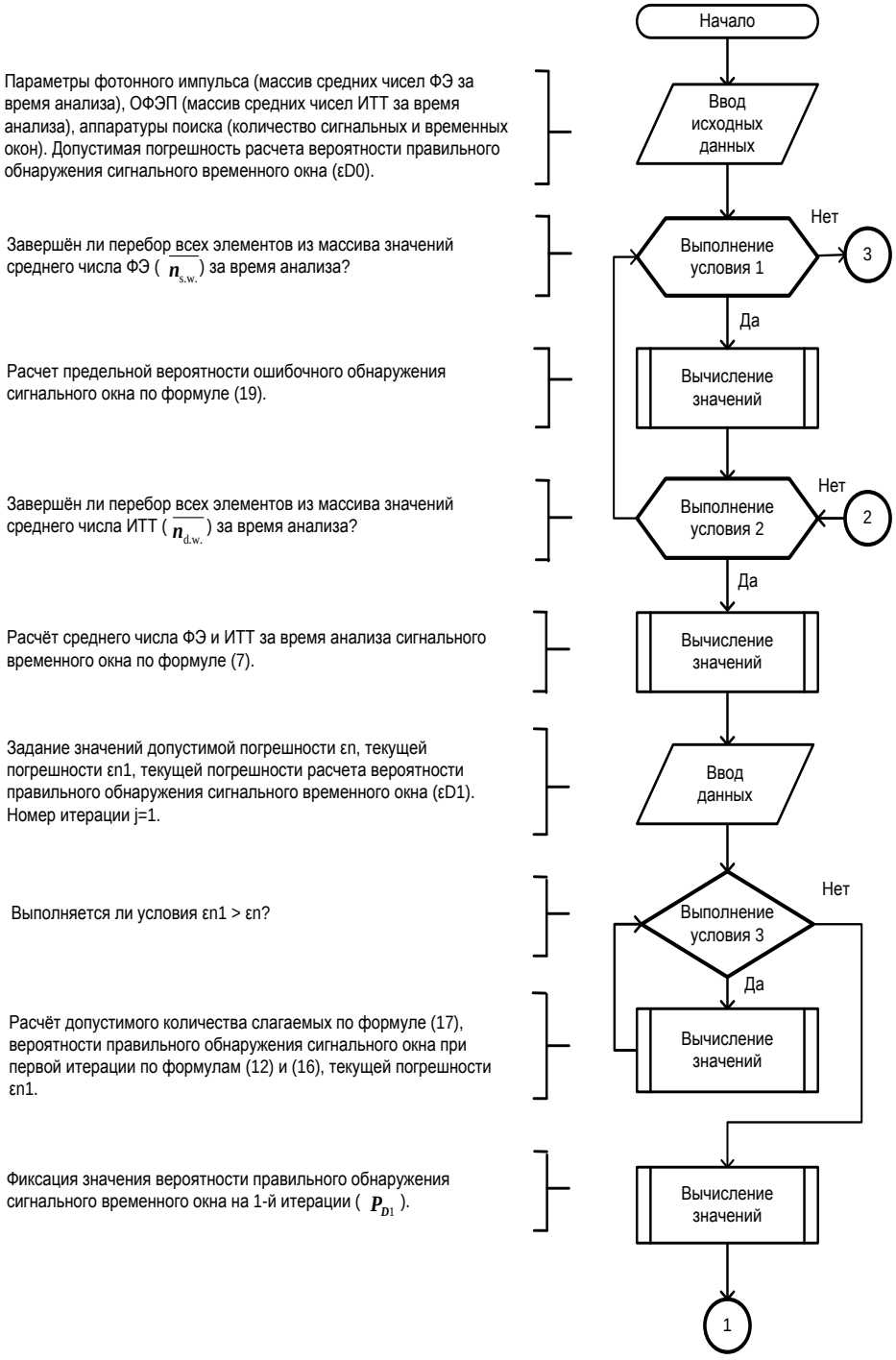

Рис. 1. Блок-схема алгоритма расчёта вероятности правильного обнаружения сигнального временного окна

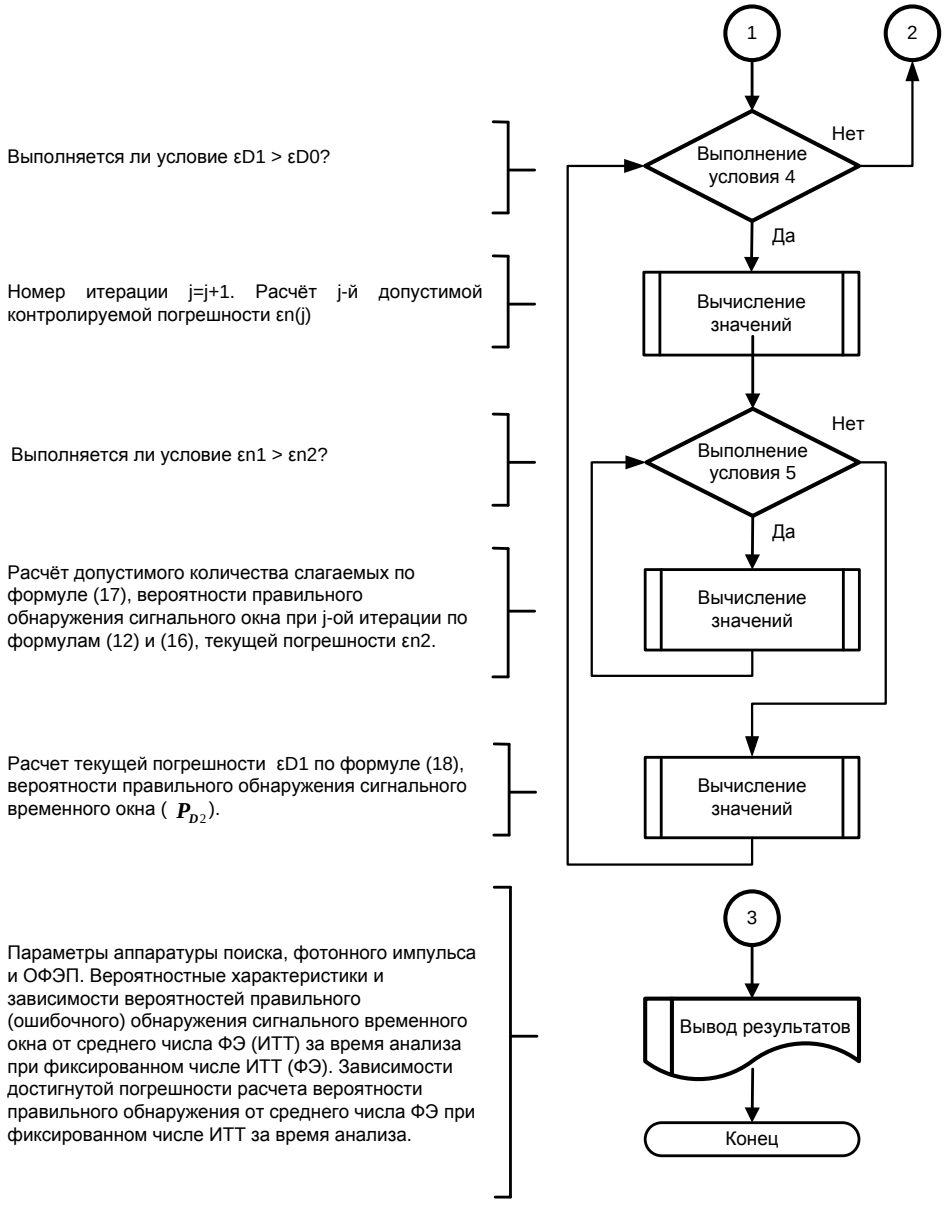

Рис. 1. (Окончание)

Все остальные зависимости, описывающие реально достигнутые погрешности расчёта, не превышают допустимый уровень. Так, например, при среднем числе ИТТ $\overline{n_{d.w}} = 0{,}02$ максимальное и минимальное значения достигнутой погрешности равны соответственно 0,0093 и 0,0042 в диапазоне изменений среднего числа ФЭ за время анализа от 8 до 10. Отметим, что «изрезанность» этих зависимостей связана с тем, что вычисления производились только при целом среднем числе ФЭ за время анализа сигнального окна.

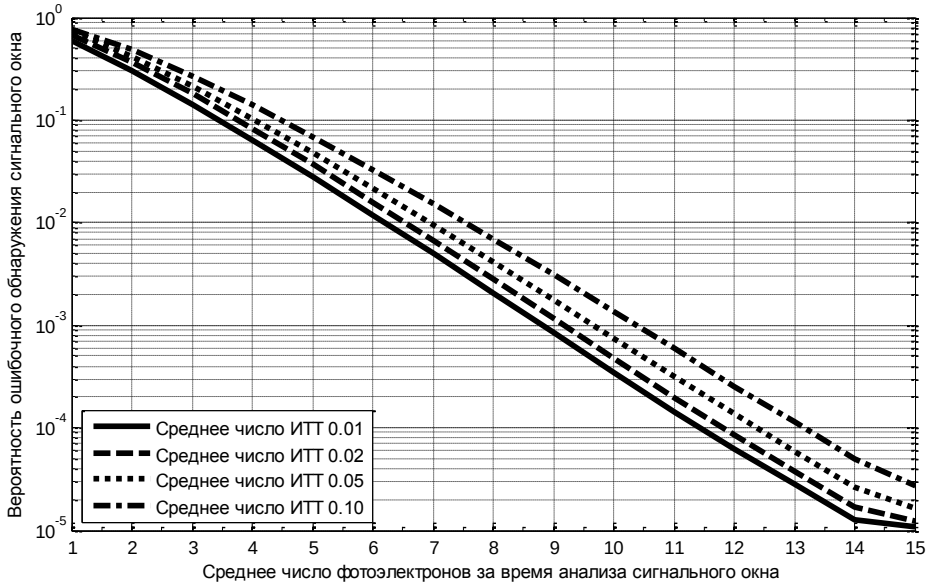

Рис. 2. Зависимости вероятности ошибочного обнаружения сигнального временного окна от среднего числа ФЭ за время анализа

Следует отметить наблюдаемые отклонения изменений вероятности ошибочного обнаружения сигнального временного окна от монотонного характера при большом среднем числе регистрируемых ФЭ. Так, например, при задании погрешности расчёта вероятности правильного обнаружения равной 0,1 %, наблюдались отклонения от монотонного характера вероятности ошибочного обнаружения в пределах от 0,0001 до 0,00007 в диапазоне средних чисел ФЭ от 12 до 15. Однако при снижении значения допустимой погрешности до 0,01 % функция приобретала монотонный характер. При этом в том же диапазоне средних чисел ФЭ, вероятность ошибочного обнаружения изменялась в пределах от 0,0001 до 0,00001 (см. рис. 2).

Определённый интерес представляет рис. 4, на котором представлена зависимость достаточного количества суммирований (учитываемого количества ФЭ и ИТТ) в формуле (16) от среднего числа ФЭ за время анализа сигнального временного окна. Из графических зависимостей, как и следовало ожидать, видно, что расчёты вероятности правильного или ошибочного обнаружения по формулам (12) и (16) требуют суммирования большего числа слагаемых. Так, например, если при среднем числе ФЭ за время анализа $\overline{n_{s.w}}$ =1 потребуется суммирование 8-ми слагаемых, то при $\overline{n_{s.w}}$ =12 − уже порядка 30-ти. Следует отметить практически линейную зависимость числа суммируемых слагаемых от среднего числа ФЭ за время анализа. Особо отметим практическое отсутствие влияния среднего числа регистрируемых ИТТ. Расхождения зафиксированы только при малых значениях среднего числа ФЭ за время анализа. Так, например, в диапазоне изменений среднего числа ФЭ от 1 до 5 зафиксирована разница всего в одно слагаемое.

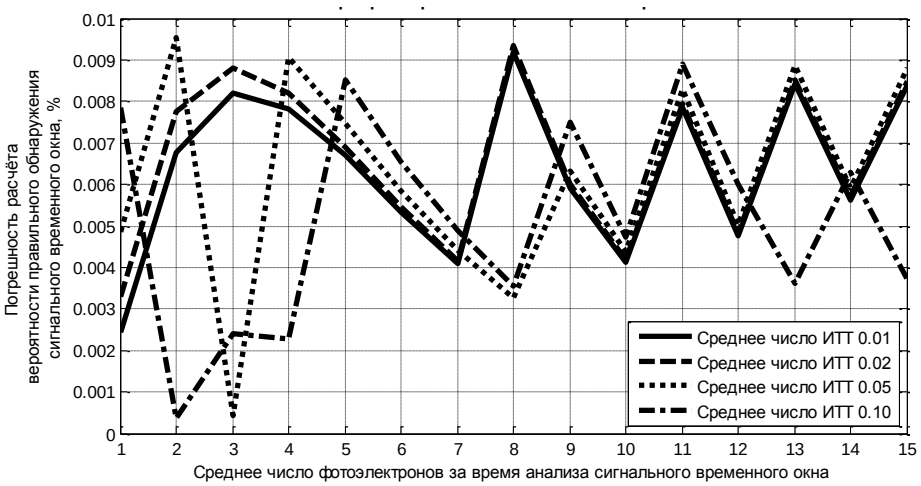

Рис. 3. Зависимости достигнутой погрешности расчёта вероятности правильного обнаружения сигнального временного окна от среднего числа ФЭ за время анализа

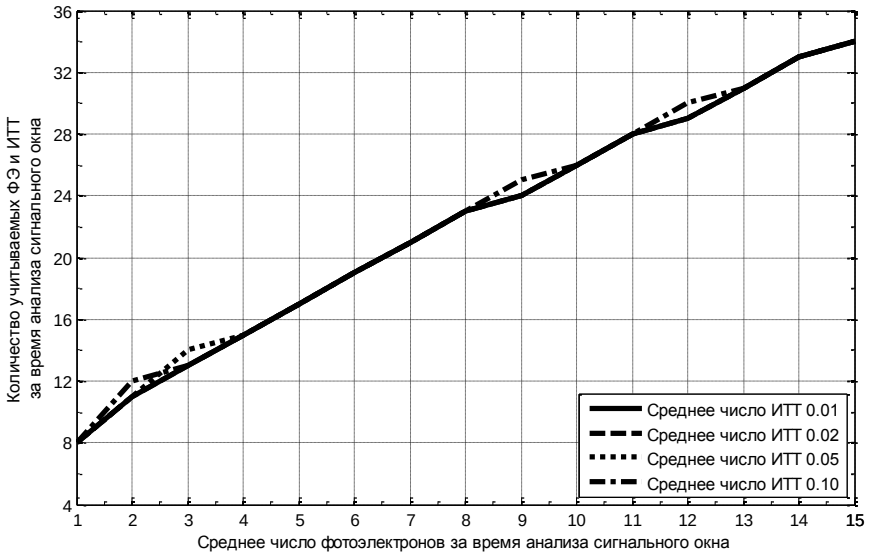

Рис. 4. Зависимости числа суммирований в формуле (16) для обеспечения погрешности расчёта вероятности правильного обнаружения сигнального временного окна в 0,01 %

На рис. 5 даны графики зависимости погрешности, определяющей достаточное количество суммирований (учитываемого количества ФЭ и ИТТ) в формуле (16), от среднего числа ФЭ за время анализа сигнального временного окна. Видно, что обеспечение требуемой допустимой погрешности определения вероятности правильного обнаружения сигнального временного окна (ε_{D0}=0,01 %) возможно только при выборе на два порядка более низкой погрешности ε_n, определяющей количество суммируемых слагаемых в формуле (16). Из графиков на рис. 5 видно,

что при среднем числе ФЭ ($\overline{n_{s.w}}$) от 1 до 15 и среднем числе ИТТ ($\overline{n_{d.w}}$) от 0,01 до 0,1, погрешность, определяющая достаточное количество суммирований в формуле (16), не превышает 0,001 %. При тех же средних числах ФЭ и ИТТ из рис. 3 видно, что значение погрешности вероятности правильного обнаружения не превышает требуемого значения 0,01 %. Следовательно, приступая к расчету вероятности правильного обнаружения сигнального временного окна с требуемой погрешностью ε_{D0}, можно при первой итерации ориентироваться на значение

$$\varepsilon_{n1} = \varepsilon_{D0} / 10. \quad (20)$$

Использование условия (20) позволяет снизить вычислительные затраты, что имеет высокую значимость с практической точки зрения.

Интерес представляет предельный случай, когда среднее число регистрируемых ИТТ равно нулю ($\overline{n_{d.w}} = 0$). При этом вероятность ошибочного обнаружения сигнального временного окна возможна лишь при условии, что не будет зарегистрированных ФЭ. Для этого случая вероятность ошибочного обнаружения сигнального временного окна определяется выражением $\exp\left(-\overline{n_{s.w}}\right)$ и, следовательно, может рассматриваться как предельно реализуемая вероятность (рис. 6).

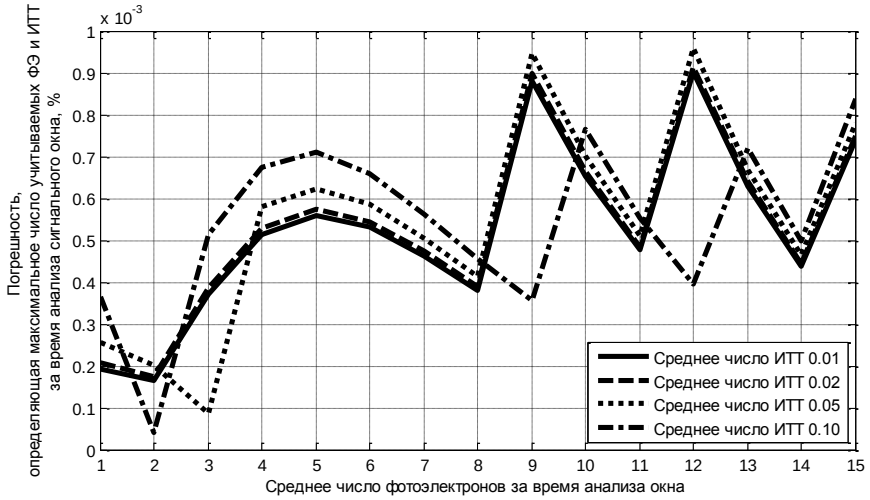

Рис. 5. Графики зависимостей погрешности, определяющей достаточное количество суммирований в формуле (16), от среднего числа ФЭ за время анализа сигнального временного окна

Из графика на рис. 6 можно заключить, что для получения вероятности ошибочного обнаружения не ниже 0,01 достаточным количеством ФЭ будет являться значение, превышающее 4,5.

Представленная на рис. 6 характеристика может использоваться для выбора минимального числа ФЭ, превышение которого гарантирует получение меньшего значения вероятности ошибочного обнаружения.

Полученные соотношения и графические зависимости позволяют предложить методику проектирования СКРК в режиме вхождения в синхронизм (процесс предварительного поиска сигнального временного окна) при идеальной однофотонной регистрации.

Методика проектирования СКРК в режиме вхождения в синхронизм при идеальной однофотонной регистрации. Исходными данными для проектирования СКРК в режиме предварительного поиска сигнального временного окна при использовании идеального однофотонного регистратора выступают параметры сигнального фотонного импульса, ОФЭП и аппаратуры поиска.

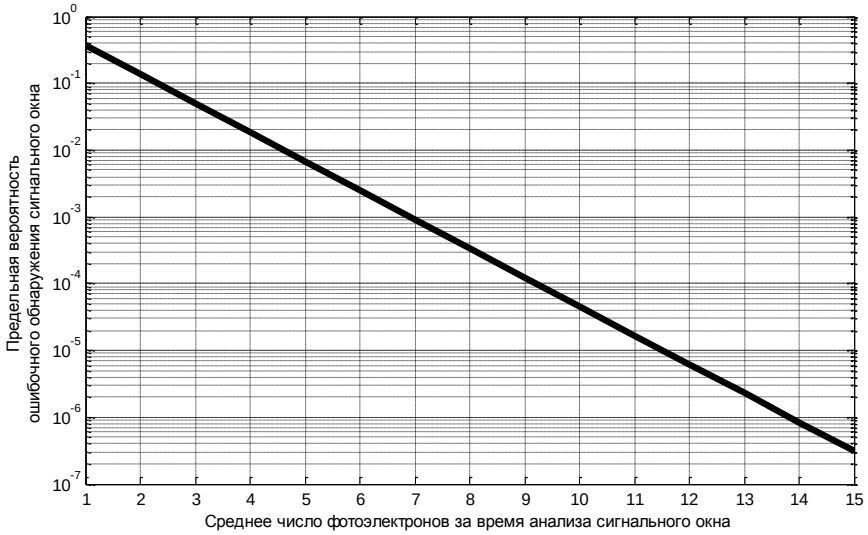

Рис. 6. Графики зависимостей предельных значений вероятности ошибочного обнаружения сигнального временного окна от среднего числа ФЭ за время анализа

Пусть известна длительность τ_s=1 нс и частота следования f_s=800 Гц (период следования T_s=1250 мкс) сигнальных фотонных импульсов. Причём предполагается абсолютная стабильность периода следования ΔT_s=0 и длительности $\Delta\tau_s$=0 оптических сигналов. Для обеспечения высокого уровня безопасности ориентируемся на среднее число ФЭ в фотонном импульсе $\overline{n_s}$=0,1.

Пусть частота появления импульсов темнового тока в применяемом ОФЭП составляет ξ_d=1000 Гц.

За период следования фотонных импульсов аппаратурой поиска производится анализ N_w=100 временных окон. Аппаратура поиска должна обеспечивать вероятность (безусловную) правильного обнаружения сигнального временного окна не хуже P_D=0,99.

При заданном периоде следования оптических импульсов T_s=1250 мкс находим длительность каждого из N_w=100 временных окон:

$$\tau_w = T_s / N_w = 12{,}5 \text{ мкс}.$$

Заметим, что длительность временного 12,5 мкс более чем в 12 500 раз превышает длительность фотонного импульса 1 нс. Следовательно, приближение при проведённом ранее анализе об исключении случая расположения фотонного импульса на границе двух временных окон справедливо для рассматриваемого примера.

За период следования оптических импульсов T_s=1250 мкс будет приниматься в среднем $\xi_d T_s = 1000 \cdot 1250 \cdot 10^{-6}$=1,25 импульсов темнового тока, а за длительность τ_w=12,5 мкс временного окна – $\overline{n_{d.w1}} = \xi_d \tau_w$ =0,0125.

По условию среднее число фотоэлектронов в фотонном импульсе равно $\overline{n_s}$=0,1. Следовательно, отношение сигнал/шум (в нашем случае отношение средних чисел ФЭ за длительность фотонного импульса и ИТТ за длительность временного окна) равно 8.

График на рис. 6 показывает, что предельное значение вероятности ошибочного обнаружения сигнального окна

$$P_E = 1 - P_D = \exp\left(-n_{s.w}\right) = 1\text{-}0{,}99 = 0{,}01$$

потребует обеспечить регистрацию в среднем 4,5 ФЭ за время анализа.

При наличии ИТТ вероятность ошибочного обнаружения сигнального окна возрастает. Так, например, из рис. 2 видно, что при $\overline{n_{d.w}} = N_t \overline{n_{d.w1}}$ =0,1 вероятность ошибочного обнаружения в 1 % реализуется уже при $\overline{n_{s.w}}$ =7,5.

Пусть $\overline{n_{s.w}}$ =13. Это позволяет, используя (8), рассчитать необходимое число выборок $N_t = n_{s.w} / n_s$ =13/0,1=130. За выборку объёмом N_t=130 при известном среднем числе регистрируемых ИТТ за длительность временного окна $\overline{n_{d.w1}}$ =0,0125 согласно (4) находим $\overline{n_{d.w}} = N_t \overline{n_{d.w1}}$ =1,625. В сигнальном временном окне среднее количество регистрируемых ФЭ и ИТТ за время анализа согласно (7) составит $\overline{n_w}\overline{n_{d.w}} + \overline{n_{s.w}}$ =14,625.

Расчёт по формулам (12), (16)–(20) позволяет найти безусловную вероятность правильного P_D=99,11 % и ошибочного $P_E = 1 - P_D$=0,89 % обнаружения сигнального временного окна в режиме предварительного поиска. Погрешность расчёта вероятности правильного обнаружения составила 0,0053 % при количестве суммирований 34 (при погрешности ε_n =0,0004 %) в формуле (16). Видно, что полученные вероятностные характеристики обеспечивают требования задания с высокой точностью.

Выбор исходных параметров фотонного импульса в представленной методике опирается на экспериментальные данные, полученные при проведении экспериментальных испытаний стенда квантово-криптографической сети на базе СКРК Clavis2 IDQuantique [10, 11].

Выводы. В результате проведенных исследований получены аналитические выражения для расчёта вероятностных характеристик СКРК в режиме вхождения в синхронизм при использовании фотонных импульсов для повышения защищённости СКРК от несанкционированного съёма информации. Соотношения позволяют оценивать влияние параметров фотонного импульса, ОФЭП и аппаратуры поиска с идеальным регистратором фотоэлектронов на вероятностные характеристики. Обоснован алгоритм расчёта с заданной погрешностью безусловной вероятности правильного обнаружения сигнального временного окна в режиме предварительного поиска, исключающий необходимость суммирования бесконечного числа слагаемых. На основе изложенного алгоритма разработана программа для ЭВМ, имитирующая процесс вхождения в синхронизм системы КРК. Предложена методика проектирования СКРК в режиме вхождения в синхронизм при идеальной однофотонной регистрации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Bennet C.H. Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984. – P. 175-179.
2. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, № 1. – P. 145-195.
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. *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.
6. *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.
7. *Гальярди Р.М., Карп Ш.* Оптическая связь: Пер. с англ. / Под ред. А.Г. Шереметьева. – М.: Связь, 1978. – 424 с.
8. *Hughes R.J., Nordholt J.E., Derkacs D., Peterson G.* Practical free-space quantum key distribution over 10 km in daylight andat night // New Journal of Physics. – 2002. – 4:43.
9. *Шереметьев А.Г.* Статистическая теория лазерной связи. – М.: Связь, 1971. – 264 с.
10. *Плёнкин А.П., Румянцев К.Е.* Стенд для научных исследований квантово-криптографической системы // Современные тенденции в образовании и науке: Сб. науч. тр. по материалам Международной науч.-практ. конференции 31 октября 2013 г.: В 26 ч. Ч. 2. – Тамбов: Изд-во ТРОО «Бизнес–Наука–Общество», 2013. – С. 108-111.
11. *Горбунов А.В., Мамаев А.В., Румянцев К.Е., Панюшкин С.А.* Разработка квантово-криптографической системы на базе аппаратной платформы иностранного производства // Материалы четвертой Всероссийской конференции по волоконной оптике «ВКВО–2013» (г. Пермь, 16–19 октября 2013 года). – Пермь: Фотон–экспресс, 2013. – № 6 (110). – С. 84-85.

REFERENCES

1. *Bennet C.H. Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing, *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984,* pp. 175-179.
2. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography, *Reviews of Modern Physics,* 2002, Vol. 74, No. 1, pp. 145-195.
3. Kvantovaya kriptografiya: idei i praktika, Pod red. S.Ya. Kilina, D.B. Khoroshko, A.P. Nizovtseva. Minsk: Belaruskaya navuka, 2008, 392 p.
4. *Rumyantsev K.E.* Sistemy kvantovogo raspredeleniya klyucha [System for quantum key distribution]: Monografiya. Taganrog: Izd-vo TTI YuFU, 2011, 264 p.
5. *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.
6. *Rumyantsev K.E., Rozova Ya.S.* Patentno-litsenzionnaya situatsiya v oblasti kvantovoy kriptografii [Patent licensing situation in the field of quantum cryptography], *Elektrotekhnicheskie i informatsionnye kompleksy i sistemy* [Electrical Engineering and Information Systems and Systems], 2011, T. 7, No. 1, pp. 3-10.
7. *Gagliardi, R M Karp, S.* Optical Communications. Published by John Wiley and Sons, 1976 [Russ. ed.: Gal'yardi R.M., Karp Sh. Opticheskaya svyaz]. Moscow: Svyaz' Publ, 1978, 424 p.
8. *Hughes R.J., Nordholt J.E., Derkacs D., Peterson G.* Practical free-space quantum key distribution over 10 km in daylight andat night, *New Journal of Physics*, 2002, 4:43.
9. *Sheremet'ev A.G.* Statisticheskaya teoriya lazernoy svyazi [Statisticheskaya theory of laser communication]. Moscow: Svyaz', 1971, 264 p.

10. *Plenkin A.P., Rumyantsev K.E.* Stend dlya nauchnykh issledovaniy kvantovo-kriptograficheskoy sistemy [Stand for scientific research of quantum-cryptographic systems], *Sovremennye tendentsii v obrazovanii i nauke: Sb. nauch. tr. po materialam Mezhdunarodnoy nauch.-prakt. konferentsii 31 oktyabrya 2013 g.: V 26 ch. Ch. 2* [Sat. scientific papers on materials of the International scientific-practical conference on October 31, 2013: In 26 parts. Part 2. Tambov: Izd-vo TROO «Biznes–Nauka–Obshchestvo», 2013, pp. 108-111.
11. *Gorbunov A.V., Mamaev A.V., Rumyantsev K.E., Panyushkin S.A.* Razrabotka kvantovo-kriptograficheskoy sistemy na baze apparatnoy platformy inostrannogo proizvodstva [The development of a quantum-cryptographic system based on the hardware platform of foreign production], Materialy chetvertoy Vserossiyskoy konferentsii po volokonnoy optike «VKVO–2013» (g. Perm', 16–19 oktyabrya 2013 goda) [The materials of the fourth all-Russian conference on fiber optics "wcwo-2013" (, Perm, 16-19 October 2013)]. Perm': Foton–ekspress, 2013, No. 6 (110), pp. 84-85.

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

Румянцев Константин Евгеньевич – Южный федеральный университет; e-mail: rke2004@mail.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 89281827209; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Плёнкин Антон Павлович – e-mail: pljonkin@mail.ru; тел.: 89054592158; кафедра информационной безопасности телекоммуникационных систем; аспирант.

Rumyatsev Konstantin Evgen'evich – Southern Federal University; e-mail: rke2004@mail.ru; 44, Nekrasovskiy, Taganrog, 347928, Russia; phone: +79281827209; the department of information security of telecommunication systems; 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.

УДК 003.26.09

А.В. Трепачева

КРИПТОАНАЛИЗ ШИФРОВ, ОСНОВАННЫХ НА ГОМОМОРФИЗМАХ ПОЛИНОМИАЛЬНЫХ КОЛЕЦ

Проводится анализ защищенности симметричных гомоморфных криптосхем шифрования, построенных на гомоморфизмах полиномиальных колец. Предлагается простой метод вычисления секретного ключа при наличии у криптоаналитика нескольких пар (шифртекст, открытый текст) в случае, когда пространство открытых текстов – конечное поле $\mathbb{F}_q$. *Он позволяет определить правильный ключ с вероятностью, равной единице, при наличии хотя бы пяти пар в случае небольших* q. *Для больших же значений* q *достаточно уже двух пар. Обсуждается, каким образом можно адаптировать этот метод для случая, когда пространство открытых текстов – кольцо вычетов* $\mathbb{Z}_n$, *где* n *– составное число. Также обсуждается метод, позволяющий скорректировать вычисленное с использованием пар значение ключа в случае, когда количество пар (шифротекст, открытый текст) меньше пяти. Для его работы необходимо знание вероятностного распределения на множестве открытых текстов и наличие дополнительной последовательности шифртекстов, зашифрованных на том же ключе. Данный метод успешно раскрывает ключ практически в 100 % случаев, если на открытых текстах задано распределение, достаточно сильно отличающееся от равномерного (например, нормальное распределение с небольшой дисперсией).*

Атака по известным открытым текстам; гомоморфное шифрование; облачные вычисления; полиномы.