Научная статья
DOI 10.66424/2071-8217-2026-2-12
УДК 003.26

ИННОВАЦИОННЫЙ МЕТОД ВИЗУАЛЬНОЙ КРИПТОГРАФИИ

И. А. Сикарев[1*], Т. М. Татарникова[2]

[1]Российский государственный гидрометеорологический университет, Санкт-Петербург, Россия
[2]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, Россия

✉ *sikarev@yandex.ru

ДЛЯ ЦИТИРОВАНИЯ
Сикарев И. А., Татарникова Т. М. Инновационный метод визуальной криптографии // Проблемы информационной безопасности. Компьютерные системы. 2026. № 2. С. 149–157.
DOI: 10.66424/2071-8217-2026-2-12

ПОСТУПИЛА 17.02.2026
ПРИНЯТА 06.05.2026
ОПУБЛИКОВАНА 15.06.2026

Издатель: Санкт-Петербургский политехнический университет Петра Великого

АННОТАЦИЯ

Предложен инновационный метод визуальной криптографии с использованием маршрутной перестановки при небольшом размере графического файла и регулярной смене ключей шифрования. Предлагается принять один пиксель изображения в качестве одного элемента шифрования, отказаться от последовательных перемещений и использовать двумерное пространство размерностью $n \times n$ для перемещения пикселей. Предлагаются сценарии применения предложенного инновационного алгоритма визуальной криптографии, такие как хранение биометрических данных в защищенном виде, совместное использование секретов и предварительная обработка изображения для блочного шифрования. Выполнена оценка предложенного метода визуальной криптографии.

КЛЮЧЕВЫЕ СЛОВА

Визуальная криптография, маршрутные перестановки, изображение, метод, программное приложение

Original article
DOI 10.66424/2071-8217-2026-2-12

VISUAL CRYPTOGRAPHY INNOVATIONS METHOD

I. A. Sikarev[1*], T. M. Tatarnikova[2]

[1]Russian State Hydrometeorological University, St. Petersburg, Russia
[2]State University of Aerospace Instrumentation, St. Petersburg, Russia

✉ *sikarev@yandex.ru

FOR CITATION
Sikarev I. A., Tatarnikova T. M. Visual cryptography innovations method. *Problems of information security. Computer systems*. 2026. No. 2, pp. 149–157.
DOI: 10.66424/2071-8217-2026-2-12
(In Russian)

ABSTRACT

Proposed innovative method of visual cryptography using route permutation for small image file size and regular change of encryption keys. It is proposed to take one pixel of the image as one encryption element, to abandon sequential movements and to use a two-dimensional space of dimension $n \times n$ for moving pixels. Application scenarios of the proposed innovative visual cryptography algorithm are proposed, such as storing biometric data in a secure form, sharing

RECEIVED 17.02.2026
ACCEPTED 06.05.2026
PUBLICATION 15.06.2026

secrets, and preprocessing images for block encryption. The proposed visual cryptography algorithm is evaluated.

KEYWORDS

Visual cryptography, route permutations, image, method, software application

1. ВВЕДЕНИЕ

Традиционными задачами обеспечения информационной безопасности являются криптографическая защита, разделение прав доступа, целостность, подлинность электронных документов и др. [1–3]. Для решения указанных задач обеспечения безопасности может использоваться визуальная криптография [4].

Визуальная криптография является методом шифрования зрительной информации – картинки или текста таким образом, что дешифрование становится механической операцией, не требующей использования компьютера.

Самый известный метод визуальной криптографии – это графическая схема с разделением секрета, разработанная М. Наором и А. Шамиром в 1994 г., согласно которой изображение разделено на n частей так, что только имеющий все n частей мог расшифровать изображение, в то время как остальные (n–1) части не несут никакой информации об оригинальном изображении. Каждая часть напечатана на отдельном диапозитиве. Расшифровка осуществлялась путем наложения всех частей, в результате чего появлялось исходное изображение. Переложение этого алгоритма в компьютерную систему предполагает наложение частей изображения друг на друга с помощью логических операций конъюнкции, дизъюнкции, исключающего или.

Если изображение представить квадратной матрицей, размер которой соответствует количеству пикселей по горизонтали и вертикали, то использование маршрутных перестановок также может стать основой шифрования изображения. Каждая промежуточная перестановка может считаться отдельным диапозитивом. Отметим, что для текстовых сообщений подобные алгоритмы уже существуют. Алгоритмы визуальной криптографии [5–8] обладают определенными недостатками и могут быть улучшены способом за счет применения идеи шифров маршрутной перестановки [9].

Идея перестановочных шифров в целом адекватна идее визуальной криптографии, поскольку процесс шифрования больше механический, чем вычислительный. Каждая перестановка может считаться одним слоем; за один элемент шифрования может быть принят один пиксель изображения.

Целью исследования является разработка инновационного метода визуальной криптографии за счет изменений схем применения маршрутной перестановки.

2. МЕТОДЫ И МАТЕРИАЛЫ

В ходе исследования рассмотрены математические аспекты переупорядочивания набора целых чисел. Также использовались методические основы следующих алгоритмов визуальной криптографии: простой алгоритм визуальной криптографии для бинарных (черно-белых) изображений [5]; визуальная схема (k, N) [6]; частный случай (2, N) визуальной схемы шифрования (k, N) [7]; алгоритм шифрования цветного изображения [8].

3. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

В ходе исследований установлено, что основной недостаток маршрутных перестановок, например, решетки Кардано состоит в том, что шифр формируется

определенным образом – слева направо, сверху вниз, что делает его легко раскрываемым. Решением данной проблемы является усиление алгоритма шифрования следующими требованиями: отказаться от последовательного вписывания символов в «окна» решетки; отказаться от последовательного поворачивания решетки по или против часовой стрелки; использовать алгоритм в двумерном пространстве размерностью $n \times n$ для перемещения пикселей; искусственно усложнить алгоритм в рамках языка программирования.

Формирование ключа в предлагаемом алгоритме состоит из следующих шагов (на примере формирования ключа 4×4):

• выбираем классическую матрицу (решетку)

*	*	*	X
*	*	*	*
X	*	X	*
*	X	*	*

• выбираем P-Box (перестановку):

*	*	*	3
*	*	*	*
1	*	4	*
*	2	*	*

• выбираем комбинацию поворотов, например, [2031].

Получаем конечный массив перестановок:

$$[2, 5, 16, 10, 15, 12, 1, 7, 9, 14, 4, 11, 8, 3, 13, 6]_{4\times4=16.}$$

На плоскости маршрут выглядит так, как на рис. 1. В линейном виде маршрут перестановок приведен на рис. 2.

Общее количество ключей рассчитывается как произведение числа матриц на число поворотов:

$$\text{Количество ключей } = 4^{N^2/4} \cdot 24 .$$

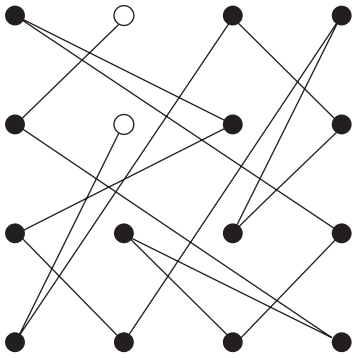

Рис. 1 | Маршрут перестановок на плоскости

Fig. 1 | The route of permutations on the plane

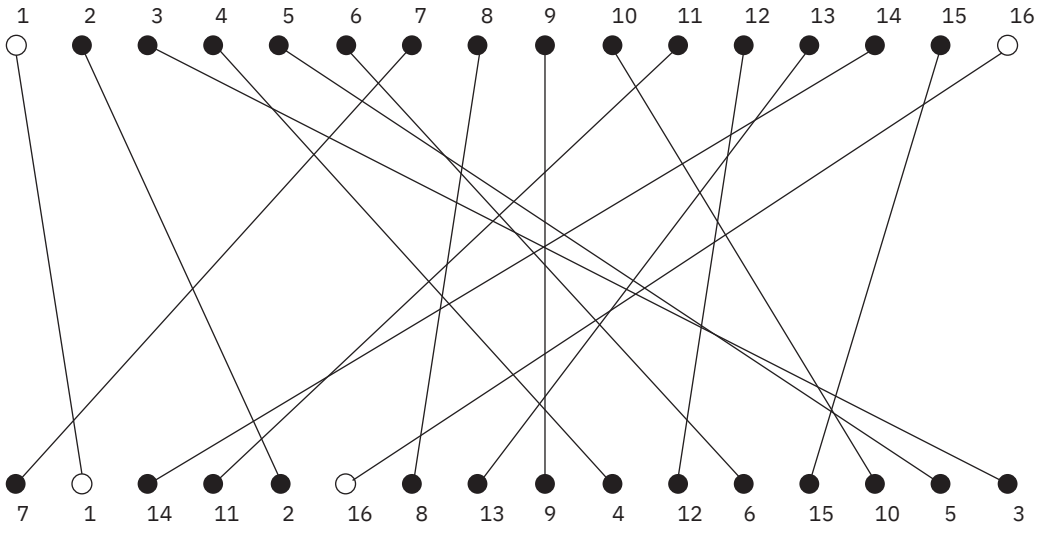

Рис. 2 | Линейный маршрут перестановок

Fig. 2 | Linear route of permutations

Для предлагаемого метода общее число матриц маршрутных перестановок равно произведению числа матриц на число поворотов и число возможных последовательностей:

$$\text{Количество ключей} = 4^{N^2/4} \cdot 24 \cdot \left[\left(\frac{N^2}{4}!\right)\right]^4.$$

На основании данных формул построим сводную таблицу с данными о количестве ключей для классического и предложенного методов в соответствии с размерностью матрицы маршрутных перестановок $n \times n$ и при $N > 16$ количество ключей в предлагаемом методе становится практически бесконечным.

На рис. 3. приведен график зависимости количества ключей от размерности матрицы 14×14, из которого можно проследить зависимость между возрастанием количества ключей с применением классического и предлагаемого метода.

Количество ключей
Quantity of keys

N	Количество ячеек	Количество ключей	
		Классический метод	Предлагаемый метод
2	4	96	96
4	256	6144	2038431744
6	262144	6291456	1,09095*E*+29
8	4294967296	1,03079*E*+11	1,97537*E*+64
10	1,13*E*+15	2,70216*E*+16	1,5642*E*+117
12	4,72*E*+21	1,13337*E*+23	2,1703*E*+189
14	3,17*E*+29	7,6059*E*+30	1,0413*E*+282
16	3,40*E*+38	8,16678*E*+39	∞

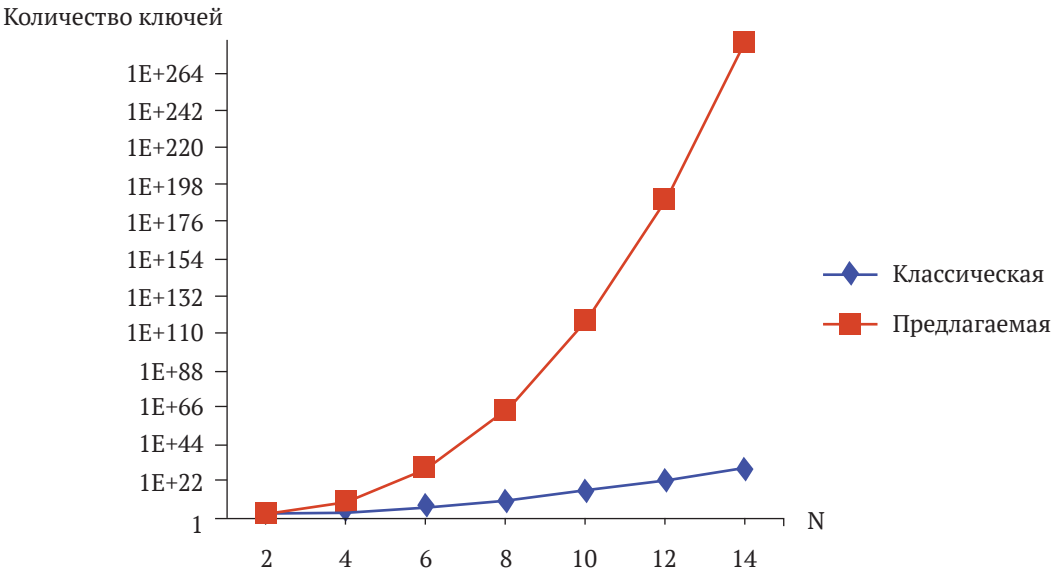

Рис. 3 | График зависимости количества ключей от способа шифрования

Fig. 3 | Graph of the dependence of the number of keys on the encryption method

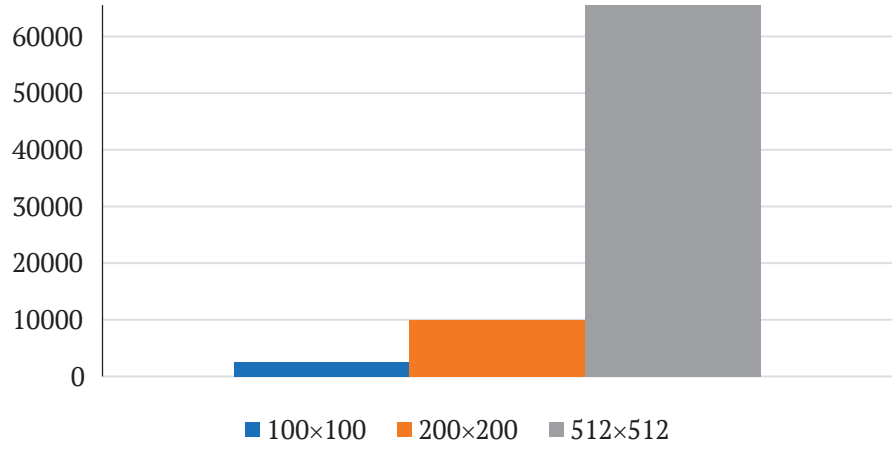

Рис. 4 | Сложность генерации маршрутных перестановок для шифрования изображений разного размера

Fig. 4 | The complexity of generating route permutations for encrypting images of different sizes

В соответствии с предлагаемым методом шифрования для визуальной криптографии оценена сложность генерации маршрутных перестановок для шифрования изображений разного размера. На рис. 4 приведены результаты этих сравнений.

4. ОБСУЖДЕНИЕ

Предлагаемый метод визуальной криптографии может найти несколько вариантов применения.

Первый сценарий – это хранение в защищенном виде биометрических данных. Разработанное приложение визуальной криптографии можно использовать для защищенного хранения визуальных файлов малого размера. Это применимо к биометрическим системам, основанным на работе с отпечатками пальцев, такие системы хранят изображения малого размера и предложенный алгоритм визуальной криптографии способен сокрыть информацию с этих изображений [10]. Также можно передавать эти зашифрованные изображения и расшифровывать их на другой стороне, для чего нужно передать файл с ключом по защищенному каналу. Злоумышленник не сможет определить, какой алгоритм шифрования использован пока не получит доступ к коду программы и не узнает способ генерации и поворота матриц.

Вторая схема применения предлагаемого алгоритма визуальной криптографии – разделение секрета путем создания коалиции участников из некоторой первоначальной группы участников с установлением утвержденного лимита числа участников коалиции. Каждый участник имеет свою сгенерированную матрицу: у одного участника решетка без поворота, у второго с поворотом на 90°, у третьего – 180°, у четвертого – 270°. После наложения всех решеток друг на друга и применения этой результирующей решетки на зашифрованное изображение получится расшифровать это изображение. При отсутствии хотя бы одной решетки расшифровать изображение не удастся, т.е. злоумышленнику недостаточно перехватить одну или несколько из решеток, ему нужно перехватить все решетки, зашифрованное изображение из открытого канала и знать какой алгоритм применялся для сокрытия секрета.

Третий вариант применения – предварительная подготовка изображения для шифрования блочными алгоритмами типа AES, GOST и др. Как правило во всех этих алгоритмах перед непосредственно шифрованием происходит выравнивание

статистических свойств блока, т.е. равновероятное распределение битов нулей и единиц. Для такого случая также можно использовать предлагаемый алгоритм.

Еще один вариант применения алгоритма – это симметричная схема обмена визуальной информацией.

В ходе исследования по предложенному методу визуальной криптографии разработано и реализовано приложение, которое работает с изображениями квадратной формы формата bmp. В приложении, согласно алгоритму, изображение разбивается на блоки и строятся матрицы перестановки. Выходом приложения является зашифрованное изображение и сообщение об их несоответствии с эталонным. В качестве справочной информации выступает файл с расширением .txt, хранящий ключи шифрования. На рис. 5 приведены результаты шифрования (справа) некоторых контрольных изображений (слева).

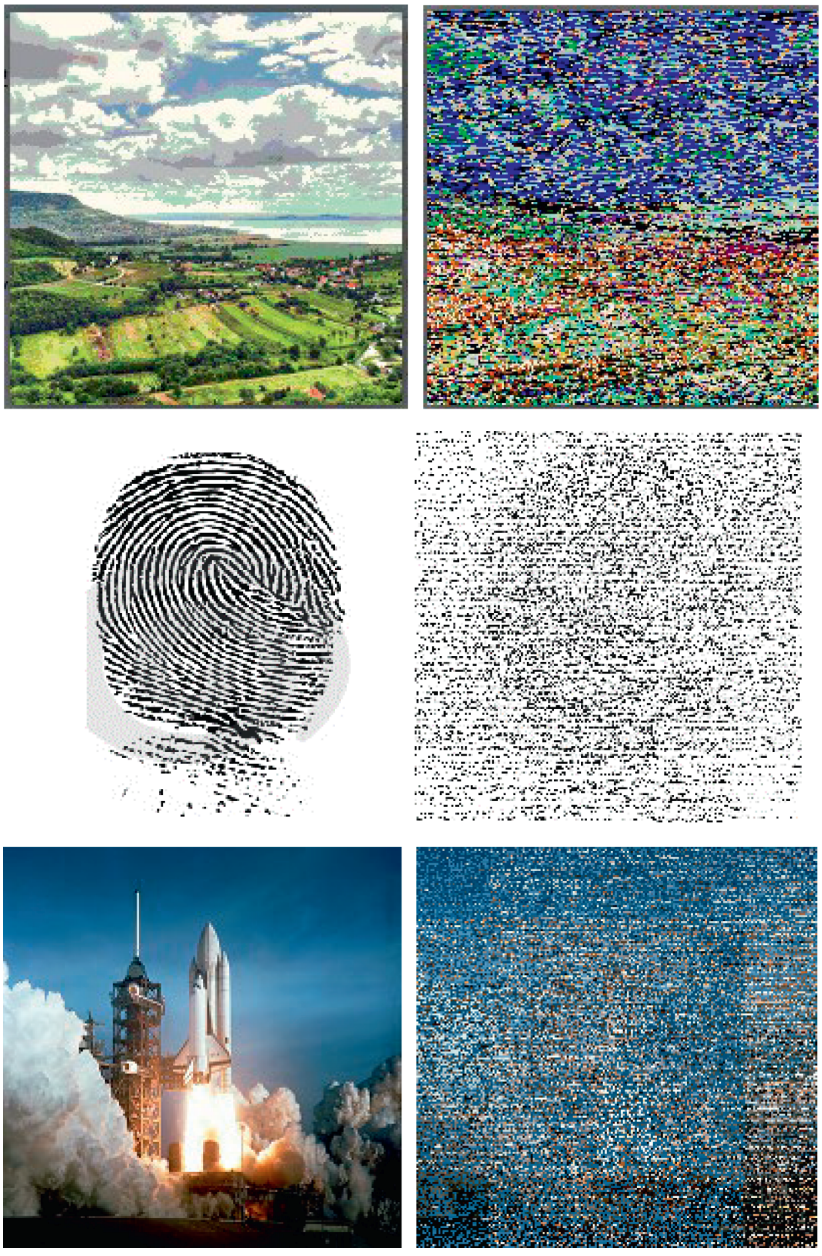

Рис. 5 | Примеры шифрования изображений небольших объемов

Fig. 5 | Examples of small-volume image encryption

5. ЗАКЛЮЧЕНИЕ

Предложено применить маршрутные перестановки для визуальной криптографии. Указано, что идея перестановочных шифров хорошо отображает идеи визуальной криптографии, заключающийся в том, что процесс шифрования сводится не к вычислениям, а перестановкам и за один элемент шифрования может быть принят один пиксель изображения.

Предложено усовершенствование классического шифра маршрутных перестановок применительно к визуальной криптографии за счет отказа от последовательных перестановок и использовании *n*-мерного пространства перестановок.

Предложенный метод может найти применение при шифровании графических файлов небольшого объема и при регулярной смене ключей шифрования/дешифрования. Выполнена оценка предложенного метода визуальной криптографии, которая показала экспоненциальный рост количества ключей в сравнении с классическим методом.

Показано, что предложенный метод может быть применен при хранении в защищенном виде биометрических данных. Следует указать, что он также может быть использован в геоинформационных системах [11–18], автоматизированных транспортных системах [19–21] и в области высшего образования [22].

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Автор заявляет об отсутствии конфликта интересов / The author declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. **Tatarnikova T. M., Sikarev I. A., Bogdanov P. Yu., Timochkina T. V.** Botnet Attack Detection Approach in Out Networks // Automatic Control and Computer Sciences. 2022. Vol. 56. № 8. P. 838–846. DOI: 10.3103/s0146411622080259. EDN: VILOAN.
2. **Сикарев И. А., Абрамов В. М., Простакевич К. С. и др.** Инфокоммуникационный инструментарий для управления природными рисками при мореплавании автономных судов в Арктике при изменении климата // Проблемы информационной безопасности. Компьютерные системы. 2024. № 1(58). С. 110–120. DOI: 10.48612/jisp/v28t-z3kr-nrn2. EDN: RUESZV.
3. **Бескид П. П., Татарникова Т. М.** О некоторых подходах к решению проблемы авторского права в сети интернет // Ученые записки Российского государственного гидрометеорологического университета. 2010. № 15. С. 199–210.
4. **Ibrahim D. R., Teh J. S., Abdullah R.** An overview of visual cryptography techniques // Multimed Tools Appl. 2021. № 80. P. 31927–31952. DOI: 10.1007/s11042-021-11229-9.
5. **Prasad S., Pal A. K.** An RGB color image steganography scheme using overlapping block-based pix-el-value differencing // Royal Society Open Science. 2017. Vol. 4. № 161066. DOI: 10.1098/ rsos.161066.
6. **Косолапов Ю. В.** О построении (k,n)-схемы визуальной криптографии с применением класса линейных хэш-функций над бинарным полем // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2018. Т. 18. Вып. 2. С. 227–239. DOI: 10.18500/1816-9791-2018-18-2-227-239. EDN: XQFNSP.
7. **Lakshmanan R., Arumugam S.** Construction of a (k, n)-visual cryptography scheme // Des. Codes Cryptogr. 2017. Vol. 82. Iss. 3. P. 629–645. DOI: 10.1007/s10623-016-0181-z.
8. **Савельева М. Г., Урбанович П. П.** Метод стеганографического преобразования web-документов на основе растровой графики и модели RGB // Труды БГТУ. Сер. 3:

Физико-математические науки и информатика. 2022. № 2 (260). С. 99–107.
9. **Татарникова Т. М.** Анализ данных в прикладных задачах обеспечения информационной безопасности. СПб. : ГУАП, 2018. 115 с.
10. **Ефремов Д. А., Борисова С. Н.** Использование отпечатков пальцев в задачах биометрического ограничения доступа // Успехи современного естествознания. 2011. № 7. С. 107–108.
11. **Sikarev I. A., Chistyakov G. B., Garanin A. V., Moskvin D. A.** Algorithms for Enhancing Information Security in the Processing of Navigation Data of Unmanned Vessels of the Technical Fleet of the Inland Waterways of the Russian Federation // Automatic Control and Computer Sciences. 2020. Vol. 54. № 8. P. 964–967. DOI: 10.3103/S0146411620080325. EDN: AKAYKV.
12. **Lukyanov S., Popov N., Sikarev I. et al.** Digital learning technologies within geoinformation management // E3S Web of Conferences, 17–19 February 2021, Chelyabinsk, Russia. 2021. P. 01004. DOI: 10.1051/e3sconf/202125801004. EDN: GWVYAN.

REFERENCES

1. **Tatarnikova T. M., Sikarev I. A., Bogdanov P. Yu., Timochkina T. V.** Botnet Attack Detection Approach in Out Networks. *Automatic Control and Computer Sciences*. 2022. Vol. 56. No. 8, pp. 838–846. DOI: 10.3103/s0146411622080259. EDN: VILOAN.
2. **Sikarev I. A., Abramov V. M., Prostakevich K. S. et al.** Infocommunication instrumentarium for natural risk management while navigation of autonomous vessels in Arctic under climate change. *Problems of information security. Computer systems*. 2024. No. 1, pp. 110–120. DOI: 10.48612/jisp/v28t-z3kr-nrn2. (In Russian)
3. **Beskid P. P., Tatarnikova T. M.** About some approaches to the copyright solution of a problem in the internet. *Proceedings of the Russian State Hydrometeorological University*. 2010. No. 15, pp. 199–210. (In Russian)
4. **Ibrahim D. R., Teh J. S., Abdullah R.** An overview of visual cryptography techniques. *Multimed Tools Appl*. 2021. No. 80, pp. 31927–31952. DOI: 10.1007/s11042-021-11229-9.
5. **Prasad S., Pal A. K.** An RGB color image steganography scheme using overlapping block-based pix-el-value differencing. *Royal Society Open Science*. 2017. Vol. 4. No. 161066. DOI: 10.1098/ rsos.161066.
6. **Kosolapov Yu. V.** On the Construction of (k, n)-Schemes of Visual Cryptography Using a Class of Linear Hash Functions Over a Binary Field. *Izv. Saratov Univ. (N. S.), Ser. Math. Mech. Inform.* 2018. Vol. 18. Iss. 2, pp. 227–239. DOI: 10.18500/1816-9791-2018-18-2-227-239. EDN: XQFNSP. (In Russian)
7. **Lakshmanan R., Arumugam S.** Construction of a (k, n)-visual cryptography scheme. *Des. Codes Cryptogr*. 2017. Vol. 82. Iss. 3, pp. 629–645. DOI: 10.1007/s10623-016-0181-z.
8. **Saveleva M. G., Urbanovich P. P.** Method of steganographic transformation of web-documents based on raster graphics and RGB model. *Proceedings of BSTU, issue 3, Physics and Mathematics. Informatics*. 2022. No. 2 (260), pp. 99–107. (In Russian)
9. **Tatarnikova T. M.** Data analysis in applied information security tasks. St. Petersburg : GUAP, 2018, 115 p.
10. **Efremov D. A., Borisova S. N.** The use of fingerprints in biometric access control tasks. *Advances in current natural sciences*. 2011. No. 7, pp. 107–108.
11. **Sikarev I. A., Chistyakov G. B., Garanin A. V., Moskvin D. A.** Algorithms for Enhancing Information Security in the Processing of Navigation Data of Unmanned Vessels of the Technical Fleet of the Inland Waterways of the Russian Federation. *Automatic Control and Computer Sciences*. 2020. Vol. 54. No. 8, pp. 964–967. DOI: 10.3103/S0146411620080325. EDN: AKAYKV.
12. **Lukyanov S., Popov N., Sikarev I. et al.** Digital learning technologies within geoinformation management. E3S Web of Conferences, 17–19 February 2021, Chelyabinsk, Russia. 2021, pp. 01004. DOI: 10.1051/e3sconf/202125801004. EDN: GWVYAN.

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

СИКАРЕВ Игорь Александрович – д-р техн. наук, профессор, Российский государственный гидрометеорологический университет, Россия, 192007, Санкт-Петербург, Воронежская ул., д. 79
Email: sikarev@yandex.ru
ORCID: 0000-0001-6289-3295

SIKAREV Igor A. – Doctor of Engineering Sciences, Professor, Russian State Hydrometeorological University, Russia, 192007, St. Petersburg, Voronezhskaya str., 79

ТАТАРНИКОВА Татьяна Михайловна – профессор, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Россия, 190000, Санкт-Петербург, Большая Морская ул., д. 67, лит. А
Email: Tm-tatarn@yandex.ru
ORCID: 0000-0002-6419-0072

TATARNIKOVA Tatiana M. – Doctor of Engineering Sciences, Professor, State University of Aerospace Instrumentation, Russia, 190000, St. Petersburg, Bolshaya Morskaya str., 67, lit. A