Оригинальная статья / Original article

https://doi.org/10.21869/2223-1536-2025-15-1-144-156

УДК 004.052

Модель обработки сообщений от нескольких источников, кодированных в режиме сцепления блоков

М. О. Таныгин[1] ✉, М. В. Посканный[1]

[1] Юго-Западный государственный университет
ул. 50 лет Октября, д. 94, г. Курск 305040, Российская Федерация

✉ e-mail: tanygin@yandex.com

Резюме

Цель исследования. *В статье рассматривается модель обработки сообщений, поступающих в приёмник из нескольких источников. Для класса распределённых систем с ограничениями на размер передаваемых сообщений и размер их идентификационных полей актуальным является использование кодирования в режиме сцепления блоков, которое при неизменном размере идентификатора предполагает существенно меньшую вероятность коллизии идентификаторов. Негативным последствием этого является необходимость определять источник не для одного сообщения, а для последовательности сообщений, ассоциированных с источником. В результате чего в приёмнике одно и то же сообщение в каждый момент времени может рассматриваться как потенциальное сообщение от нескольких источников, вынуждая хранить его в различных банках результатов промежуточных вычислений. Цель работы состоит в снижении вероятности ошибки определения источника сообщений за счёт учёта результатов параллельной обработки в независимых структурах.*

Методы. *Рассмотрен подход к повышению достоверности обработки сообщений заключается в параллельном формировании динамических структур, хранящих сообщения, которые могут быть ассоциированы с соответствующим источником. При принятии решения о принадлежности сообщения одному из рассматриваемых источников, информация о таком сообщении удаляется из всех структур, в которых она содержалась, так как для таких структур это сообщение является посторонним.*

Результаты. *Создана математическая модель параллельной обработки сообщений в независимых структурах. Рассчитаны вероятности возникновения ошибок на основе использования метода без использования совместной обработки сообщений и с использованием. Графически построены зависимости возникновения ошибок от величины интенсивности и длины сообщений. Получены значения вероятностей ошибок для двух сравниваемых вариантов обработки данных.*

Заключение. *В статье показано, как использование результатов обработки сообщений в независимых структурах, ассоциированных с соответствующим источником распределённой системы, может сказаться на достоверности и трудоёмкости процесса определения источников сообщений, кодированных в режиме сцепления блоков.*

Ключевые слова: *передатчик; приёмник; целевой источник; сцепление блоков; длина поля; последовательность сообщений; вероятность формирования; интенсивность.*

Конфликт интересов*: Авторы декларируют отсутствие конфликта интересов, связанных с публикацией данной статьи.*

Для цитирования: Таныгин М. О., Посканный М. В. Модель обработки сообщений от нескольких источников, кодированных в режиме сцепления блоков // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2025. Т. 15, № 1. С. 144–156. https://doi.org/ 10.21869/2223-1536-2025-15-1-144-156

Поступила в редакцию 24.01.2025 *Подписана в печать 18.02.2025* *Опубликована 31.03.2025*

A model for processing messages from multiple sources encoded in the block coupling mode

Maxim O. Tanygin[1] ✉, Mikhail V. Poskannyy[1]

[1] Southwest State University
50 Let Oktyabrya Str. 94, Kursk 305040, Russian Federation

✉ e-mail: tanygin@yandex.com

Abstract

Purpose of research*. The article considers a model for processing messages received by the receiver from several sources. For a class of distributed systems with restrictions on the size of transmitted messages and the size of their identification fields, it is relevant to use block coupling encoding, which, with the identifier size unchanged, implies a significantly lower probability of identifier collisions. A negative consequence of this is the need to identify the source not for a single message, but for a sequence of messages associated with the source. As a result, the receiver can consider the same message at any given time as a potential message from several sources, forcing it to be stored in various banks of intermediate calculation results. The aim of the work is to reduce the probability of error in determining the source of messages by taking into account the results of parallel processing in independent structures.*

Methods. *An approach to improving the reliability of message processing is considered. It consists in the parallel formation of dynamic structures storing messages that can be associated with the corresponding source. When deciding whether a message belongs to one of the sources under consideration, information about such a message is deleted from all structures in which it was contained, since for such structures this message is extraneous.*

Results. *A mathematical model of parallel message processing in independent structures has been created. The probabilities of errors are calculated based on the use of the method without using joint message processing and using. The dependences of error occurrence on the intensity and length of messages are graphically plotted. Error probability values were obtained for the two compared data processing options.*

Conclusion. *The article shows how using the results of message processing in independent structures associated with the corresponding source of a distributed system can affect the reliability and complexity of the process of determining the sources of messages encoded in the block coupling mode.*

Keywords: *transmitter; receiver; target source; block coupling; field length; message sequence; probability of formation; intensity.*

Conflict of interest: *The authors declares no conflict of interest related to the publication of this article.*

For citation: Tanygin M.O., Poskannyy M.V. A model for processing messages from multiple sources encoded in the block coupling mode. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Serija: Upravlenie, vychislitel'naja tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering.* 2025;15(1):144–156. (In Russ.) https://doi.org/ 10.21869/2223-1536-2025-15-1-144-156

Received 24.01.2025 *Accepted 18.02.2025* *Published 31.03.2025*

***

Введение

В современном мире существует много подходов к обмену информацией между удалёнными абонентами. При передаче сообщений от источника к приёмнику могут возникать различные ошибки, порождаемые наличием в передающем тракте помех, наличием других абонентов, использующих данный канал связи, особенностями кодирования данных и другими факторам. Помимо этого возможны ошибки получения сообщений от других источников, которые будут опознаны приёмником как сообщения от целевого истчоника [1]. Принимая сообщения от посторонних передатчиков, приёмник может неверно выстроить поток информации, что приведёт к некорректной её последующей обработке. В рамках настоящей работы мы рассматриваем класс ошибок, связанных с некорректным определением в приёмнике последовательности поступающих от источника сообщений, кодированных в режиме сцепления блоков (Cipher Block Chaining – CBC) [2]. Стандартный метод CBC имеет ряд ограничений и уязвимостей, которые на данный момент ограничивают его применение [3]. Обычными для такого алгоритма проблемами являются проблемы распространения ошибки и невозможности распараллеливания процессов вычислений. Последний из данных недостатков [4] значительно замедляет работу алгоритма в сравнении с другими актуальными на данный момент решениями. В рамках данной статьи рассмотрен алгоритм аутентификации, т. е. подтверждения авторства поступающих в приёмник сообщений, основанный на CBC и обладающий главным его преимуществом – более высокой достоверностью по сравнению с обычным блочным кодированием, но имеющий ряд доработок, позволяющих значительно повысить скорость обнаружения ошибок при приёме сообщений от большого количества источников информации.

Материалы и методы

Рассмотрим общий подход к аутентификации в условиях множественности источников сообщений. В приёмник поступает некоторая последовательность сообщений $p_1, p_2 \dots p_i$. Для кодирования сообщений [5] источник использует известный источнику и приёмнику ключ Q. Пусть $u_1 u_2 \dots u_i$ – множество закодированных таким образом сообщений.

Алгоритм кодирования исходного сообщения представим с помощью функции E_Q. Кодирование сообщения в таком случае будет происходить по формуле

$$u_i = E_Q\left(p_i, Q\right). \qquad (1)$$

Для удобства обработки сообщений они хранятся в буферной памяти приёмника [6]. Каждое закодированное сообщение состоит из двух слов – u^{inf} и u^h. Слово u^{inf} закодированного сообщения содержит информацию о адресе данного сообщения. Хеш-составляющая хранит информацию о следующем элементе последовательности. В соответствии с принципами кодирования в режиме сцепления блоков должно выполняться следующее условие:

$$u_2^{\inf} \oplus Q = u_1^h . \qquad (2)$$

Таким образом, сообщения в приёмнике выстраиваются в некоторую последовательность, которую можно представить в виде графа (рис. 1). Боковые ветви формируются в результате получения приёмником сообщений от сторонних источников.

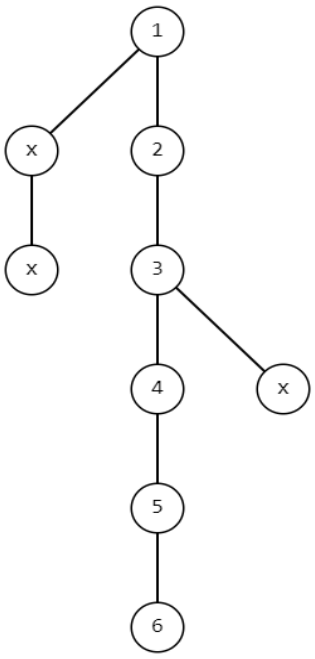

Рис. 1. Представление цепочки сообщений в виде графа [7]

Fig. 1. Representation of the message chain in the form of a graph [7]

Определение последовательности аутентичных сообщений [8] происходит с помощью вычисления наибольшей длины последовательности только тогда, когда приёмник примет определённое количество закодированных сообщений от данного источника. Именно те сообщения, которые следуют друг за другом по правилам блочного кодирования, будут опознаны как сообщения целевого источника. Определить такие цепочки можно, приняв только последовательность сообщений, из которых будет формироваться ряд из 5 и более [9]. На данном графе цепочка целевого приёмника обозначена цифрами, а нежелательные элементы обозначены символом *x*.

В реальных условиях работы приёмник зачастую принимает сообщения от большого количества источников [10]. Представим ситуацию, в которой приёмник получает сообщения от двух источников (рис. 2).

На каждом из представленных графов корректной последовательностью сообщений определяется цепочка сообщений (на рис. 2 – сообщения с цифрами). Посторонние сообщения, полученные в процессе передачи, отмечены символом *x*. Элементы, хранящие информацию об адресации сообщений в буфере [11], можно определить как вершины графа, а дугами графа в данном случае будут хеши, за счёт которых происходит построение последовательностей сообщений. Каждое сообщение обоих источников имеет равный шанс попасть в любую ячейку кэша памяти [12], указанного на нижней части рисунка 2.

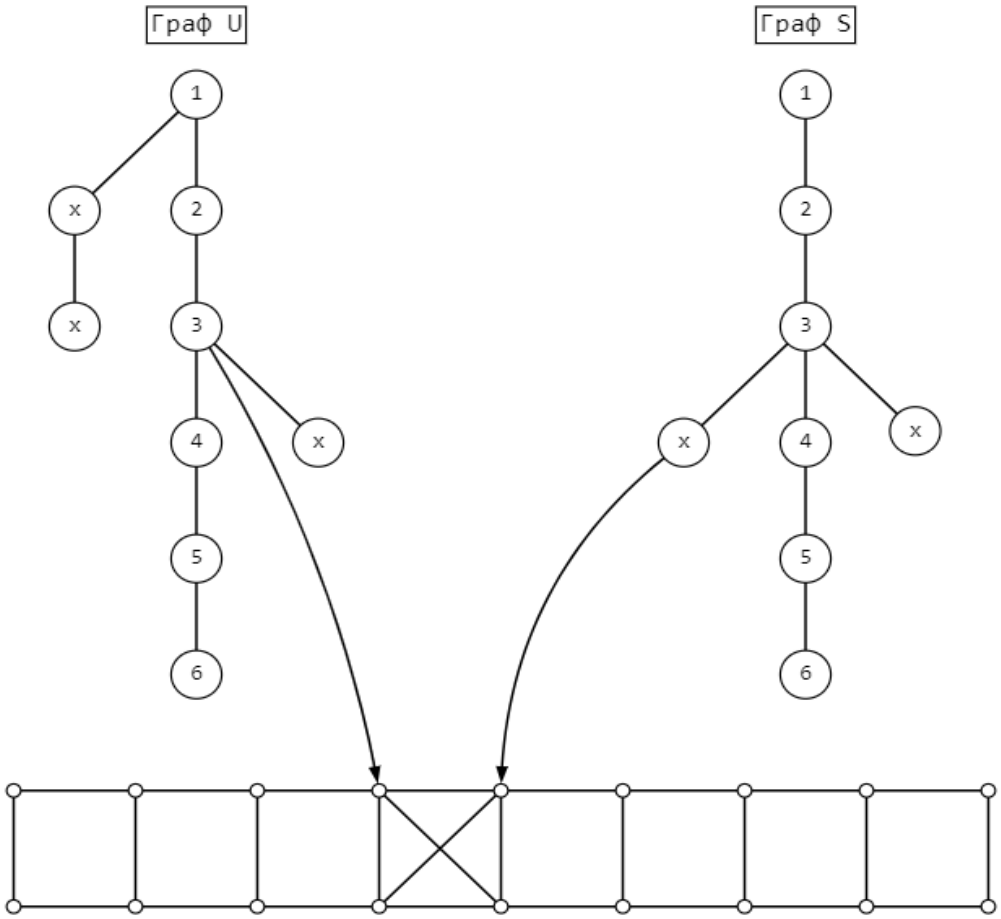

Рис. 2. Ситуация с приёмом сообщений от двух источников

Fig. 2. The situation with receiving messages from two sources

Возникают ситуации, в которых при приёме сообщений от нескольких источников приёмник находит две переменные с одинаковыми адресами, которые ведут к одной и той же ячейке информации (рис. 3).

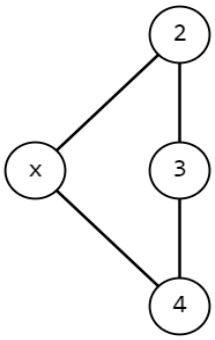

Рис. 3. Ситуация возникновения ошибки

Fig. 3. The situation of the error occurrence

Одна из них является аутентичной, а вторая – ошибочной, содержащей постороннее сообщение. Менее вероятны ошибки, описывающие более сложные кольцевые структуры, поэтому в настоящем исследовании мы их не рассматриваем. Такие ситуации чаще свойственны беспроводным вариантам передачи [13].

Если игнорировать факт обнаружения постороннего сообщения в одном графе в качестве аутентичного в другом, вероятность ошибок определяется лишь разрядностью хеша каждого сообщения. Очевидно, что в таком случае коллизию в первом графе можно предотвратить,

проанализировав граф сообщений, формируемых для другого источника, обнаружив в нём сообщение, которое сформировало коллизия в первом графе, и если оно было определено как аутентичное для второго источника, в первом графе удалить такую ветку.

Результаты и их обсуждение

Рассмотрим модель обработки сообщений от нескольких источников с контролем попадания аутентичных сообщений одних графов в другие, но уже в качестве посторонних. Она позволит рассчитать вероятности ошибок от каждого элемента последовательности элементов сообщений.

Из [14] использованы формулы для вероятности формирования коллизии в хешах сообщений, приводящих к формированию структуры, показанной на рисунке 3.

$$p_{col}(j)=\sum_{l=1}^{u-m}\left[p_j(l)\left(1-\left(1-2^{-H}\right)^l\right)\right], \quad (3)$$

где $p_j(l)$ – вероятность формирования; l – побочных ветвей в j-й позиции последовательности сообщений; H – длина поля (длина хеша); U – общее число сообщений полученных приёмником; m – длина последовательности сообщений от рассматриваемого источника.

Вероятность $p_j(l)$ определяется по рекуррентным формулам [15]:

$$p_r\left(k_r\right)=\sum_{l=k_r}^{|U|-M}\left[p^w(l)\cdot\sum_{k_{r-1}=1}^{|U|-M}p_{r-1}^h\left(k_{r-1}^h\right)\frac{\left(k_{r-1}^h l2^{-H}\right)^l\cdot e^{-k_{r-1}^h l2^{-H}}}{l!}\right],$$

$$p_r^h\left(k_r^h\right)=\sum_{l=k_r^h}^{|U|-M}\left[p_r(l)\cdot\left(\left(2^{-H}\right)^{j-k_r^h}\prod_{k=1}^{k_r^h}\left(1-(k-1)2^{-H}\right)\right)\right]. \quad (4)$$

Имеем L+1 источников информации, тогда каждый источник формирует сообщение с интенсивностью K_j, $j = 0…L$, длина последовательности сообщений j-го источника m_j. Каждое сообщение j-го источника дополняется хешем размером H_j, $j = 0…L$. Кроме источников информации, для которых происходит процесс идентификации [6], в системе действует источник посторонних сообщений, который осуществляет навязывание ложных данных [16] (каждое его сообщение считаем сформированным случайно). В реальности может быть несколько таких источников, но для упрощения модели мы объединяем их в один, считая суммарную интенсивность таких источников равной K*, и длину последовательности таких посторонних сообщений принимаем за m*

Рассматриваем обработку сообщений от 0-го источника [17]. Вероятность коллизии для одного сообщения данного источника будет равна p_{col}^{0} и определяется по формуле (1) при условии, что $U = \frac{\sum_{i=0}^{L} K_i + K^*}{K_0} m_0$, $m = m_0$, $H = H_0$.

Вероятность того, что сообщение, сформировавшее коллизию, было сформировано источником под номером $j = 1 \ldots L$, определится как $\frac{K_j}{\sum_{i=1}^{L} K_i + K^*}$.

Вероятность того, что сообщение от данного j-го источника будет обработано без ошибок и раньше, чем текущее сообщение нулевого источника, равно произведению $\left(1 - p_{\text{col}}^{j}\right)\frac{K_j}{K_j + K_0}$, где p_{col}^{j} – вероятность коллизии в таком сообщении j-го источника (определяется также по формуле (1) с параметрами $U = \frac{\sum_{i=0}^{L} K_i + K^*}{K_j} m_j$, $m = m_j$, $H = H_j$).

Тогда вероятность ошибки при обработке m_0 сообщений рассматриваемого нулевого источника определится по формуле

$$P^{\text{MET}} = 1 - \left\{ \left(1 - p_{\text{col}}^{0}\right) + p_{\text{col}}^{0} \sum_{l=1}^{L} \left[\frac{K_j}{\sum_{i=1}^{L} K_i + K^*} \left(1 - p_{\text{col}}^{j}\right) \frac{K_j}{K_j + K_0} \right] \right\}^{m_0}. \quad (5)$$

Вероятность возникновения ошибки без использования рассматриваемого метода определится по формуле совместного наступления m_0 независимых событий [18]:

$$P^{\text{ORIG}} = 1 - \left(1 - p_{\text{col}}^{0}\right)^{m_0}. \quad (6)$$

Опираясь на описанные формулы, построим графики [19] сравнения моделей без использования совместной обработки сообщений и с использованием этого алгоритма (рис. 4).

Анализируя оба графика, можно отметить, что в диапазоне параметров, где вероятность ошибки без использования контроля сообщений в графах не превышает 0,2, использование такого контроля позволяет снизить исходную вероятность ошибки в 2–3 раза (до значений, не превышающих 0,1). Такая тенденция в графике наблюдается при увеличении длины сообщений. Относительное уменьшение вероятности (значение (P^{MET} – P^{ORIG}) / P^{ORIG}) приведено ниже (рис. 5).

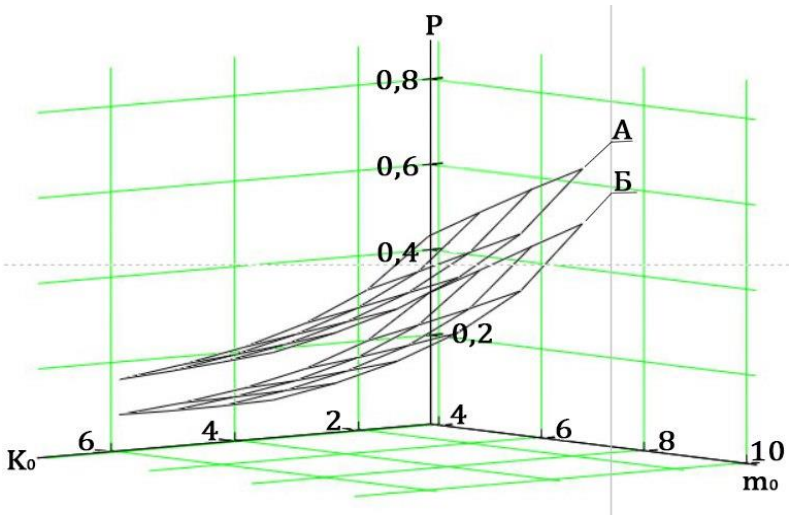

Рис. 4. Вероятность ошибочной обработки последовательности сообщений источника в зависимости от интенсивности формирования источником сообщений K_0 и длины последовательности сообщений m_0 при $\sum_{i=1}^{L} K_i + K^* = 56$: А – без использования совместной обработки сообщений; Б – с использованием совместной обработки сообщений

Fig. 4. Depending on the intensity of formation the source of the messages K_0 and the length of the message sequence m_0 when $\sum_{i=1}^{L} K_i + K^* = 56$: A – without using joint message processing; Б – using joint message processing

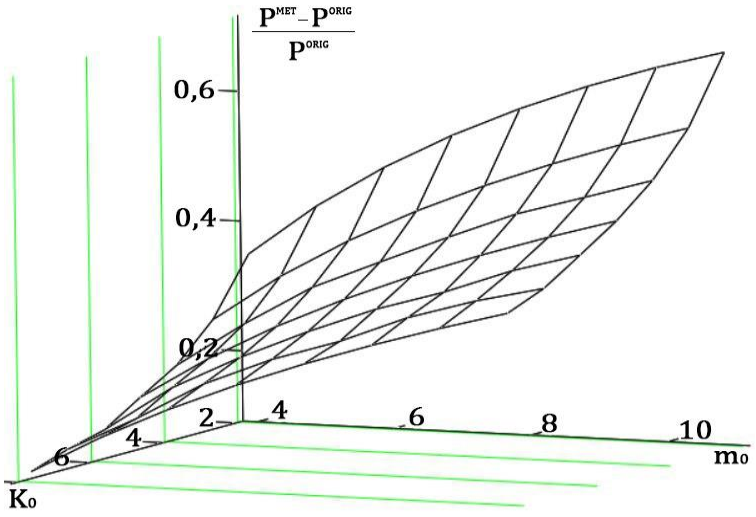

Рис. 5. Зависимость отношения разности P^{MET} и P^{ORIG} к P^{ORIG} от интенсивности формирования источником сообщений K_0 и длины последовательности сообщений m_0 при $\sum_{i=1}^{L} K_i + K^* = 56$

Fig. 5. The dependence of the ratio of the difference between P^{MET} and P^{ORIG} to P^{ORIG} on the intensity of the formation of messages by the source K_0 and the length of the message sequence m_0 at $\sum_{i=1}^{L} K_i + K^* = 56$

Исходя из полученного графика видно, что при увеличении интенсивности [20] и длины сообщений отношение разности вероятности появления ошибки с использованием ранее описанного метода и без него к P^{ORIG} увеличивается, делая более целесообразным контроль попадания сообщений в различные динамические структуры, формируемые приёмником.

Выводы

В данной работе был рассмотрен алгоритм с использованием совместной обработки сообщений. Были обозначены основные понятия, такие как интенсивность, длина поля сообщений, длина последовательности сообщений, вероятность возникновения ошибки. Графически проиллюстрирован принцип работы алгоритма и пример возникновения ошибки в рамках передачи информации на основе работы приёмника несколькими источниками единовременно. Рассчитаны вероятности возникновения ошибок с использованием контролем попадания аутентичных сообщений одних графов в другие и без такового контроля. Построены графики вероятности ошибочной обработки последовательности сообщений источника в зависимости от интенсивности формирования источником сообщений K_0 и длины последовательности сообщений m_0 и, а также зависимости относительного уменьшения исходной вероятности ошибки в зависимости от данных параметров. Исследования показали, что эффективность подхода увеличивается с уменьшением изначальной вероятности ошибки при большом числе сообщений в последовательности и высокой относительной интенсивности формирования сообщений целевым источником. В области высокой исходной вероятности ошибки (0,4–0,6) она снижается до диапазона 0,2–0,4. При исходной вероятности ошибки менее 0,2 достигается кратное снижение вероятности ошибки до уровня 0,05–0,10.

Данное исследование предполагает его развитие в области проектирования высокопроизводительных алгоритмов поиска сообщений в различных графах, формируемых приёмником, а также исследование влияния интенсивности множества источников на достигаемые показатели достоверности с целью балансирования интенсивности передаваемых сообщений для достижения оптимальной общей вероятности ошибок определения источника сообщений.

Список литературы

1. O'Brien D., Rajbhandari S., Chun H. Transmitter and receiver technologies for optical wireless // Philos. Trans. A Math. Phys. Eng. Sci. 2020. N 378 (2169). P. 20190182. https://doi.org/10.1098/rsta.2019.0182

2. Таныгин М. О., Ахмад А. А., Казакова О. В. Модель размещения данных во внутренней памяти вычислителя, реализующего схему кодирования данных в режиме сцепления блоков // Известия Юго-Западного государственного университета. 2023. Т. 27, № 1. С. 73–91. https://doi.org/10.21869/2223-1560-2023-27-1-73-91

3. Бакулина М. П. Эффективный метод блочного кодирования двухуровневых изображений // Программные продукты и системы. 2017. Т. 30, № 2. С. 282–285. https://doi.org/10.15827/0236-235X.030.2.282-285

4. Уязвимости в учете времени при симметричной расшифровке в режиме CBC с использованием заполнения. URL: https://learn.microsoft.com/ru-ru/dotnet/standard/security/vulnerabilities-cbc-mode (дата обращения: 04.12.2024).

5. Wolfowitz J. The coding of messages subject to chance errors. URL: https://projecteuclid.org/journalArticle/Download?urlId=10.1215%2Fijm%2F1255380682 (дата обращения: 10.12.2024).

6. Таныгин М. О., Альшаяа Х. Ю., Кулешова Е. А. Способ контроля целостности информации передаваемых блоков // Радиоэлектроника, информатика, управление. 2020. № 1. С. 181–189.

7. Zhanfang Zhao, Sung-Kook Han, In-Mi So. Architecture of Knowledge Graph Construction Techniques // International Journal of Pure and Applied Mathematics. 2018. Vol. 118, N 19. P. 1869–1883.

8. Плугатарев А. В. Модель определения источника сообщений на основе статистического анализа метаданных в открытом канале связи // Прикаспийский журнал: управление и высокие технологии. 2022. № 4 (60). С. 30–37.

9. Таныгин М. О., Чеснокова А. А., Ахмад А. А. А. Снижение ресурсных затрат на обработку кодов аутентификации сообщений за счет ограничения числа обрабатываемых сообщений // Прикаспийский журнал: управление и высокие технологии. 2022. № 4 (60). С. 22–29.

10. Установление доверительного канала обмена данными между источником и приёмником информации с помощью модифицированного метода одноразовых паролей / М. О. Таныгин, Х. Я. Алшаиа, В. А. Алтухова, А. Л. Марухленко // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. Т. 8, № 4 (29). С. 63–71.

11. Kai Luo, Athanassios Manikas. Joint Transmitter – Receiver Optimization in Multi-target MIMO Radar // IEEE Transactions on Signal Processing. 2017. Vol. 65, is. 23. P. 6292–6302. https://doi.org/10.1109/TSP.2017.2726993

12. Bidokhti Sh. S., Wigger M., Timo R. Noisy Broadcast Networks With Receiver Caching // IEEE Transactions on Information Theory. 2018. Vol. 64, is. 11. P. 6996–7016. https://doi.org/10.1109/TIT.2018.2835507

13. Методика оценки функциональных характеристик систем радиомониторинга при ограниченных данных о параметрах надежности / Ю. В. Васильков, А. В. Тимошенко,

В. А. Советов, А. С. Кирмель // Труды МАИ. 2019. № 108. С. 1–23. https://doi.org/10.34759/trd-2019-108-16

14. Повышение скорости обнаружения ошибок при формировании цепочек блоков данных на основе анализа числа совпадений хешей / М. О. Таныгин, Е. А. Кулешова, А. В. Митрофанов, Е. Ю. Гладилина // Прикаспийский журнал: управление и высокие технологии. 2022. № 1 (57). С. 85–93. https://doi.org/10.54398/2074-1707_2022_1_85

15. Mathematical modelling and discrete mathematics: opportunities for modern mathematics teaching / G. Greefrath, H.-S. Siller, K. Vorhölter, G. Kaiser // ZDM – Mathematics Education. 2022. Vol. 54. P. 865–879.

16. Tung-Huang Feng, Wei Teng Li, Min-Shiang Hwang. A false data report filtering scheme in wireless sensor networks: A Survey // International journal of network security. 2015. Vol. 17, N 3. P. 141.

17. Таныгин М. О., Алшаиа Х. Я., Митрофанов А. В. Сложность алгоритма определения источника данных // Труды МАИ. 2021. № 117. С. 1–21. https://doi.org/10.34759/trd-2021-117-12

18. The classical origin of modern mathematics / F. Gargiulo, A. Caen, R. Lambiotte, T. Carletti // EPJ Data Science. 2016. N 5. P. 26. https://doi.org/10.1140/epjds/s13688-016-0088-y

19. Таныгин М. О. Исследование вероятности возникновения одного типа ошибок в системе определения источника информационных пакетов // Известия вузов. Приборостроение. 2020. Т. 63, № 9. С. 777–785. https://doi.org/10.17586/0021-3454-2020-63-9-777-7

20. Spyros G. Tzafestas. Information I: Communication, Transmission, and Information Theory // Energy, Information, Feedback, Adaptation, and Self-organization. Cham: Springer, 2018. P. 157–217.

Reference

1. O'Brien D., Rajbhandari S., Chun H. Transmitter and receiver technologies for optical wireless. *Philos. Trans. A Math. Phys. Eng. Sci.* 2020;(378):20190182. https://doi.org/10.1098/ rsta.2019.0182

2. Tanygin M.O., Akhmad A.A., Kazakova O.V. A model for placing data in the internal memory of a computer implementing a data encoding scheme in the block coupling mode. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2023;27(1):73–91. (In Russ.) https://doi.org/10.21869/2223-1560-2023-27-1-73-91

3. Bakulina M.P. Effective method of block coding of two-level images. *Programmnye produkty i sistemy = Software Products and Systems*. 2017;30(2):282–285. (In Russ.) https://doi.org/ 10.15827/0236-235X.030.2.282-285

4. Time accounting vulnerabilities in symmetric decryption in CBC mode using padding. Available at: https://learn.microsoft.com/ru-ru/dotnet/standard/security/vulnerabilities-cbc-mode (accessed 04.12.2024)

5. Wolfowitz J. The coding of messages subject to chance errors. Available at: https://projecteuclid.org/journalArticle/Download?urlId=10.1215%2Fijm%2F1255380682 (accessed 10.12.2024).

6. Tanygin M.O., Alshaya H.Yu., Kuleshova E.A. A method for monitoring the integrity of information of transmitted blocks. *Radioelektronika, informatika, upravlenie = Radio Electronics, Computer Science, Management*. 2020;1:181–189. (In Russ.)

7. Zhanfang Zhao, Sung-Kook Han, In-Mi So. Architecture of Knowledge Graph Construction Techniques. *International Journal of Pure and Applied Mathematics*. 2018;118(19):1869–1883. (In Russ.)

8. Plugatarev A.V. A model for determining the source of messages based on statistical analysis of metadata in an open communication channel. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies.* 2022;(4):30–37. (In Russ.)

9. Tanygin M.O. Chesnokova A.A. Akhmad A.A.A Reduction in resource costs for processing message authentication codes by limiting the number of processed messages. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies*. 2022;(4):22–29. (In Russ.)

10. Tanygin M.O., Alshaia H.Ya., Altukhova V.A., Marukhlenko A.L. Establishing a trusted data exchange channel between the source and receiver of information using a modified one-time role method. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering*. 2018;8(4):63–71. (In Russ.)

11. Kai Luo, Athanassios Manikas. Joint Transmitter – Receiver Optimization in Multi-target MIMO Radar. *IEEE Transactions on Signal Processing*. 2017;65:6292–6302. https://doi.org/10.1109/TSP.2017.2726993

12. Bidokhti Sh. S., Wigger M., Timo R. Noisy Broadcast Networks With Receiver Caching. *IEEE Transactions on Information Theory*. 2018;64:6996–7016. https://doi.org/10.1109/TIT.2018.2835507

13. Vasilkov Y.V., Timoshenko A.V., Sovetov V.A., Kirmel A.S. Methodology for assessing the functional characteristics of radio monitoring systems with limited data on reliability parameters. *Trudy MAI = Proceedings of MAI*. 2019;(108):1–23. (In Russ.) https://doi.org/10.34759/trd-2019-108-16

14. Tanygin M.O., Kuleshova E.A., Mitrofanov A.V., Gladilina E.Yu. Increasing the speed of error detection in the formation of data block chains based on the analysis of the

number of hash matches. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies.* 2022;1:85-93. (In Russ.) https://doi.org/10.54398/2074-1707_2022_1_85

15. Greefrath G., Siller H.-S., Vorhölter K., Kaiser G. Mathematical modelling and discrete mathematics: opportunities for modern mathematics teaching. *ZDM – Mathematics Education*. 2022;54:865–879.

16. Tung-Huang Feng, Wei Teng Li, Min-Shiang Hwang. A false data report filtering scheme in wireless sensor networks: A Survey. *International Journal of Network Security.* 2015;17(3):141.

17. Tanygin M.O., Alshaia H.Ya., Mitrofanov A.V. The complexity of the algorithm for determining the data source. *Trudy MAI = Proceedings of MAY*. 2021;(117):1–21. https://doi.org/10.34759 / trd-2021-117-12

18. Gargiulo F., Caen A., Lambiotte R., Carletti T. The classical origin of modern mathematics. *EPJ Data Science*. 2016;(5):26. https://doi.org/10.1140/epjds/s13688-016-0088-y

19. Tanygin M.O. Investigation of the probability of occurrence of one type of error in the system for determining the source of information packages. *Izvestiya vuzov. Priborostroenie = Journal of Instrument Engineering.* 2020;63(9):777–785. (In Russ.) https://doi.org/10.17586/0021-3454-2020-63-9-777-7

20. Spyros G. Tzafestas. Information I: Communication, Transmission, and Information Theory. *Energy, Information, Feedback, Adaptation, and Self-organization.* Cham: Springer; 2018. P. 157–217.

Информация об авторах / Information about the Authors

Таныгин Максим Олегович, доктор технических наук, декан факультета фундаментальной и прикладной информатики, Юго-Западный государственный университет, г. Курск, Российская Федерация,
e-mail: tanygin@yandex.ru,
ORCID: 0000-0002-4099-1414

Посканный Михаил Владимирович, аспирант кафедры информационной безопасность, Юго-Западный государственный университет, г. Курск, Российская Федерация,
e-mail: mposkannyy@bk.ru,
ORCID: 0009-0006-5633-5645

Maxim O. Tanygin, Candidate of Sciences (Engineering), Head of the Department of Information Security, Southwest State University, Kursk, Russian Federation,
e-mail: tanygin@yandex.ru,
ORCID: 0000-0002-4099-1414

Mikhail V. Poskanny, Post-Graduate Student of the Department of Information Security, Southwest State University,
Kursk, Russian Federation,
e-mail: mposkannyy@bk.ru,
ORCID: 0009-0006-5633-5645