18. *Rivest R.L., Smith W.D.* Three voting protocols: ThreeBallot, VAV, and Twin, *USENIX/ACCURATE Electronic Voting Technology (EVT 2007), 2007*.
19. *Santin A.O., Costa R.G., Maziero C.A.* A three-ballot-based secure electronic voting system, *IEEE Security & Privacy*, 2008, Vol. 6, No. 3, pp. 14-21.
20. *Henry K.J., Stinson D.R., Sui J.* The effectiveness of receipt-based attacks on threeballot, IEEE *Transactions on Information Forensics and Security*, 2009, Vol. 4, No. 4, pp. 699.

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

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@tsure.ru; г. Таганрог, 18-ый переулок, 43; тел.: 89054530191; кафедра безопасности информационных технологий; д.т.н.; профессор.

Писарев Илья Александрович – e-mail: ilua.pisar@gmail.com; г. Таганрог, ул. Котлостроительная 7, кв. 35; тел.: 89885350837; кафедра безопасности информационных технологий; студент.

Babenko Ludmila Klimentevna – Southern Federal University; e-mail: blk@tsure.ru; 18th Lane, 43, Taganrog, Russia; phone: +79054530191; the department of information technology security; dr. of eng. sc.; professor.

Pisarev Ilya Aleksandrovich – e-mail: ilua.pisar@gmail.com; 7, Kotlostroitelnaia street, Apt. 35, Taganrog, Russia; phone: +79885350837; the department of information technology security; student.

УДК 621.396.624 DOI 10.23683/2311-3103-2018-5-56-68

К.Е. Румянцев, Е.А. Рудинский

ОЦЕНКА ПАРАМЕТРОВ ДВУХЭТАПНОГО АЛГОРИТМА ОДНОФОТОННОЙ СИНХРОНИЗАЦИИ АВТОКОМПЕНСАЦИОННОЙ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА

Решение проблемы обеспечения секретности при распределении ключа базируется на принципах квантовой криптографии и предполагает кодирование квантового состояния фотона. Анализ стратегий съёма информации посредством атак в квантовых системах показывает, что реализация многофотонного режима в процессе синхронизации потенциально упрощает злоумышленнику организацию несанкционированного доступа к информации. Последнее определяет актуальность разработки и исследования методов и алгоритмов синхронизации систем квантового распределения ключа (КРК) с автоматической компенсацией поляризационных искажений, обеспечивающих повышенную защищённость процесса от несанкционированного доступа. Исследована защита процесса синхронизации автокомпенсационных системы КРК от несанкционированного доступа. Предложенный алгоритм синхронизации позволяет использовать однофотонные лавинные фотодиоды (ОЛФД) со значительной временной задержкой между моментами приёма фотона и восстановления ОЛФД. В данной работе описан графоаналитический метод оценки параметров однофотонной синхронизации системы распределения квантовых ключей с автоматической компенсацией. В работе формируется и описывается диаграмма состояний и переходов для случайного поиска импульса фотона с учетом вероятности ложных срабатываний. На основе результатов анализа определены выражения для вычисления математического ожидания, дисперсии и среднего количества шагов, затраченных на процесс синхронизации. Определён интервал для среднего числа шагов, используемых в процессе синхронизации. Среднее время синхронизации согласно предложенному алгоритму оценивается с учетом вероятности ложной тревоги. Расчеты показали, что ошибка в определении среднего времени синхронизации согласно представленным выражениям составляет не более 1,7 %. Таким образом, графоаналитический метод оценки параметров однофотонной синхронизации системы автокомпенсационной системы КРК позволяет определить статистические характеристики и среднее время синхронизации с низким уровнем ошибки.

Квантовое распределение ключа; синхронизация; защита; волоконно-оптическая линия; двухэтапный алгоритм; однофотонная регистрация.

K.E. Rumyantsev, E.A. Rudinsky

ESTIMATION OF THE PARAMETERS OF A TWO-STAGE ALGORITHM FOR SINGLE-PHOTON SYNCHRONIZATION OF AN AUTO-COMPENSATION QUANTUM KEY DISTRIBUTION SYSTEM

Solving the problem of secrecy in the process of key distribution is based on the principles of the encoding of the photon quantum state. Analysis of information strategies in quantum systems shows that the implementation of the multiphoton mode in the synchronization process potentially makes it easier unauthorized access to information. This determines the researching of methods and algorithms for synchronization of quantum key distribution (QKD) systems with automatic compensation of polarization distortions that provide increased protection from unauthorized access. The synchronization process protecting of auto-compensation QKD systems from unauthorized access is investigated. The synchronization algorithm allows the use of single-photon avalanche photodiodes (SPAD) with a significant time delay between the moment of photon reception, avalanche formation, its quenching and subsequent recovery. In this article we describe the graph-analytical method for estimating single-photon synchronization parameters of an auto-compensation quantum key distribution system. In this paper is formed and described diagram of states and transitions for random search for a photon pulse with allowance for false detection. Based on the results of the analysis, expressions are defined for calculating the mathematical expectation, dispersion and average number of steps spent on the synchronization process. The interval for the average number of steps used for the synchronization process is determined. The average synchronization time according to the proposed algorithm is estimated considering the probability of false alarm. The calculations showed that the error in determining the mean synchronization time according to the expressions is no more than 1.7 %. Thus, the graph-analytic method for estimating the single-photon synchronization parameters of the QKD auto-compensation system allows to determine the statistical characteristics and the average synchronization time with a low error.

Quantum key distribution; synchronization; security; fiber-optic line; two-stage algorithm; single-photon registration.

Введение. Техническим решением проблемы обеспечения секретности при распределении секретного ключа между легитимными пользователями являются системы квантового распределения ключа (КРК), успешно реализованные и доведенные до коммерческого использования [1, 2]. Важнейшей составляющей данной системы является синхронизация станций Алиса и Боб [3]. Результаты анализа коммерческих систем КРК [4, 5] показали, что процесс синхронизации реализуется в многофотонном режиме. Однако в работе [6] показано, что реализация данного режима потенциально упрощает злоумышленнику организацию несанкционированного доступа (НСД) к информации. Вышесказанное определяет актуальность разработки и исследования методов и алгоритмов однофотонной синхронизации автокомпенсационных систем КРК для обеспечения повышенной защищённости процесса синхронизации от НСД.

В [7−10] предложены и исследованы алгоритмы однофотонной синхронизации двухпроходной автокомпенсационной системы КРК, подразумевающий разбиение временного кадра на временные окна. Однако, при проведении данных исследований не учитывались особенности функционирования однофотонных лавинных фотодиодов (ОЛФД) и вероятность ложных срабатываний в процессе синхронизации [11−13]. Так как ОЛФД способен регистрировать только первый фотон за время анализа и ему требуется время для восстановления своей работоспособности, то время синхронизации согласно описанному выше алгоритму многократно увеличивается [14].

В [15] предложен метод синхронизации фотонными импульсами системы КРК, учитывающий параметры реальных ОЛФД. Установлено [16−17], что предложенный двухэтапный алгоритм синхронизации обеспечивает значительный вы-

игрыш (в сотни раз) во времени вхождения в синхронизм по сравнению с аналогичным алгоритмом, подразумевающим разбиение временного кадра на временные окна. В [18] доказано, что алгоритм обеспечивает достаточно низкую вероятность ошибки синхронизации ($P_{err.sync} = 0{,}0043$).

Практический интерес представляет оценка временных и статистических характеристик двухэтапного алгоритма с учётом ложных срабатываний. Цель исследований состоит в установлении зависимостей временных и статистических характеристик алгоритма от параметров реальных ОЛФД и вероятности ложных тревог.

Аналитический метод расчёта параметров модуля для двухэтапной однофотонной синхронизации. Согласно предложенному в [15] двухэтапному алгоритму аппаратура синхронизации первоначально работает в режиме поиска фотона. При первом превышении порогового уровня процессом с выхода однофотонного фотодетектора аппаратура переходит в режим тестирования. Повторный опрос фотодетектора производится только в интервалах ожидаемого прихода фотонного импульса во время действия импульса стробирования с длительностью τ_{strob}. В остальное время приёмная аппаратура не реагирует на приём фотонов.

Рассмотрим временные характеристики алгоритма однофотонной синхронизации в режиме тестирования. Решение о синхронизации согласно данному алгоритму выносится при первой регистрации фотона в режиме тестирования (рис. 1).

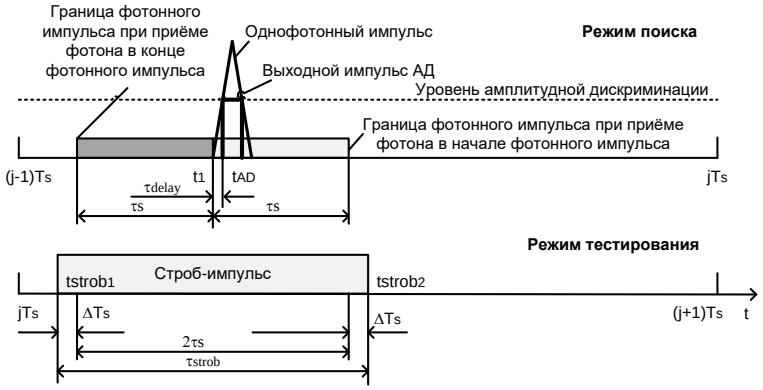

Рис. 1. Иллюстрация двухэтапного временного метода синхронизации

В [15] установлено, что среднее время тестирования составляет

$$\tau_{test} = T_s \frac{P_{strob0}}{1 - P_{strob0}} \langle 1 + [(N_{test} - 1)P_{strob0} - N_{test}] {P_{strob0}}^{N_{test}-1} \rangle + \\ + \tau_{strob} \left(1 - {P_{strob0}}^{N_{test}}\right), \quad (1)$$

где T_s – период следования оптических синхросигналов, P_{strob0} - вероятность отсутствия приёма фотонов и ИТТ за длительность стробирующего импульса.

При этом количество требуемых тестов N_{test} для обеспечения заданной вероятности ошибки в принятии решения об обнаружении синхросигнала в режиме тестирования P_{err} определяется ближайшим целым числом к значению, рассчитываемому по формуле [15]

$$N_{test} = \frac{1}{\overline{n_s}} \cdot ln\left(\frac{1}{P_{err}}\right), \quad (2)$$

где $\overline{n_s}$ – среднее число фотонов за длительность оптического импульса.

Анализ (1) показывает возможность его преобразования к виду [17]:

$$\tau_{test} = T_s \frac{1 - \overline{n_s}}{\overline{n_s}}. \quad (3)$$

Установлено, что различие в расчётах по формулам (1) и (3) не превышает 15 % при ориентации на P_{err}=0,1 и протяжённости ВОЛС более 10 км, а при P_{err}≤0,01 – 3 %.

Рассмотрим временные характеристики предложенного алгоритма синхронизации в целом в предположении отсутствия темнового тока ОЛФД. Исключение из рассмотрения внутренних шумов ОЛФД позволяет получить нижнюю оценку (предельно реализуемого) среднего времени вхождения в синхронизм.

Проведённый анализ ситуаций при 1-м, 2-м и 3-м шагах поиска синхросигнала позволил получить выражение для расчёта среднего времени вхождения в синхронизм [15]

$$\tau_{sync} = \sum_{j=1}^{\infty}[(j-1)T_s + \tau_1]P_0^{j-1}P + \\ + \sum_{j=2}^{\infty}\sum_{k=1}^{j-1}\frac{(j-1)!}{(j-1-k)!\cdot k!}[(j-1-k)T_s + k\tau_2 + \tau_1]P_0^{j-1-k}P_1^{k}P. \quad (4)$$

Здесь усреднённое время прекращения поиска на первом шаге и на втором шаге определяется соответственно выражениями

$$\tau_1 = \frac{3T_s}{2} - \frac{\tau_{strob}}{2} + \tau_{test}; \quad (5)$$

$$\tau_2 = N_{test}\cdot T_s + 0{,}5T_s + 0{,}5\tau_{strob.} \quad (6)$$

В формуле (4) можно выделить три основные составляющие.

$$\tau_{sync1} = T_s \cdot \frac{P\cdot P_0}{(1-P_0)^2} + \tau_1 \cdot \frac{P}{1-P_0}, \quad (7)$$

$$\tau_{sync2} = P_1 P\left[\frac{2T_s P_0}{(1-P_0)^3} + \frac{\tau_2+\tau_1}{(1-P_0)^2}\right], \quad (8)$$

$$\tau_{sync3} = {P_1}^2 P\left[\frac{3T_s P_0}{(1-P_0)^4} + \frac{[2\tau_2+\tau_1]}{(1-P_0)^3}\right]. \quad (9)$$

Первая составляющая τ_{sync1} определяет время на вхождение в синхронизм, когда на первых (j-1) шагах не регистрируется факт приёма оптического импульса. И только на последнем шаге фиксируется фотон, принадлежность которого импульсу подтверждается тестированием.

Вторая составляющая τ_{sync2} отражает время, затрачиваемое на вхождение в синхронизм при допущении, что первое срабатывание не подтверждается тестированием. И только второе срабатывание завершается вхождением в синхронизм.

Третья составляющая определяет время вхождения в синхронизм при допущении, что первое и второе срабатывания не подтверждаются тестированием. Лишь третье срабатывание завершается вхождением в синхронизм.

Расчёты показали, что учёт первых трёх слагаемых гарантирует погрешность расчётов среднего времени синхронизации ниже 0,6 % во всём диапазоне изменений вероятности ошибки на этапе тестирования. Даже при учёте первых двух слагаемых погрешность расчётов среднего времени при P_{test}=0,9 не превышает 4,2 %, а при P_{test}≤0,95 – 1,2 %.

Проведённый анализ показывает возможность расчёта среднего времени вхождения в синхронизм по формуле

$$\tau_{sync} = \tau_{sync1} + \tau_{sync2} + \tau_{sync3}. \quad (10)$$

Для экспресс-анализа системы можно использовать приближённую формулу

$$\frac{\tau_{\text{sync}}}{T_s} = P_{test} \cdot \frac{2}{\overline{n_s}} + P_{test} \cdot P_{err}\left(\frac{3}{\overline{n_s}} + 2 + N_{test}\right) + \\ + P_{test} \cdot P_{err}^2\left(\frac{4}{\overline{n_s}} + 2{,}5 + 2 \cdot N_{test}\right). \quad (11)$$

Расчеты по формуле (11) дают погрешность до 14 % (погрешность не превышает 2 % в диапазоне P_{test}=0,99…0,999).

Среднее время синхронизации без учёта ложных срабатываний. Проведём количественный расчёт характеристик двухэтапного алгоритма синхронизации. Пусть волоконно-оптическая линия связи (ВОЛС) спроектирована на одномодовом оптическом волокне (ОВ) Corning®SMF-28e$^+$ с погонным затуханием $\alpha = 0{,}2$ дБ/км и показателем преломления оптического излучения в сердцевине $\mathrm{n}_{fiber} = 1{,}4682$ на рабочей длине волны 1550 нм. Протяжённость ВОЛС, связывающей приемо-передающую и кодирующую станции системы КРК, равна $L_{FOL} = 10$ км. Скорость распространения оптического излучения в ВОЛС составит $v_{fiber} = \mathrm{c}_{opt}/n_{fiber} = 204\,331{,}8$ км/с.

Минимальное значение периода следования импульсов $T_{s.min} = 2L_{FOL}/v_{fiber} = 97{,}8$ мкс. Следовательно, максимально допустимое значение частоты следования импульсов $f_{s.max} = 1/T_{s.min} = 10{,}2$ кГц. Принимаем частоту и период следования оптических синхроимпульсов равными соответственно $f_s = 10$ кГц и $T_s = 100$ мкс.

Приёмный оптический модуль реализован на ОЛФД Id100-20, у которого частота генерации импульсов темнового тока (ИТТ) ξ_{DCR} в малошумном исполнении не превышает 2 Гц. Среднее число ИТТ за период следования оптических сигналов – $\overline{n_{DCR.T}} = \xi_{DCR} \cdot T_s = 0{,}0002$.

Для обеспечения защиты системы КРК принимаем среднее число фотонов за длительность оптического импульса на выходе из кодирующей станции Алиса $\overline{n_{s0}}$ равным 0,1. Тогда среднее число фотонов за длительность фотонного импульса

$$\overline{n_s} = \overline{n_{s0}} \cdot 10^{-\frac{\alpha[\text{дБ/км}] \cdot L_{FOL}[\text{км}]}{10}} = 0{,}063.$$

Рассчитываем предельную безусловную вероятность обнаружения фотонного импульса в режиме поиска [15]

$$P_{D.max} = \overline{n_s}/(\overline{n_{DCR.T}} + \overline{n_s}) = 0{,}996.$$

Пусть вероятность ошибки тестирования P_{err} равна 0,01. Число тестов, необходимых для обеспечения данной вероятности согласно (2) составит $N_{test.max} \geq 73$. Для практической реализации целесообразно принять $N_{test} = 128 = 2^7$. Тогда вероятность ошибки на втором этапе составит $\mathrm{P_{err}} = \exp(-\mathrm{N_{test}}\overline{\mathrm{n_s}}) = 0{,}0003$, а общая вероятность ошибки синхронизации – $\mathrm{P_{err.sync}} = 1 - \mathrm{P_{D.max}}(1 - \mathrm{P_{err}}) = 0{,}0043$.

Определяем вероятность приёма хотя бы одного фотона за длительность оптического импульса $\mathrm{P_s} = 1 - \exp(-\overline{\mathrm{n_s}}) = 0{,}0611$. Вероятность обнаружения фотонного импульса в процессе тестирования составит $\mathrm{P_{test}} = 1 - \exp(-\mathrm{N_{test}} \cdot \overline{\mathrm{n_s}}) = 0{,}9997$.

Вхождение в синхронизм при регистрации фотона в первом кадре происходит с вероятностью $\mathrm{P_s P_{test}} = 0{,}061$. Вероятность возврата к поиску после тестирования равна $\mathrm{P_s}(1 - \mathrm{P_{test}}) \approx 1{,}83 \cdot 10^{-5}$.

Среднее время тестирования согласно (1) составляет $\tau_{test} = 1{,}53$ мс. По формуле (5) находим среднее время прекращения поиска на первом шаге $\tau_1 = 1{,}68$ мс . Согласно (6) находим время на прекращение поиска во втором шаге $\tau_2 = 12{,}85$ мс, если факт приёма оптического импульса не подтверждён тестированием.

По формулам (7) − (9) рассчитывается среднее время на вхождение в синхронизм в процессе первого $\tau_{sync1} = 3{,}21$ мс, второго $\tau_{sync2} = 4.57$ мкс и третьего $\tau_{sync3} = 2.71$ нс тестирования.

Используя (10), находим среднее время вхождения в синхронизм $\tau_{sync} \approx 3{,}216$ мс. Отклонение среднего времени синхронизации от минимально возможного значения $\tau_{sync1} \approx 3{,}211$ мс не превышает 0,16 %. Кроме того, расчёт по приближённой формуле (11) для экспресс-анализа системы даёт $\tau_{sync} \approx 3{,}18$ мс (погрешность не превышает 1,12 %).

Диаграммы состояний и переходов при поиске фотонного импульса с учётом ложных срабатываний. При реализации двухэтапного алгоритма синхронизации необходимо учитывать, что допустимая протяженность ВОЛС непосредственно зависит от частоты ИТТ ξ_{DCR} используемого ОЛФД. Так, при частоте генерации ИТТ $\xi_{DCR} = 5$ Гц результирующая вероятность ошибки синхронизации $P_{err.sync} \leq 0.1$ достигается при протяженности ВОЛС L_{FOL} не более 40 км.

Определим временные и вероятностные характеристики алгоритма синхронизации с учетом ложных срабатываний при $\overline{n_s} \gg \overline{n_{DCR.T}}$.

На рис. 2 приведены диаграмма состояний и вероятности переходов для конечной марковской цепи [19, 20], где:

- непоглощающее состояние a_1 – поиск фотонного импульса (ФИ), анализ временного кадра (интервала) протяжённостью T_s;
- непоглощающие состояния $a_2, a_{2a}, a_{2b}, \dots, a_{2n}$ – режим тестирования при правильном обнаружении ФИ на этапе поиска, режим тестирования начинается с момента $t_1 + T_s - \tau_{strob}/2$;
- непоглощающие состояния $a_3, a_{3a}, a_{3b}, \dots, a_{3n}$ – режим тестирования при ложной тревоге;
- поглощающее состояние a_4 – состояние синхронизации приёмопередающей и кодирующей станций системы КРК;
- P_{11} – вероятность не обнаружить ФИ и ИТТ на этапе поиска;
- P_{12} – вероятность обнаружения ФИ на интервале $t_1 \in [0, T_s]$ на этапе поиска и перехода к состоянию a_2;
- P_{13} – вероятность ложной тревоги и перехода к состоянию a_3;

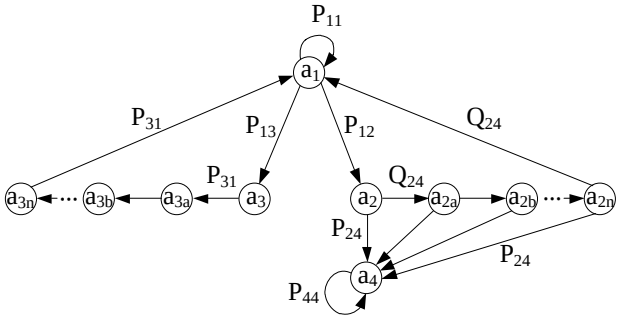

Рис. 2. Диаграмма состояний и переходов для случайного поиска с учётом ложного обнаружения

- Q_{24} – вероятность отсутствия приёма ФИ или ИТТ за длительность импульса стробирования $\tau_{strob} = \tau_{strob} = 2\tau_s + 2\Delta T_s$, где ΔT_s − нестабильность периода следования синхроимпульсов;

♦ $P_{31} = 1$ – вероятность отсутствия приёма ФИ во время стробирования τ_{strob} (поскольку для указанного ранее ограничения по протяженности ВОЛС справедливо неравенство $\overline{n_s} \gg \overline{n_{DCR.T}}$, то вероятность ложных срабатываний на тестирования стремится к 0);

♦ P_{24} – вероятность приёма ФИ или ИТТ за длительность импульса стробирования на этапе тестирования.

Отметим, что диаграмма, представленная на рис. 2, является реализацией поочередного алгоритма тестирования согласно [16–20]. На этапе тестирования производится N_{test} тестов и при приёме первого фотона тестирование прекращается и принимается решение о вхождении в синхронизм.

На рис. 3 представлены вероятности перехода системы между состояниями согласно представленной на рис. 2 диаграмме состояний и переходов марковской цепи.

	a_1	a_2	a_{2a}	a_{2b}	...	a_{2n}	a_3	a_{3a}	a_{3b}	...	a_{3n}	a_4
a_1	P_{11}	P_{12}					P_{13}					
a_2			Q_{24}									P_{24}
a_{2a}				Q_{24}								P_{24}
a_{2b}					Q_{24}							P_{24}
...						Q_{24}						P_{24}
a_{2n}	Q_{24}											P_{24}
a_3								1				
a_{3a}									1			
a_{3b}										1		
...											1	
a_{3n}	1											
a_4												1

Рис. 3. Вероятности перехода между состояниями

Определение статистических характеристик двухэтапного алгоритма с учетом ложных срабатываний. Рассмотрим случай, когда выполняется всего один тест $N_{test} = 1$. Для нахождения статистических характеристик процесса поиска образуем стохастическую матрицу вероятностей перехода

$$P = \begin{pmatrix} P_{11} & P_{12} & P_{13} & 0 \\ Q_{24} & 0 & 0 & P_{24} \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Математическое ожидание числа прохождений процесса через непоглощающее (переходное) состояние a_j определяется выражением

$$T = \{M_i[n_j]\} = (I - Q)^{-1} = \begin{pmatrix} \frac{1}{P_{12}P_{24}} & \frac{1}{P_{24}} & \frac{P_{13}}{P_{12}P_{24}} \\ -\frac{P_{24}-1}{P_{12}P_{24}} & \frac{1}{P_{24}} & -\frac{P_{13}(P_{24}-1)}{P_{12}P_{24}} \\ \frac{1}{P_{12}P_{24}} & \frac{1}{P_{24}} & \frac{P_{13}+P_{12}P_{24}}{P_{12}P_{24}} \end{pmatrix}.$$

Здесь матрица Q образуется вычеркиванием из матрицы P всех строк и столбцов, соответствующих поглощающим состояниям. Если процесс начинается с непоглощающего состояния a_1, то он пройдет непоглощающее состояние a_2 в среднем $M_1(n_2) = 1/P_{24}$ раз.

Дисперсия числа прохождений определяется выражением

$$\{D_i[n_j]\} = T(2T_{\text{дг}} - I) - T_{\text{кв}} =$$

$$\begin{pmatrix} -\frac{P_{12}P_{24}-1}{P_{12}^2P_{24}^2} & \frac{1-P_{24}}{P_{24}^2} & \frac{P_{13}(P_{13}+P_{12}P_{24})}{P_{12}^2P_{24}^2} \\ \frac{(1-P_{24})(P_{24}(1-P_{12})+1)}{P_{12}^2P_{24}^2} & \frac{1-P_{24}}{P_{24}^2} & \frac{P_{13}(1-P_{24})(P_{13}+(P_{12}+P_{13})P_{24})}{P_{12}^2P_{24}^2} \\ -\frac{P_{12}P_{24}-1}{P_{12}^2P_{24}^2} & \frac{1-P_{24}}{P_{24}^2} & \frac{P_{13}(P_{13}+P_{12}P_{24})}{P_{12}^2P_{24}^2} \end{pmatrix}.$$

где $T_{\text{дг}}$ – «диагональная» матрица, совпадающая с матрицей T по главной диагонали, но имеющая в остальных позициях нули; $T_{\text{кв}}$ – «квадратная» матрица, образованная из T возведением в квадрат каждого её элемента.

Если процесс начинает в непоглощающем состоянии a_1, то дисперсия числа прохождений процесса через непоглощающее состояние a_2 составит $D_1[n_2] = (1 - P_{24})/P_{24}^2$.

Определяем среднее число шагов t, которое затрачивается при переходе процесса из непоглощающего состояния в поглощающее

$$t = Tc = \begin{pmatrix} \frac{1 + P_{12} + P_{13}}{P_{12}P_{24}} \\ \frac{Q_{24} + P_{12} + P_{13}Q_{24}}{P_{12}P_{24}} \\ \frac{1+P_{13} + P_{12}(P_{24} + 1)}{P_{12}P_{24}} \end{pmatrix}.$$

Первый элемент вектор-столбца t является средним числом шагов, которое процесс проходит в поглощающее состояние a_4 (состояние синхронизации), при предположении, что он начинается из состояния a_1, второй элемент – среднее число шагов при начале процесса в состояния a_2 и третий элемент – при начале процесса в состоянии a_3.

Так как процесс поиска начинается в состоянии a_1, то интересующее нас число шагов до достижения состояния a_4 будет

$$t_1 = \frac{1+P_{12}+P_{13}}{P_{12}P_{24}} = \frac{1}{P_{24}} + \frac{1+P_{13}}{P_{12}P_{24}} = \frac{1}{1-Q_{24}} - \frac{1+P_{13}}{P_{12}(Q_{24}-1)}. \quad (12)$$

Пусть $\tau = T_s$ – длительность шага процесса синхронизации. Тогда среднее время, затрачиваемое на вхождение в синхронизм будет равно $t_1\tau$.

Дисперсия числа шагов, затрачиваемых на переход процесса из непоглощающего состояния в поглощающее, определяется выражением

$$\{D_i[\alpha_m]\} = (2T - I)t - t_{\text{кв}} =$$

$$= \begin{pmatrix} \frac{(1 + P_{12} + P_{13})^2}{P_{12}^2P_{24}^2} - \frac{3 + P_{12} + P_{13}}{P_{12}P_{24}} \\ \frac{1 - P_{24}}{P_{24}^2} - \frac{(P_{24} - 1)(2P_{13} - P_{24} + P_{13}P_{24} + 2)}{P_{12}P_{24}^2} - \frac{(1 + P_{13})^2(P_{24}^2 - 1)}{P_{12}^2P_{24}^2} \\ \frac{(1 + P_{12} + P_{13})^2}{P_{12}^2P_{24}^2} - \frac{3 + P_{12} + P_{13}}{P_{12}P_{24}} \end{pmatrix},$$

где a_m – число шагов на переход из непоглощающего состояния a_i в поглощающее, $t_{кв}$ – «квадратный» вектор столбец.

Таким образом, дисперсия числа шагов на переход процесса из состояния a_1 в поглощающее состояние a_4 определяется выражением

$$d_1 = \frac{(1+P_{12}+P_{13})^2}{P_{12}^2 P_{24}^2} - \frac{3+P_{12}+P_{13}}{P_{12}P_{24}} =$$

$$= \frac{Q_{24}}{(Q_{24}-1)^2} + \frac{2P_{13}+P_{12}\left((P_{13}+3)Q_{24}+P_{13}-1\right)+{P_{13}}^2+1}{{P_{12}}^2(Q_{24}-1)^2}. \quad (13)$$

Рассмотрим случай, когда количество тестов $N_{test} = 2$. Если процесс поиска начинается в состоянии a_1, то число шагов до достижения состояния a_4 будет

$$t_1 = \frac{1}{P_{24}} - \frac{2P_{13}+1}{(P_{24}-2)P_{12}P_{24}} = \frac{1}{1-Q_{24}} - \frac{1+2P_{13}}{P_{12}(Q_{24}^2-1)}. \quad (14)$$

Дисперсия числа шагов может быть рассчитана по формуле

$$d_1 = \frac{{Q_{24}}^3+2{Q_{24}}^2+Q_{24}}{({Q_{24}}^2-1)^2} + \frac{4P_{13}+P_{12}\left((4P_{13}+5){Q_{24}}^2+4P_{13}-1\right)+4{P_{13}}^2+1}{{P_{12}}^2({Q_{24}}^2-1)^2}. \quad (15)$$

Аналогично, для случая, когда количество тестов $N_{test} = 3$ находим математическое ожидание и дисперсию числа шагов на переход процесса из непоглощающего состояния a_1 в поглощающее a_4

$$t_1 = \frac{1}{P_{24}} + \frac{3P_{13}+1}{\left({P_{24}}^2-3P_{24}+3\right)P_{12}P_{24}} = \frac{1}{1-Q_{24}} - \frac{1+3P_{13}}{P_{12}(Q_{24}^3-1)}.$$

$$d_1 = \frac{{Q_{24}}^5+2{Q_{24}}^4+3{Q_{24}}^3+2{Q_{24}}^2+Q_{24}}{({Q_{24}}^3-1)^2} + \frac{6P_{13}+P_{12}\left((9P_{13}+7){Q_{24}}^3+9P_{13}-1\right)+9{P_{13}}^2+1}{{P_{12}}^2({Q_{24}}^3-1)^2}. \quad (16)$$

Используя методы математической индукции к формулам (12), (14), (16) и (13), (15), (17) находим, что при числе тестов N_{test} на втором этапе синхронизации математическое ожидание и дисперсия числа шагов, затрачиваемых при переходе процесса из состояния a_1 (поиск фотонного импульса) в a_4 (установленная синхронизация) определяются соответственно выражениями

$$t_1 = \frac{1}{1-Q_{24}} - \frac{1+N_{test}P_{13}}{P_{12}(Q_{24}^{N_{test}}-1)}.$$

$$d_1 = \frac{\sum_{k=1}^{N_{test}} k\,{Q_{24}}^k + \sum_{k=1}^{N_{test}-1}(N_{test}-k){Q_{24}}^{k+N_{test}}}{\left({Q_{24}}^{N_{test}}-1\right)^2} +$$

$$\frac{2N_{test}P_{13}+P_{12}\left(\left(N_{test}^2P_{13}+2N_{test}+1\right){Q_{24}}^{N_{test}}+N_{test}^2P_{13}-1\right)+N_{test}^2{P_{13}}^2+1}{{P_{12}}^2({Q_{24}}^{N_{test}}-1)^2}. \quad (18)$$

При известном среднеквадратическом отклонении (СКО) $\sigma = \sqrt{d_1}$ число шагов затрачиваемых на переход в поглощающее состояние a_4 с вероятностью порядка 0,9973 расположено в интервале $[t_1 - 3\sigma; t_1 + 3\sigma]$.

Оценка среднего времени вхождения в синхронизм с учётом ложных срабатываний. Рассмотрим случай отсутствия ложных срабатываний на этапе поиска ФИ ($P_{13} = 0$). Тогда (18) может быть преобразовано к виду:

$$t_1 = \frac{1}{1-Q_{24}} - \frac{1}{P_{12}(Q_{24}^{N_{test}}-1)}. \quad (19)$$

Воспользуемся параметрами ВОЛС и передающей станции рассмотренной ранее системы КРК: ОВ – Corning®SMF-28, $L_{FOL} = 10$ км, $f_s = 10$ кГц, $T_s = 100$ мкс, ξ_{DCR}=2 Гц, $\overline{n_s} = 0{,}063$, $\overline{n_{strob}} \approx 0{,}063$, $N_{test} = 128$, $P_{err} = 0{,}0003$.

Пусть вероятность ошибки на этапе тестирования P_{err} равна 0,01. Вероятность обнаружения фотонного импульса в режиме поиска

$$P_{12} = 1 - exp(-\overline{n_s} - \xi_{DCR} \cdot \tau_s) = 0{,}0611.$$

Общая вероятность ошибки на втором этапе синхронизации составит

$$P_{err} = exp(-N_{test}\overline{n_s}) = 0{,}0003.$$

Определим вероятность ошибки во время одного тестирования

$$Q_{24} = exp(-\overline{n_{strob}}) \approx 1 - \overline{n_{strob}} = 0{,}9389.$$

Согласно (19) среднее число шагов составит $t_1 = 32{,}71$, а среднее время на синхронизацию – $t_1 T_s = 3{,}271$ мс. Отметим, что согласно ранее описанной методике среднее время вхождения в синхронизм при тех же условиях составит $\tau_{sync} \approx 3{,}216$ мс (различие ниже 1,7 %).

В случае допустимости ложных срабатываний на этапе поиска ФИ вероятность ложной тревоги составит $P_{13} = 1 - exp(-\xi_{DCR} \cdot T_s) \approx 2 \cdot 10^{-4}$.

В таком случае согласно (18) среднее число шагов, затрачиваемое при переходе процесса из непоглощающего состояния a_1 в поглощающее a_4 составит $t_1 = 33{,}13$. Среднее время синхронизации с учетом вероятности ложной тревоги составит $t_1 T_s = 3{,}31$ мс.

Выводы. Дана оценка временных и статистических параметров двухэтапного алгоритма однофотонной синхронизации автокомпенсационной системы КРК.

Получены соотношения для расчёта среднего времени тестирования поочерёдного алгоритма. Установлено, что значительное снижение вероятности ошибки на этапе тестирования не приводит к столь же значительному снижению среднего времени синхронизации. Получены соотношения для расчёта временных характеристик алгоритма синхронизации в предположении отсутствия ложных срабатываний. Отмечено, что по мере уменьшения вероятности ошибки тестирования среднее время синхронизации стремится к предельному минимальному значению, определяемому средним временем вхождения в синхронизм в процессе первого тестирования. Получено выражение для экспресс-анализа системы, которое дает погрешность ниже 14 % (погрешность не превышает 2 % в диапазоне P_{test}=0,99…0,999).

Определены выражения для расчёта временных и статистических характеристик (математическое ожидание и дисперсия числа шагов, затрачиваемых на процесс синхронизации) алгоритма синхронизации с учётом вероятности ложных срабатываний. Отмечено, что различие в определении среднего времени синхронизации согласно представленным методикам составила не более 1,7 %, что свидетельствует о корректности проведенных исследований и полученных выражений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / под ред. Д. Боумейстера, А. Экерта, А. Цайлингера. – М.: Постмаркет, 2002. – 376 с.
2. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145-195.
3. *Румянцев К.Е.* Синхронизация в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Телекоммуникации. – 2017. – № 2. – С. 32-40.
4. *Плёнкин А.П.* Исследование режима вхождения в синхронизм при использовании фотонных импульсов системы квантового распределения ключа // ES-ФМ-2014-011: Сб. материалов международного научного е-симпозиума. Россия, г. Москва, 27–28 декабря 2014 г. – Киров: МЦНИП, 2015. – С. 101-113.

5. *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.
6. *Румянцев К.Е.* Защита процесса синхронизации в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Телекоммуникации. – 2017. – № 3. – С. 36-44.
7. *Румянцев К.Е., Плёнкин А.П.* Синхронизация системы квантового распределения ключа в режиме однофотонной регистрации импульсов для повышения защищенности // Радиотехника. – 2015. – № 2. – С. 125-134.
8. *Румянцев К.Е., Плёнкин А.П.* Повышение эффективности алгоритма вхождения в синхронизм системы квантового распределения ключей // Известия ЮФУ. Технические науки. – 2015. – № 8 (169). – С. 6-19.
9. *Pljonkin A., Rumjantsev K.* Preliminary Stage Synchronization Algorithm of Autocompensation Quantum Key Distribution System with an Unauthorized Access Security // Proceeding of the 15th International Conference on Electronics, Information, and Communication 2016 (ICEIC 2016). Jan 27−30, 2016. Danang, Vietnam. – Paper № 1570220423.
10. *Pljonkin A., Rumjantsev K.* Single-photon Synchronization Mode of Quantum Key Distribution System // Proceeding of the International Conference on Computational Techniques in Information and Communication Technology. 2016. (ICCTICT 2016). 11th – 13th March 2016. New Delhi, India. – Paper 1570218403.
11. *Гуядичи А., Симмерес Д., Веронезе Д., Биази Р., Шулинатти А., Рич И., Гилни М., Макяньти П.* Компактные модули на основе SPAD-детекторов для регистрации одиночных фотонов в ближней инфракрасной области спектра // Фотоника. – 2012. – № 6 (36). – С. 32-40.
12. *Pljonkin A.P.* Features of the Photon Pulse Detection Algorithm in the Quantum Key Distribution System // Proceedings of the 2017 International Conference on Cryptography, Security and Privacy (ICCSP 2017). – P. 81-84. SP029. Wuhan, China March 17-19, 2017. ACM New York, NY, USA 2017. ISBN: 978-1-4503-4867-6. Doi: 10.1145/3058060.3058078.
13. *Anton Plenkin, Konstantin Rumyantsev.* Features of Detection of a Single-Photon Pulse at Synchronization in Quantum Key Distribution Systems. Track Name. Imaging & Vision // Proceedings of the 6th International Conference on Informatics, Electronics & Vision (ICIEV) // 1−3.09.2017. University of Hyogo, Himeji, Hyogo, Japan. Paper 109.
14. *Rumyantsev K.E., Pljonkin A.P.* Synchronization Safety Problem in Quantum Key Distribution System // Proceedings of the International Conference on Electronics, Information, and Communication. 11-14 January 2017. Phuket, Thailand.
15. *Rumyantsev K.E., Rudinsky E.A.* Time synchronization method in quantum key distribution system with automatic compensation of polarization distortions // Proceedings of the 2017 International Conference on Cryptography, Security and Privacy (ICCSP 2017), Wuhan, China, March 17-19, 2017. Paper 91.
16. *Румянцев К.Е., Рудинский Е.А.* Двухэтапный временной алгоритм синхронизации в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Известия ЮФУ. Технические науки. – 2017. – № 5 (190). – С. 75-89.
17. *Rumyantsev K.E., Rudinsky E.A.* Parameters of the two-stage synchronization algorithm for the quantum key distribution system // Proceedings of the 10th International Conference on Security of Information and Networks (SIN-2017), Manipal University Jaipur, Rajasthan, India, October 13-15, 2017. Paper 116.
18. *Anton Plenkin, Konstantin Rumyansev, Eugene Rudinsky.* Comparative analysis of single-photon synchronization algorithms in the quantum key distribution system // Proceedings of the IEEE East-West Design & Test Symposium (EWDTS), Serbia, Novi Sad, 29.09-2.10.2017. Paper 120.
19. *Шереметьев А.Г.* Статистическая теория лазерной связи. – М.: Связь, 1971. – 264 с.
20. *Eugene Rudinsky and Konstantin Rumyantsev.* Graph-analytical method for estimating single-photon synchronization parameters of an auto-compensation quantum key distribution system // Proceedings of the First International Conference on Futuristic Trends in Network and Communication Technologies (FTNCT-2018). Department of Computer Science and Engineering, Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh, India. February 9-10, 2018. Submission ID 166.

REFERENCES

1. 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.
2. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography, *Reviews of Modern Physics*, 2002, Vol. 74, No. 1, pp. 145-195.
3. *Rumyantsev K.E.* Sinkhronizatsiya v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoy kompensatsiey polyarizatsionnykh iskazheniy [Synchronisation in quantum key distribution system with automatic indemnification of polarising distortions], *Telekommunikatsii* [Telecommunications], 2017, No. 2, pp. 32-40.
4. *Plenkin A.P.* Issledovanie rezhima vkhozhdeniya v sinkhronizm pri ispol'zovanii fo-onnykh 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: Cb. materialov mezhdunarodnogo nauchnogo e-simpoziuma. Rossiya, g. Moskva, 27-28 dekabrya 2014 g.* [ES-FM-2014-011: Collector materials of the international scientific e-Symposium. Russia, Moscow, 27-28 December 2014]. Kirov: MTSNIP, 2015, pp. 101-113.
5. *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* [Photonics], 2012, No. 5, pp. 54-66.
6. *Rumyantsev K.E.* Zashchita protsessa sinkhronizatsii v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoy kompensatsiey polyarizatsionnykh iskazheniy [Synchronisation in quantum key distribution system with automatic indemnification of polarising distortions], *Telekommunikatsii* [Telecommunications], 2017, No. 3, pp. 36-44.
7. *Rumyantsev K.E., Plenkin A.P.* Sinkhronizatsiya sistemy kvantovogo raspredeleniya klyucha v rezhime odnofotonnoy registratsii impul'sov dlya povysheniya zashchishchennosti [Synchronization system of quantum key distribution in the regime of single-photon pulses registering for enhanced protection], *Radiotekhnika* [Radioengineering], 2015, No. 2, pp. 125-134.
8. *Rumyantsev K.E., Plenkin A.P.* Povyshenie effektivnosti algoritma vkhozhdeniya v sinkhronizm sistemy kvantovogo raspredeleniya klyuchey [Improving efficient of synchronization algorithm of quantum key distribution system], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 8 (169), pp. 6-19.
9. *Pljonkin A., Rumjantsev K.* Preliminary Stage Synchronization Algorithm of Autocompensation Quantum Key Distribution System with an Unauthorized Access Security, *Proceeding of the 15th International Conference on Electronics, Information, and Communication 2016 (ICEIC 2016). Jan 27−30, 2016. Danang, Vietnam*. Paper № 1570220423.
10. *Pljonkin A., Rumjantsev K.* Single-photon Synchronization Mode of Quantum Key Distribution System, *Proceeding of the International Conference on Computational Techniques in Information and Communication Technology. 2016. (ICCTICT 2016). 11th – 13th March 2016. New Delhi, India*. Paper 1570218403.
11. *Guyadichi A., Simmeres D., Veroneze D., Biazi R., SHulinatti A., Rich I., Gilni M., Makyan'ti P.* Kompaktnye moduli na osnove SPAD-detektorov dlya registratsii odinochnykh fotonov v blizhney infrakrasnoy oblasti spektra [Compact modules based on SPAD-detectors for registration single photons in the near infrared region of the spectrum], *Fotonika* [Photonics], 2012, No. 6 (36), pp. 32-40.
12. *Pljonkin A.P.* Features of the Photon Pulse Detection Algorithm in the Quantum Key Distribution System, *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy (ICCSP 2017).* – P. 81-84. SP029. Wuhan, China March 17-19, 2017. ACM New York, NY, USA 2017. ISBN: 978-1-4503-4867-6. Doi: 10.1145/3058060.3058078.
13. *Anton Plenkin, Konstantin Rumyantsev.* Features of Detection of a Single-Photon Pulse at Synchronization in Quantum Key Distribution Systems. Track Name. Imaging & Vision, *Proceedings of the 6th International Conference on Informatics, Electronics & Vision (ICIEV) 1−3.09.2017. University of Hyogo, Himeji, Hyogo, Japan*. Paper 109.
14. *Rumyantsev K.E., Pljonkin A.P.* Synchronization Safety Problem in Quantum Key Distribution System, *Proceedings of the International Conference on Electronics, Information, and Communication. 11-14 January 2017. Phuket, Thailand.*

15. *Rumyantsev K.E., Rudinsky E.A.* Time synchronization method in quantum key distribution system with automatic compensation of polarization distortions, *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy (ICCSP 2017), Wuhan, China, March 17-19, 2017*. Paper 91.
16. *Rumyantsev K.E., Rudinskiy E.A.* Dvukhetapnyy vremennoy algoritm sinkhronizatsii v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoy kompensatsiey polyarizatsionnykh iskazheniy [Two - stage timing algorithm of synchronization in quantum key distribution system with automatic polarization distortion compensation], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2017, No. 5 (190), pp. 75-89.
17. *Rumyantsev K.E., Rudinsky E.A.* Parameters of the two-stage synchronization algorithm for the quantum key distribution system, *Proceedings of the 10th International Conference on Security of Information and Networks (SIN-2017), Manipal University Jaipur, Rajasthan, India, October 13-15, 2017*. Paper 116.
18. *Anton Plenkin, Konstantin Rumyansev, Eugene Rudinsky.* Comparative analysis of single-photon synchronization algorithms in the quantum key distribution system, *Proceedings of the IEEE East-West Design & Test Symposium (EWDTS), Serbia, Novi Sad, 29.09-2.10.2017.* Paper 120.
19. Sheremet'ev A.G. Statisticheskaya teoriya lazernoy svyazi [Statistical theory of laser coupling]. Moscow: Svyaz', 1971, 264 p.
20. *Eugene Rudinsky and Konstantin Rumyantsev*. Graph-analytical method for estimating single-photon synchronization parameters of an auto-compensation quantum key distribution system, *Proceedings of the First International Conference on Futuristic Trends in Network and Communication Technologies (FTNCT-2018). Department of Computer Science and Engineering, Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh, India. February 9-10, 2018. Submission ID 166*.

Статью рекомендовал к опубликованию к.ф.-м.н. А.А. Бутин.

Румянцев Константин Евгеньевич − Южный федеральный университет; e-mail: rke2004@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 89281827209; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Рудинский Евгений Андреевич – e-mail: rud.ea@mail.ru; тел.: 89198978808; кафедра информационной безопасности телекоммуникационных систем; аспирант.

Rumyantsev Konstantin Evgenievich – Southern Federal University; e-mail: rke2004@mail.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +79281827209; the department of information security of telecommunication systems; head of department; dr. of eng. sc.; professor.

Rudinsky Evgeny Andreevich – e-mail: rud.ea@mail.ru; phone: +79198978808; the department of information security of telecommunication systems; postgraduate student.