ОБЗОРНАЯ СТАТЬЯ
УДК 004.056.5
https://doi.org/10.26907/2541-7746.2025.3.413-436

Состояние исследований в области ассоциативной защиты данных

И.С. Вершинин, Р.Ф. Гибадуллин ✉, В.А. Райхлин

Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, г. Казань, Россия

✉ *RuslanGibadullin@vk.com*

Аннотация

Ассоциативная защита данных не имеет и никогда не имела аналогов в мировой практике, поэтому до сих пор с осторожностью воспринимается специалистами. Настала пора дать о ней целостное представление, показав ее несомненные достоинства. Наша единственная цель – убедить специалистов в этих достоинствах путем систематизации основных результатов оригинальных исследований. Без полной детализации, но с нужными ссылками рассмотрены особенности ассоциативной защиты, установленные авторами: вопросы морфологии, стегостойкость, криптостойкость, помехоустойчивость, объемы передаваемой и хранимой информации. Потенциально перспективный симбиоз стеганографии и криптографии – главный научный результат проведенного исследования. Среди частных результатов наиболее значимы разработки алгоритма маскирования и стратегий ассоциативной защиты картографических сцен и текстов; достижение т. н. полноты покрытия; открытие базовой теоремы однозначности распознавания; оценки числа ключей, стегостойкости, криптостойкости и помехоустойчивости ассоциативной защиты. Приведены ссылки на выполненные разработки систем управления базами данных (СУБД) с такой защитой. Авторы видят значительные перспективы дальнейшего развития теории и практики ассоциативной защиты данных.

Ключевые слова: ассоциативная защита картографических и текстовых данных, вопросы морфологии, симбиоз стеганографии и криптографии, повышение помехоустойчивости, снижение объемов передач, практическая ценность

Благодарности. Авторы выражают искреннюю благодарность академику В.К. Левину за поддержку работ по ассоциативной защите данных.

Для цитирования: *Вершинин И.С., Гибадуллин Р.Ф., Райхлин В.А.* Состояние исследований в области ассоциативной защиты данных // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. 2025. Т. 167, кн. 3. С. 413–436. https://doi.org/10.26907/2541-7746.2025.3.413-436.

REVIEW ARTICLE
https://doi.org/10.26907/2541-7746.2025.3.413-436

State of research in the field of associative data protection

I.S. Vershinin, R.F. Gibadullin ✉, V.A. Raikhlin

Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russia

✉ *RuslanGibadullin@vk.com*

Abstract

With no established analogues in the current or past global practice, associative data protection remains cautiously perceived by specialists. The time has come to provide an integrated perspective of this method and summarize its numerous and undoubted benefits over competing approaches. In order to demonstrate such benefits, this article overviews the main results of published original research on various aspects of associative data protection. Avoiding exhaustive detail, it focuses, with appropriate references to existing literature, on the principal features of associative data protection: morphology, steganographic strength, cryptographic strength, noise immunity, and volumes of transmitted and stored information. Our central finding is a promising symbiosis of steganography and cryptography. The most notable specific results include the development of a masking algorithm and strategies for associative protection of cartographic scenes and texts, the achievement of a so-called coverage completeness, the discovery of the basic theorem of unambiguous recognition, as well as the estimation of the number of keys, steganographic strength, cryptographic strength, and noise immunity of associative data protection. References are given to the database management systems (DBMSs) already employing associative data protection. The review highlights considerable opportunities for further elaboration of the theory and practice of associative data protection.

Keywords: associative protection of cartographic and text data, issues of morphology, symbiosis of steganography and cryptography, enhancement of noise immunity, reduction of data transmission volumes, practical value

Acknowledgments. Special thanks to Academician V.K. Levin for his valuable support of studies on associative data protection.

For citation: Vershinin I.S., Gibadullin R.F., Raikhlin V.A. State of research in the field of associative data protection. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2025, vol. 167, no. 3, pp. 413–436. https://doi.org/10.26907/2541-7746.2025.3.413-436. (In Russian)

Введение

В свое время академик П.К. Анохин заметил [1]: «А. Эйнштейн, говоря об истории науки, часто подчеркивал, что “только идеи имеют непреходящую ценность”, и очень часто сетовал, что ученые мало заботятся о написании “истории идей” ... Трудности творческого

процесса не видны обычно в конечных результатах, и поэтому для науки навсегда исчезает их познавательный и воспитательный смысл ... ». Следуя этому замечанию, сначала поясним рождение у нас идеи ассоциативной защиты данных.

Ранее Казанский авиационный институт проводил серьезные исследования в области ассоциативной обработки информации [2–4], в частности, по применению ассоциативного подхода к анализу бинарных сцен [5, 6], т. е. к укрупненному описанию изображений в терминах «объекты – координаты» [7]. В связи с этим у нас появились такие вопросы:

1) Маскирование – непременный атрибут ассоциативной обработки. Но в каких приложениях оно полезно при распознавании бинарных изображений?

2) Как преодолеть критичность ассоциативного подхода к размерам и угловому положению объектов сцены?

Ответы на оба вопроса дала идея ассоциативной защиты данных, к восприятию которой мы были уже готовы. Эта идея родилась у нас в конце прошлого века, когда возникла необходимость заняться защитой информации.

Мы различаем два вида приложений: защита картографических и текстовых данных. К конфиденциальным картографическим сценам в указанных терминах относятся карты разведывательного характера, полезных ископаемых, морские карты глубин и др. Текстовыми сценами в терминах «символы – координаты» являются характеристики таких объектов, как ракетные шахты, нефтяные скважины, залежи полезных ископаемых, содержимое береговых шельфов, различные персональные данные и др. Все это требует надежной защиты.

В основу проведенных исследований была положена методология конструктивного моделирования систем [8]. Главное в этой методологии состоит в том, что по мере накопления информации в процессе исследований формируется модель синтеза предметной системы, или S-модель (S – от Synthesis). Эта модель рассматривается как конструктивный метод. Процесс синтеза проводится с системных позиций в предположении, что синтезируемый объект моделирует поведение некоторой *гипотетической системы* – единого целого, бесконечно познаваемого и объясняемого, заданного своим оператором назначения [9]. Конструктивное моделирование позволяет выявить некоторые свойства множества эффективных реализаций системы. В силу аксиомы знания модальной логики («что известно, то верно») [10] они постулируются как закономерности и задают основу теории. *Система постулатов полагается открытой*, ибо она вводится в меру знаний и опыта, существующих в данный момент.

Для стеганографии характерно стремление обеспечить безусловную стегостойкость, т. е. невозможность установления факта передачи сообщений. Стеганографические подходы, широко применяемые в настоящее время, предполагают внедрение информации в изображение, видео- или аудиофайлы [11–15]. Имеется ряд теоретических рассмотрений т. н. совершенных стегосистем [16, 17], но их практическая реализуемость находится под сомнением. Стеганографии свойственен чрезвычайный объем сообщений. Использование для целей защиты криптографических шифров [18–21] существенно уменьшает этот объем. Но известные криптошифры обладают низкой помехоустойчивостью при хранении и передаче скрытых данных по открытым каналам связи, а развитые методы стеганографии не обеспечивают безусловную стегостойкость [22–24]. Предпринятая нами попытка симбиоза криптографии и стеганографии была призвана ликвидировать эти пробелы.

Ассоциативную защиту можно рассматривать как частный случай трафаретного способа исторической стеганографии [11], когда скрываемое сообщение записывается по трафарету на чистый лист, после чего формируется осмысленный текст с такой вставкой. Различие состоит в том, что в данном случае сообщение внедряется в шумовую картину. Но это не принципиально. Главные вопросы в обоих случаях – алгоритмизация случайного формирования трафарета (ключа) и заполнение участков, не занятых сообщением. Детали проведенных вычислительных экспериментов и все доказательства мы опускаем, что отвечает цели нашего обзора, указанной в аннотации. Эти детали содержатся в работах [25–29]. Ниже прослежена только логика исследований и приведены полученные результаты.

1. Вопросы морфологии

В данном случае использовано k-разрядное десятичное кодирование имен объектов и их координат почтовыми символами (рис. 1). Каждая десятичная цифра представлена своей двоичной матрицей-эталоном размерами $m \times n$, $m = 2n-1$. Размеры всех эталонов одинаковы. Множества их единичных элементов (показаны точками на рис. 2 (a) – для $n = 3$, рис. 2 (b) – для $n = 7$) принадлежат внешнему контуру и внутреннему «зигзагу» соответствующих матриц. Множество таких матриц мощностью $\gamma = 10$ подвергается маскированию.

Рис. 1. Множество почтовых символов
Fig. 1. Set of postal symbols

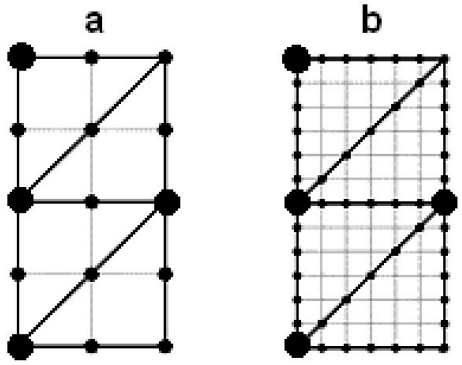

Рис. 2. Положения бинарных единиц в матрицах-эталонах при $n = 3$ (a) и $n = 7$ (b)
Fig. 2. Positions of binary ones in the etalon matrices at $n = 3$ (a) and $n = 7$ (b)

Процесс генерации масок случаен. Для каждой матрицы создается своя матрица масок тех же размеров, которая сохраняет в эталоне биты, существенные для его дальнейшей идентификации. Набор масок – это ключ распознавания. Замаскированные биты подвергаются рандомизации. В итоге исходные бинарные матрицы-эталоны трансформируются в троичные матрицы, элементы которых $\in \{0, 1, -\}$. Распознавание десятичных цифр каждого кода выполняется сравнением на множестве троичных эталонов по позициям сохраненных бит.

В результате матричной бинаризации десятичных цифр с последующим маскированием и рандомизацией каждый код трансформируется в k-секционный стегоконтейнер, который формируется следующим образом. Сначала создается т. н. пустой контейнер длиной $L = k\,(9n - 12)$ по числу бит бинарных эталонов десятичных цифр, выделенных на рис. 2. Он заполняется отрезком ПСП – ГАММОЙ. Затем в него внедряются по позициям биты кода, случайно сохраненные маскированием. Независимо от n среднее число таких бит $\ll L$, что характерно для стеганографии.

Сгенерированное множество масок является ключом распознавания. Он известен только санкционированному пользователю. Но алгоритм маскирования полагается известным широкому кругу. В данном случае S-модель определена на множестве наборов композиционных элементов <ЭТАЛОН><МАСКА>, компоненты которых суть бинарные матрицы размерами $m \times n$. Мощность любого набора равна мощности $\gamma = 10$ используемого алфавита символов.

Достаточное условие взаимной непокрываемости любой пары замаскированных троичных эталонов $\{X^t\}$, $t \in \{\overline{0,9}\}$, – различие хотя бы в одном значащем элементе x^t_{pq} троичных матриц X^{t1} и X^{t2}, $t1 \neq t2$. Элементы эталона X^t, не подлежащие маскированию, определены единичными компонентами инверсией матрицы масок $\overline{M}^t = |\overline{\mu}^t_{pq}|$ для этого эталона.

Структуризации данных картографических и текстовых сцен для их ассоциативной защиты имеют свои особенности. В обоих случаях исходное описание сцены задано в виде некоторой таблицы. Структуризация подразумевает представление этой таблицы в виде структуры данных, которые будут подвергаться в дальнейшем кодированию, бинаризации кодосимволов и их маскированию.

Случай картографических сцен. Кластеризуем исходное отношение в виде набора подтаблиц (кластеров). Для этого:

1. Случайным образом выберем некоторую строку исходной таблицы. Отметим эту строку. Позиционируем выделяемый кластер (определим его *глобальные координаты*). Саму же запись преобразуем к виду <Имя объекта><Локальные координаты объекта в данном кластере>.

2. Повторим шаг 1 на множестве неотмеченных строк. При этом всякий раз установим принадлежность вновь выделенной строки к одному из ранее введенных кластеров и преобразуем координаты (из исходных глобальных в локальные по кластеру). Если такового кластера не окажется, инициируем новый кластер. И так далее, пока не будут исчерпаны все записи исходной таблицы. *При этом мощности* (*числа записей*) *различных кластеров будут неодинаковы, а порядок следования кластеров случаен* (*не удовлетворяет критерию территориальной близости*).

Стратегию кластеризации поясним на конкретном примере (рис. 3). На этом рисунке Y и X – максимальные значения координат картографируемого массива (метры); ε – погрешность определения координат объектов (метры). Соответственно, шаг локальной координатной сетки равен 2ε.

Значение k должно удовлетворять условию равенства числа градаций в локальной и глобальной областях. Положив $X = Y = A$, получим линейный размер кластера (длину стороны квадрата) $C = 2\varepsilon\Gamma_{x,y}$. Необходимым условием представления координаты

объекта как КООРДИНАТА(x, y) = ГЛОБ. КООРД. + ЛОК. КООРД. является неравенство $A/\Gamma_{x,y} \le C$. Соответственно, $\Gamma_{x,y} \ge \sqrt{A/(2\varepsilon)}$. Пусть, например, $X = Y = 0.5 \cdot 10^6$ м, $\varepsilon = 1$ м. Тогда $\Gamma_{x,y} \ge 500$. Ближайшим будет выбор $\Gamma_{x,y} = 1000$ с $k = 3$. При этом глобальная координатная единица составит $A/\Gamma_{x,y} = 500$ м, а размер кластера $C = 2000$ м.

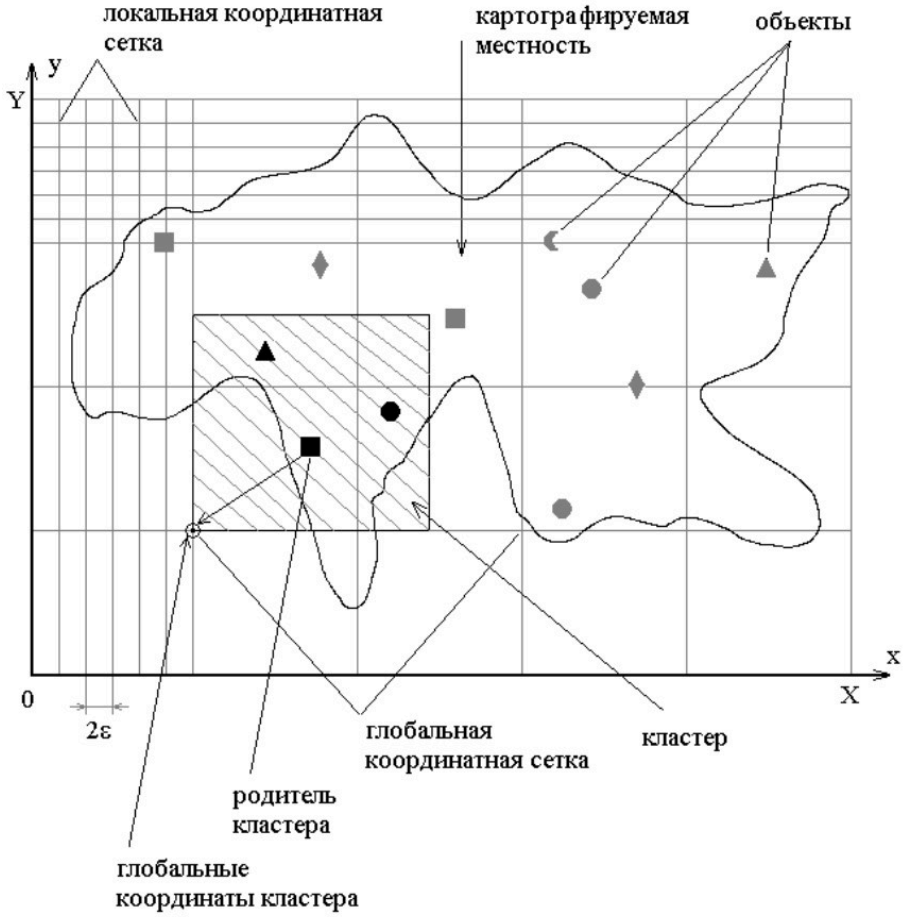

Рис. 3. Пример карты местности
Fig. 3. Sample terrain map

Отнесение некоторого объекта к тому или иному случайно формируемому кластеру определяет своеобразие реализации принципа *рассеивания* – первого основополагающего принципа защиты [30]. Реализация принципа *перемешивания* (второго основополагающего принципа защиты) достигается тем, что во избежание детерминированности расположения в кластере его «родителя» содержимое каждого кластера перемешивается.

Для заданной разрядности k кодового представления имен/координат и мощности полных множеств кодов объектов и градаций их координат имеем $\Gamma = 10^k$. Но обычно реальное число типов объектов и количество объектов (задействованных координат) на сцене $\Gamma_{obj\text{-}koord} < \Gamma$. Поэтому для выравнивания числа записей во всех кластерах, что необходимо для повышения стойкости защиты, целесообразно вводить «пустые» объекты и «пустые» координаты. Число типов тех и других $\delta_{obj\text{-}koord} = 10^k - \Gamma_{obj\text{-}koord}$. Коды конкретного «пустого» объекта и их координат должны выбираться случайно на множестве из $\delta_{obj\text{-}koord}$ вариантов.

Случай текстовых сцен. По условию любая текстовая характеристика объекта занимает одну машинописную страницу (один кластер). Формат записи в кластере:

[Код номера строки ($Local\_x$)],
[Код символа ($Symbol\_num$)],
[Код позиции в строке ($Local\_y$)].

При этом:

- Символы в поле $Symbol\_num$ [русский алфавит, английский алфавит, цифры, знаки препинания, специальные символы] кодируются трехзначными десятичными кодами согласно таблице символов ASCII (American Standard Code for Information Interchange) на множестве 000 ... 255 [31].
- Коды номеров строк и позиций в строке формируются случайным образом на множестве 000 ... 999 и хранятся после маскирования в специальной таблице базы данных.
- Нумерация строк в кластере – сверху вниз.
- Нумерация позиции символа в строке – слева направо.
- Число записей на всех страницах (фрагментах) выравнивается введением «пустых» записей, коды символов, номеров строк и позиций символов в которых выбираются случайным образом на множествах незадействованных кодов.
- Порядок следования записей в кластере *случаен*, чем достигается реализация эффектов «перемешивания» и «рассеивания».

2. Симбиоз стеганографии и криптографии

Система постулатов декларирует свойства S-модели. Она положена в основу развития теории и разработки конструктивного метода ассоциативной защиты объектов и координат при анализе сцен.

Постулат 1. *Генерируемый набор масок случаен. Число единиц инверсной матрицы масок для любого t-эталона, близкое к минимально возможному, определяется условием дихотомизации любой пары троичных эталонов в сгенерированном наборе по одному незамаскированному биту.*

Этому постулату удовлетворяет

Базовый алгоритм маскирования. Обозначим через D_ℓ множество бинарных эталонов символов $Э_t$, рассматриваемых на каждом этапе (уровне) работы алгоритма. По условию множество D_0 включает полный перечень типов эталонов.

1. $\ell := 0$.
2. Занумеровать случайную перестановку эталонов множества D_ℓ в натуральном порядке $Э_1, Э_2, \ldots, Э_\gamma$, образовав тем самым список $C_\ell = (Э_j),\ j = 1, 2, \ldots, \gamma$. Дополнить этот список пустым элементом $\mathcal{E}_{\gamma+1}$. Ни один элемент списка C_ℓ изначально не отмечен.

3. $i := 1$.

4. $j := i$, $k := 1$. Считать Θ_i первым элементом множества $D_{\ell+1}$.

5. Пока не встретится неотмеченный элемент списка C_ℓ:
$j := j + 1$. Если Θ_j не пуст, перейти к шагу 6. Иначе – к шагу 16.

6. $\Theta_i \oplus \Theta_j$ (побитно) $\to A_1$ (булева матрица).

7. Пока не встретится неотмеченный элемент списка C_ℓ:
$j := j + 1$. Если Θ_j не пуст, перейти к шагу 8. Иначе – к шагу 13.

8. $\Theta_i \oplus \Theta_j$ (побитно) $\to A_2$ (булева матрица).

9. $A_3 := A_1$.

10. $A_1 \,\&\, A_2$ (побитно) $\to A_1$. Если $A_1 \neq |0|$, перейти к шагу 7. Иначе – к шагу 11.

11. $k := k + 1$. Считать Θ_j k-м элементом множества $D_{\ell+1}$.

12. $A_1 := A_3$. Перейти к шагу 7.

13. Случайным образом выбрать один из единичных элементов матрицы A_1. Его координаты (p, q) определяют новый единичный элемент $\overline{\mu}_{pq}$ инверсной матрицы масок $\overline{M}$ для всех неотмеченных эталонов списка C_ℓ.

14. Отметить элементы списка C_ℓ, включенные во множество $D_{\ell+1}$.

15. $\ell := \ell + 1$, $D_\ell := D_{\ell+1}$, $\gamma := k$. Перейти к шагу 2.

16. Формирование инверсной маски для последнего неотмеченного элемента списка C_ℓ считать законченным. Отметить этот элемент, аннулировав тем самым список C_ℓ и множество $D_{\ell+1}$ (сделав их пустыми).

17. $\ell := \ell - 1$. Если $\ell \geq 0$, перейти к шагу 18. Иначе – к шагу 19.

18. Пока не встретится неотмеченный элемент списка C_ℓ:
$i := i + 1$. Перейти к шагу 4.

19. КОНЕЦ.

На рис. 4 (a, b) представлены случайные варианты маскирования для двух различных исходных перестановок десятичных цифр, полученные программным путем по этому алгоритму. Здесь $m = 5$, $n = 3$.

Под каждой цифрой приведена соответствующая инверсная матрица маски. Для полноты картины в табл. 1 даны примеры заполнения стегоконтейнеров в случае $n = k = 3$ для различных кодов. Битовая длина L стегоконтейнера $L = k \times (9 \times n - 12)$. Местоположения значимых бит при использовании масок на рис. 4 (a) показаны точками.

Утверждение 1. *Границы для максимального числа единиц* $(q_1)_{\max}$ *инверсных матриц масок* $\overline{M}^t$, *генерируемых алгоритмом, определены выражением*

$$\lceil \log_2 \gamma \rceil \leq (q_1)_{\max} \leq \gamma - 1.$$

a

0	***1***	***9***	***6***	***7***	***8***	***2***	***5***	***4***	***3***
100	100	100	100	100	100	000	000	100	100
000	000	001	000	000	000	000	000	000	001
010	000	000	000	001	010	000	000	001	000
100	000	010	100	010	100	110	110	010	010
010	010	010	010	010	010	010	010	010	010

b

3	***2***	***6***	***9***	***8***	***0***	***7***	***4***	***1***	***5***
000	000	010	000	000	000	000	000	000	010
100	000	001	100	001	001	000	001	001	001
001	000	000	001	010	010	001	010	010	000
000	010	010	000	010	010	000	010	010	010
001	001	001	001	011	101	001	011	101	001

Рис. 4. Варианты маскирования для двух различных исходных перестановок десятичных цифр при $m = 5$, $n = 3$

Fig. 4. Masking options for two different initial permutations of decimal digits at $m = 5$, $n = 3$

Табл. 1. Примеры заполнения стегоконтейнеров в случае $n = k = 3$

Table 1. Examples of stego container filling in the case of $n = k = 3$

Код	№ бита в контейнере																																												
	1–5					6–10					11–15					16–20					21–25					26–30					31–35					36–40					41–45				
153			.					.													.		.							.			.					.				.			.
472			.					.			.				.			.					.			.				.						.		.							.
708			.					.			.				.			.			.		.						.				.			.		.						.	
521						.		.							.						.		.							.			.			.		.						.	

Как показали многочисленные эксперименты, реально $1 \leq q_1 \leq 8$ при математическом ожидании $M_{q_1} = 5$. Средний объем вкраплений в контейнер равен kM_{q_1}. С ростом n при сохранении числа контейнеров суммарный объем вкраплений остается неизменным, а значение L увеличивается, что должно способствовать росту стегостойкости [32].

Теорема. *Для произвольной бинарной матрицы размером $m \times n$ проведение процедуры распознавания на множестве эталонов тех же размеров по маскам, сгенерированным с использованием построенного алгоритма, приведет к распознаванию в этой матрице одного и только одного эталона из указанного множества.*

Следствие. *Если при генерации наборов масок использован алгоритм, указанный выше, то для любой реализации множества рандомизированных объектов и любого вновь сгенерированного множества троичных образов X^t этих объектов каждый рандомизированный объект покрывается одним и только одним X^t.*

Это следствие легло в основу всех проведенных исследований.

Постулат 2. *При соответствующем выборе размеров матриц и генератора псевдослучайных последовательностей (ПСП) возможна реализация полноты покрытия, т. е. распознавания в каждом стегоконтейнере сообщения в целом полного множества*

кодов имен объектов и их координат, возможных для данной сцены, с первой случайной попытки формирования ГАММЫ при ограниченном переборе ключей.

Размеры $m \times n$ бинарных матриц представления десятичных кодовых цифр были определены условием, позволяющим надеяться на хорошую стегостойкость: объем битовых вкраплений не должен превышать 1 % объема носителя стегосообщения: $q = 5k < 0.01L = 0.01k(9n - 12)$. Отсюда имеем $n > \lceil 512/9 \rceil = 57$. Было принято $n = 60$. Соответственно, $m \times n = 119 \times 60$.

Утверждение 2. *При ограниченном переборе ключей и* $n = 60$ *полное покрытие с одной попытки на множествах стегоконтейнеров с вероятностью* 0.999 *обеспечивает выбор генератора ПСП «Вихрь Мерсенна»* [33] *для формирования «несущей» ГАММЫ стегоконтейнеров.*

Стегостойкость. Исследование стегостойкости проводилось с применением набора статистических тестов случайностей NIST [34–37]. Пакет NIST STS включает пятнадцать статистических тестов, которые разработаны для проверки гипотезы о случайности двоичных последовательностей произвольной длины, порождаемых генератором случайных чисел или генератором псевдослучайных чисел. Все тесты направлены на выявление различных дефектов случайности. Если ПСП успешно проходит проверку по всем тестам NIST, то она признается случайной («белой»). Если же имеется неуспех хотя бы на одном тесте, то она считается «черной».

В ходе эксперимента [28] был применен модифицированный алгоритм маскирования (см. раздел 3). За несущую ГАММУ был принят отрезок ПСП длиной 1 МБ, сформированный криптографической версией генератора ПСП «Вихрь Мерсенна» [38]. Было осуществлено $K = 100$ итераций по случайной генерации ГАММА-отрезка, проведению с этим отрезком $N = 1000$ опытов по стеговставкам на разных наборах масок и подсчету для каждой итерации вероятности $P = M/N$, где M – число стегоотрезков, прошедших тест NIST. Для полученной генеральной совокупности из значений этих вероятностей были подсчитаны математическое ожидание $\overline{P} = \dfrac{1}{K}\sum\limits_{i=1}^{K} P_i$ и среднеквадратичное отклонение $\sigma^P = \sqrt{\dfrac{1}{K-1}\sum\limits_{i=1}^{K}(P_i - \overline{P})^2}$. Полученные результаты приведены в табл. 2.

Табл. 2. Агрегированные результаты опытов
Table 2. Aggregated results of experiments

Генеральная совокупность	Статистическая оценка	
	Математическое ожидание	Среднеквадратичное отклонение
Вероятность получения «белого» стего при случайной генерации ГАММЫ с использованием модифицированного алгоритма	0.497	0.266

Была разработана 12-поточная программа генерации стегосообщения со случайным выбором ГАММЫ. С помощью этой программы на 12-ядерном сервере было проведено 1000 опытов для разных сообщений длиной 1800 символов с разными масками. Установлено, что при одновременном запуске двенадцати потоков вероятность того, что один из потоков генерирует стегосообщение, успешно проходящее тест NIST, равна 0.999.

Установив случайный характер принятой последовательности, аналитик может усомниться: а не замаскировано ли под случайность шифрованное сообщение? Тогда он прибегнет к криптоанализу.

Криптостойкость. В табл. 3 приведена найденная вычислительным экспериментом верхняя оценка числа различных ключей, генерируемых базовым алгоритмом при различных размерах эталонов. Если время получения и анализа результата применения одного ключа равно 1 мкс, то полный перебор ключей при $n = 60$ займет 10^{23} секунд, т. е. 3×10^{15} лет.

Табл. 3. Оценка числа ключей
Table 3. Key estimates

n	18	30	40	60
Число ключей	10^{23}	10^{25}	10^{27}	10^{29}

Постулат 2 отдает дань криптографическому аспекту ассоциативной защиты. Если число всевозможных кодов объектов/координат анализируемой сцены равно T/Γ и на ней сосредоточено N объектов, то в результате ограниченного перебора код каждого из N объектов может быть любым из T возможных, а коды координат – любыми из Γ возможных. В данном случае $T = \Gamma = 10^k$.

В плане криптоанализа были рассмотрены следующие виды криптоатак [39]: путем полного перебора ключей, на ГАММУ, со знанием открытого текста, отсутствия объекта, ассоциации с картой местности. Итогом явилось:

Утверждение 3. *Ассоциативная защита данных доказуемо стойкая ко всем видам рассмотренных криптоатак.*

Под доказуемой криптостойкостью понимается чрезмерная вычислительная сложность (а потому и неприемлемое время) нахождения истинного ключа.

В отношении атаки перебором ключей был принят

Постулат 3. *Велика вероятность того, что проявление последовательностей сущностей, кодируемых элементами распознаваемой сцены при ограниченном по времени случайном переборе ключей, выделит среди них сообщение, правдоподобное по критерию соответствия характеру сцены, но ошибочное.*

На рис. 5 (а) показано изображение тематического слоя тестовой карты, полученное средствами ГИС MapInfo [40] после ассоциативного сокрытия его данных и последующего дешифрования на истинном ключе. Это участок местности 300×300 км^2 республики Чувашия, который содержит 1035 точечных объектов четырех разных типов. Их условные обозначения показаны на рис. 6. На рис. 5 (б, в) представлены изображения того же слоя, полученные на двух ложных ключах.

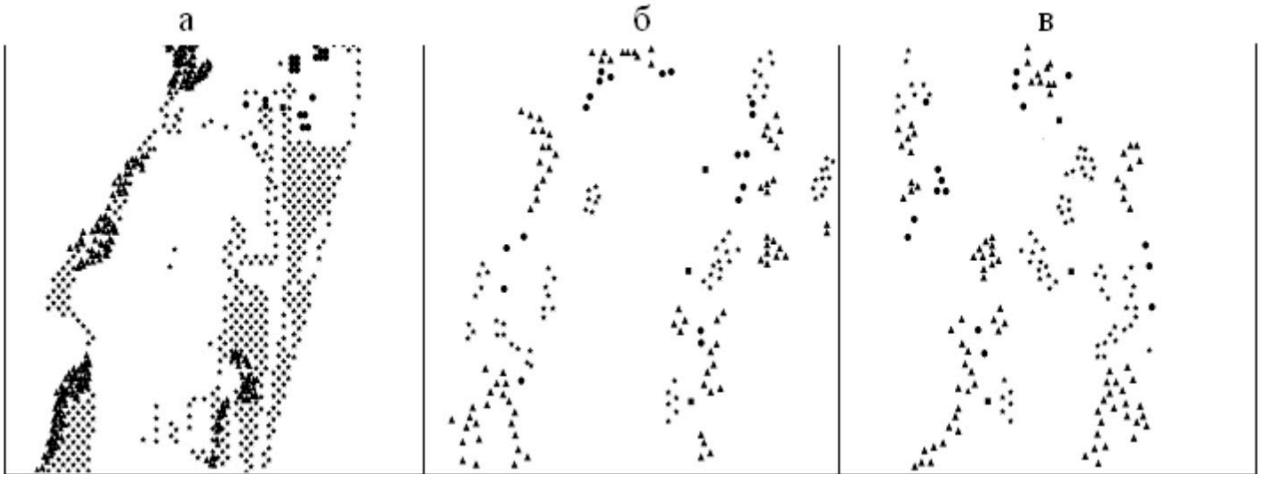

Рис. 5. Изображения тематического слоя карты, полученные после дешифрования на правильном (а) и двух ложных ключах (б, в)
Fig. 5. Images of the thematic map layer obtained after the decryption with the correct key (a) and two false keys (b, c)

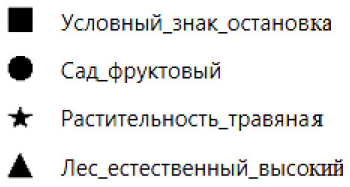

Рис. 6. Использованные условные обозначения объектов
Fig. 6. Symbols of mapped objects

При наличии некоторых знаний о характере местности одно из них может быть ошибочно принято за истинное. Если в процессе перебора, допустимого по времени, мы случайно «наткнемся» на правильный ключ, то он даст наиболее правдоподобную картину и без сомнения будет взят за искомое решение. Но вероятность такого события исчезающе мала. Зато велика вероятность получения правдоподобной, но неверной картины, которая может ввести в заблуждение.

3. Повышение помехоустойчивости

Независимо от n, наиболее часто используемыми в качестве существенных при формировании набора масок оказались укрупненные узловые точки совокупного контура всех эталонов, показанные на рис. 2. Статистическим моделированием установлено, что примерно для 61 % ключей из их полного множества биты по выделенным четырем позициям используются в качестве существенных. Поэтому велика вероятность искажения хотя бы одного из них под влиянием сетевых помех. Более равномерная функция распределения получится, если при формировании набора инверсных матриц масок запретить использование выявленных узловых битов в качестве существенных. В этом и состоит суть проведенной модификации алгоритма.

Введение избыточного маскирования. Предложено генерировать $Q \in \{3, 5, 7, \ldots\}$ наборов масок, дизъюнктивно объединяемых при погружении в стегоконтейнеры [41].

Распознавание принимаемого стегосообщения проводим по всем наборам масок. Для i-стегосимвола за результат распознавания берем эталон, число распознаваний которого $r_i \geq (Q+1)/2$. Если это условие не выполняется, то фиксируем факт возможного искажения символа (отказ от распознавания).

Действие случайных помех. Вычислительный эксперимент при $Q = 5$ показал допустимость искажения до шести бит в любом из шестнадцати байт каждого контейнера: ряд 1 на рис. 7 отвечает числу правильных распознаваний, ряд 2 – неправильных, ряд 3 – отказ от распознавания.

Рис. 7. Результаты эксперимента при $Q = 5$
Fig. 7. Experimental results at $Q = 5$

При $k = 3$, $n = 60$ допускается искажение до 6 % бит в каждом контейнере длиной 1584 бит. Для сравнения: шифры ГОСТ и AES допускают искажение лишь одного бита в 128-битном блоке (< 1 % данных) с возможностью установления факта (без исправления) такой ошибки. Поэтому при их использовании требуется дополнительное помехоустойчивое кодирование.

Преднамеренная помеха внедряется путем сложения по mod 2 одной из $\overline{M}^t$ с каждой секцией контейнера. При действии такой помехи избыточность на уровне ключей дает 100 % правильных распознаваний уже при $Q = 3$. Но противник может использовать аналогичную избыточность для генерации помех. Установлена принципиальная возможность успешного противодействия влиянию такой помехи при выборе избыточности в процессе шифрования $Q \in \{5, 7\}$.

Влияние избыточного маскирования на стего- и криптостойкость. В случае избыточного маскирования при $Q = 5$ результат тестирования, аналогичного описанному в разделе 2, почти всегда оказывался «черным» [42]. Поэтому программа была модифицирована на случай использования вычислительного кластера из шести 12-ядерных рабочих узлов и одного управляющего узла. При одновременном запуске семидесяти двух потоков вероятность генерации «белого» стегосообщения с $Q = 5$ одним из потоков оказалась равной 1. В случае избыточного маскирования с таким Q сохранялось и свойство доказуемой криптостойкости.

4. Снижение объемов передач

Размеры носителя были определены ранее с позиций стегозащиты условием, что объем битовых вкраплений не должен превышать 1 % объема носителя, что характерно для стеганографии. Соответственно, описанные исследования были проведены при размерах бинарных матриц-эталонов кодовых символов $m \times n = 119 \times 60$. При числе объектов сцены N объем сообщения с ассоциативной защитой V_{stego} (в битах) равен $V_{stego} = 3NL = 3Nk(9n - 12)$. Если не предъявлять жестких требований к помехоустойчивости при передаче зашифрованных сообщений по открытым каналам связи, то вполне приемлемыми для анализа сцен можно считать криптошифры ГОСТ и AES.

При использовании ГОСТ 34.12-2018 и AES-256 в 128-битном блоке размещают двенадцать кодов (десять битов отводят для хранения одного трехразрядного десятичного кода, остальные восемь бит блока заполняют псевдослучайными значениями). Соответственно, $V_{crypto} = 3N128/12 = 32N$, $V_{stego} = (3k(9n - 12)/32)V_{crypto}$. В случае $k = 3$, $n = 60$ получили $V_{stego} = 148.5 \cdot V_{crypto}$. Выбор $n = 30$ снижает объем передач примерно в два раза. Теперь для $k = 3$ имеем $V_{stego} = 72.56 \cdot V_{crypto}$. Значение $n = 30$ обеспечивает удовлетворение критерия полноты покрытия при небольшом переборе, высокую помехоустойчивость и доказуемую криптостойкость в случае избыточного маскирования [29].

Для оценки вероятности $P(T) = 10^{-3} \sum_{i=1}^{10^3} B_i$ генерации одним из T параллельно запущенных потоков «белого» стегосообщения при $n = 30$ ($B_i = 1$, если тест NIST успешно пройден в i-м опыте, иначе $B_i = 0$) была использована многопоточная программа генерации стегосообщения на кластерной платформе, упомянутая в разделе 3. Было получено $P(48) = 1$ для безызбыточного маскирования и $P(84) = 1$ (дополнительно были использованы двенадцать ядер управляющего узла) в случае избыточного при $Q = 5$.

5. Перспектива продолжения исследований

Эту перспективу мы связываем с изменением конфигураций цифровых эталонов при некотором расширении множества возможных единичных элементов матриц, как показано на рис. 8. Их целесообразно разместить не только по внешнему контуру и внутреннему «зигзагу» бинарных матриц, но и по двум дополнительным обратным диагоналям.

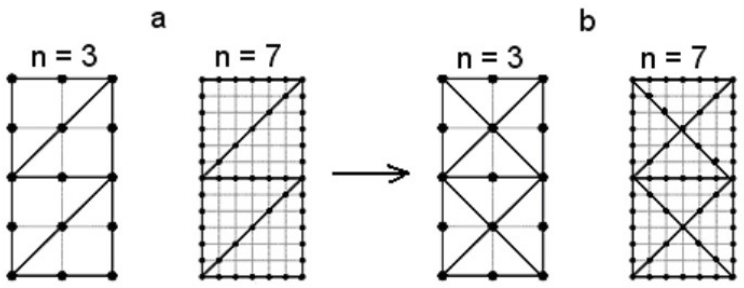

Рис. 8. Возможное размещение единиц на множестве $\{\overline{0,9}\}$ матриц-эталонов мощностью $\gamma = 10$: a) ранее использованное, b) вновь предлагаемое

Fig. 8. Possible placement of ones on the set $\{\overline{0,9}\}$ of the etalon matrices with power $\gamma = 10$: a) previously used, b) newly proposed

При использовании десятичного кодирования минимизация числа вкраплений в ГАММА-контейнер достигается, если удается провести последовательность разбиений множества эталонов на группы: $10 \to 4+6$; $4 \to 2+2$; $6 \to 2+4$; $4 \to 2+2$. В итоге получаем шесть эталонов с тремя вкраплениями и четыре эталона с четырьмя вкраплениями, в среднем – три или четыре вкрапления на один эталон. При $n = 3$ имеем всего пять возможностей первого разбиения $10 \to 4+6$ (последующие разбиения вариативны) для ранее использованного представления десятичных цифр. Они показаны на рис. 9. Позиции битов, сохраняемых при маскировании, отмечены символом $\otimes$. В общем случае число возможностей возрастает до $5\,(n-2)$. Как следует из рис. 10, на множестве вновь введенных эталонов имеем шесть возможных первых разбиений $10 \to 4+6$ против пяти в предыдущем варианте.

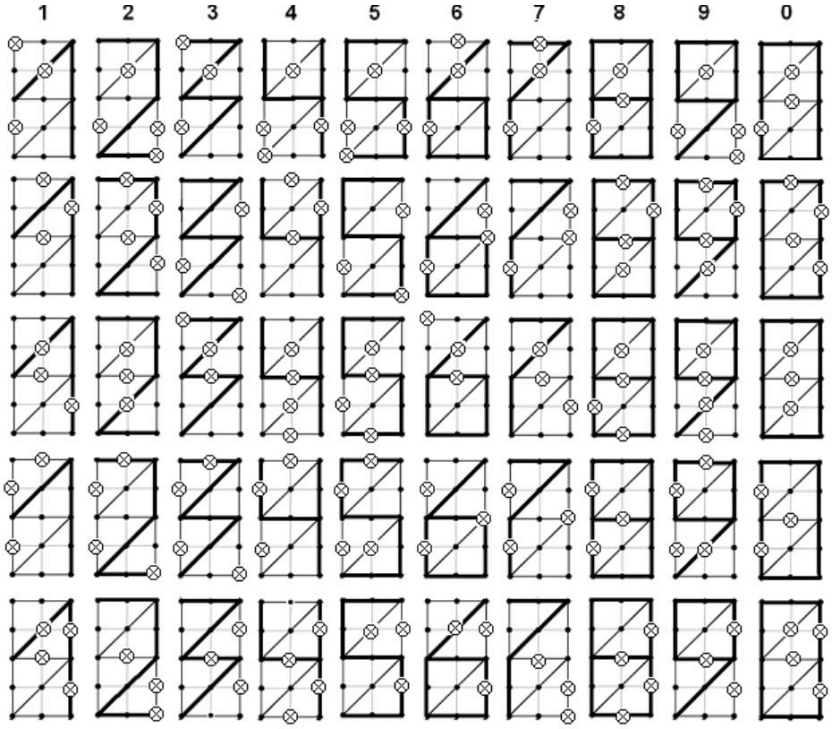

Рис. 9. По одному варианту маскирования при $n = 3$ для каждого из пяти возможных первых разбиений $10 \to 4+6$ для почтового множества $\{\overline{0,9}\}$
Fig. 9. One masking variant at $n = 3$ for each of the five possible first partitions $10 \to 4+6$ for the set of postal symbols $\{\overline{0,9}\}$

Выдвигаем следующую гипотезу:

Гипотеза. *Математическое ожидание M_{q_1} числа вкраплений в любой эталон на множестве объектов сцены снижается, если изменение конфигураций десятичных эталонов влечет рост числа возможностей первого разбиения* $10 \to 4+6$.

Длина контейнера при использовании предлагаемого расширения увеличится до $L = k\,(11n-18)$, что при $k = 3$ и $n = 30$ дает рост на 20 %. Поэтому, если новые исследования подтвердят справедливость нашей гипотезы, то значение $L/(kM_{q_1})$ при таком переходе должно зна́чимо вырасти. То же самое – с числом ключей. Соответственно, стойкость должна существенно повыситься. Вопросы помехоустойчивости, связанные с из-

менением конфигураций эталонов, требуют дополнительного исследования. Полезно будет расширить и число рассматриваемых атак.

Особый интерес вызывает переход к шестнадцатой системе с вариациями конфигураций цифровых эталонов согласно рис. 8 (b). Если мощность γ множества эталонов – степень двойки, то минимизация числа вкраплений в ГАММА-контейнер будет достигнута последовательным делением этого множества и образуемых подмножеств пополам. Тогда число вкраплений в любой эталон окажется равным $\log_2 \gamma$. Случай $\gamma = 16$ иллюстрирует рис. 11.

Максимальное число имен при $k = 3$ равно теперь $16^3 = 4096$ против $10^3 = 1000$ для десятичного кодирования. Это должно способствовать существенному росту стойкости защиты при анализе картографических сцен, если требование полноты покрытия выполнено. Тот факт, что минимальное среднее число вкраплений в эталон на множестве $\{\overline{0, 15}\}$ равно 4 против 3.4 для десятичного кодирования, не должен играть существенной роли.

В случае текстовых сцен переход к этому множеству при допустимом снижении разрядности до $k = 2$ будет способствовать повышению компактности текстовых сообщений с ассоциативной защитой. Но здесь могут возникнуть сомнения в получении приемлемой стойкости, т. к. число возможных представлений любого символа в процессе перебора ключей при полноте покрытия снизится до 256. Потребуется дополнительное исследование, чтобы преодолеть это сомнение.

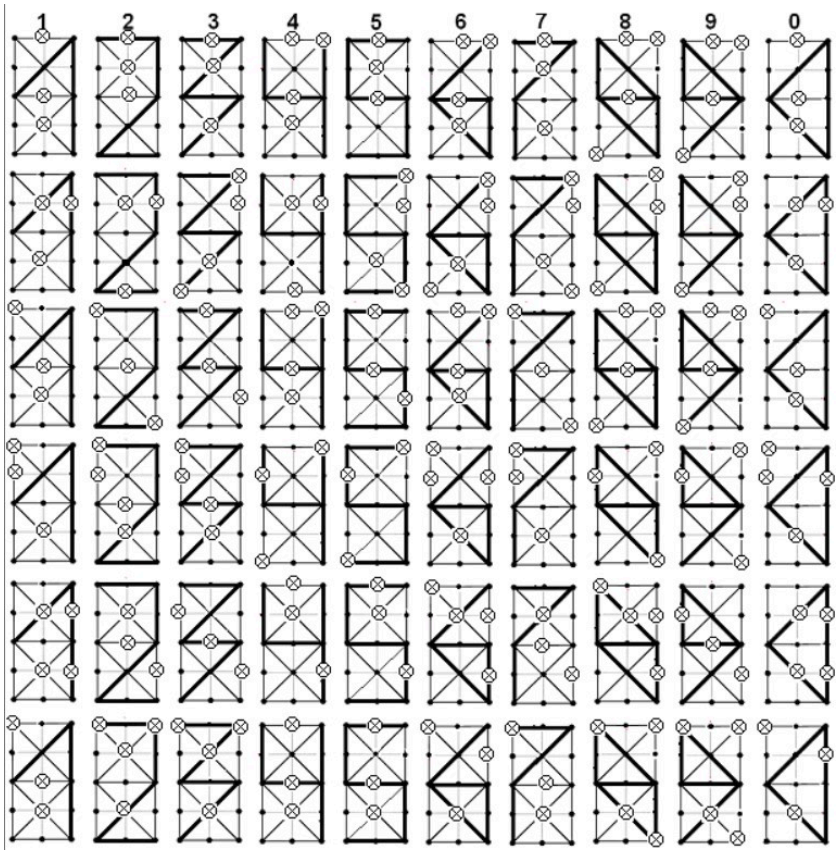

Рис. 10. По одному варианту маскирования при $n = 3$ для каждого из шести возможных первых разбиений $10 \to 4 + 6$ на множестве вновь введенных эталонов

Fig. 10. One masking variant at $n = 3$ for each of the six possible first partitions $10 \to 4 + 6$ on the set of newly introduced etalons

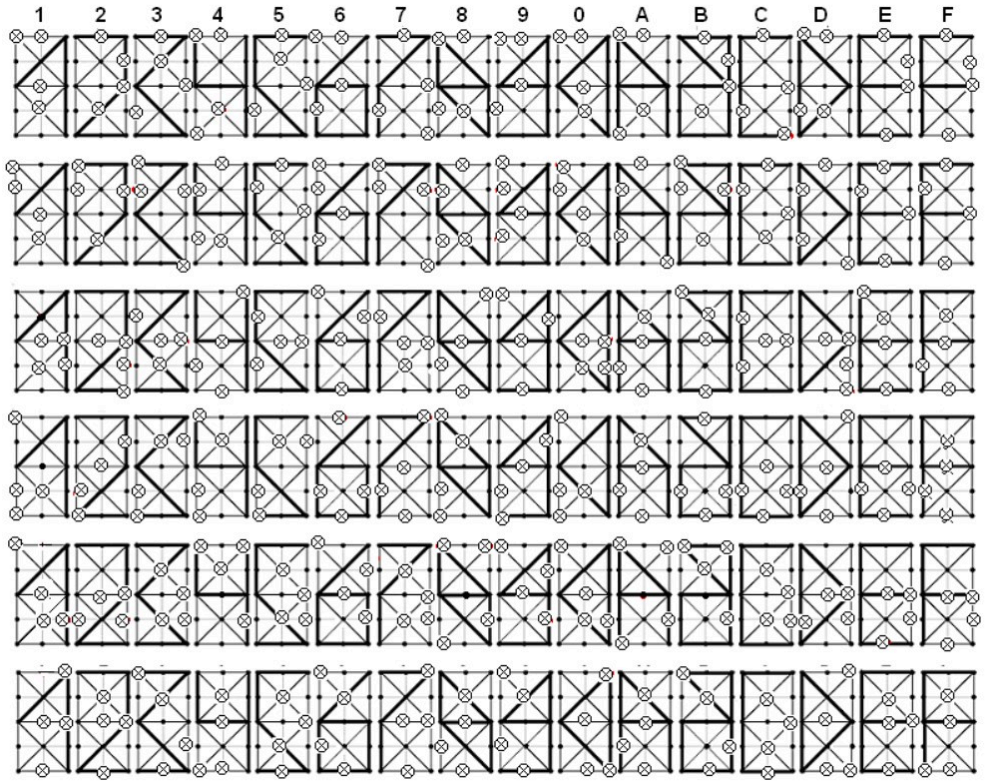

Рис. 11. По одному варианту экономного маскирования при $n = 3$ для каждого из шести возможных первых разбиений $16 \to 8 + 8$ на множестве $\{\overline{0, 15}\}$ вновь введенных эталонов
Fig. 11. One variant of effective masking at $n = 3$ for each of the six possible first partitions $16 \to 8{+}8$ on the set $\{\overline{0, 15}\}$ of newly introduced etalons

Заключение

Систематизированы главные особенности теории ассоциативной защиты информации. Рассмотрены возможности ее применения к защите данных картографических сцен и текстов. Взаимодополняющий симбиоз стеганографии и криптографии – главный научный результат проведенного исследования. С использованием развитых элементов названной теории были разработаны картографическая и текстовая СУБД с такой защитой [43–45]. Авторы видят значительные перспективы дальнейшего развития теории и практики ассоциативной защиты.

Есть один серьезный момент, который ставит под сомнение практическую достижимость в нашем случае безусловной стегостойкости. Противник едва ли поверит передаче по внешней сети адресованной случайной последовательности. Но выход имеется. Можно скрыть моменты начала передач между сервером и множеством клиентов, организовав непрерывное следование по внешней сети потока ПСП со вставкой в него стегосообщений в случайные моменты времени. Проблема представляется разрешимой в случае использования специализированной локальной сети между сотрудниками одной организации.

При этом формировать «белое» стего не нужно. Вероятности получения «белой» ГАММЫ и «белого» стего без предварительной выборки различаются всего на 10 % [43]. И если передачи «пустых» и стего контейнеров считать равновероятными, то с малой погрешностью получим равенство априорных и апостериорных вероятностей передач «черных»

и «белых» ГАММ и таких же стего. Иными словами, в этом случае критерий совершенной секретности по К. Шеннону [46] удовлетворяется в достаточной мере.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Conflicts of Interest. The authors declare no conflicts of interest.

Литература

1. *Анохин П.К.* Идеи и факты в разработке теории функциональных систем // Психол. журн. 1984. Т. 5, № 2. С. 107–118.
URL: https://spkurdyumov.ru/evolutionism/idei-i-fakty-v-razrabotke-teorii-funkcionalnyx-sistem.

2. *Райхлин В.А., Медведев А.С., Мотягин В.Г.* Вопросы разработки матричных компиляторов // Вычисл. сист. 1981. № 89. С. 69–83.

3. *Райхлин В.А.* Операционные логико-запоминающие среды. Вопросы применения и синтеза // Автомат. и телемех. 1983. № 11. С. 161–171.

4. *Райхлин В.А., Медведев А.С., Мотягин В.Г., Ильин А.В., Шварцман М.И.* К исследованию эффективности комплектования универсальных ЭВМ средней производительности матричными процессорами ассоциативного типа // Управляющ. сист. и машины. 1985. № 3. С. 23–28.

5. *Райхлин В.А* Об использовании аппарата двумерного ассоциативного поиска в процессе распознавания. Казань: КАИ, 1991. С. 38–54.

6. *Райхлин В.А* Анализ производительности процессорных матриц при распознавании двоичных образов // Автометрия. 1996. № 5. С. 97–103.

7. *Duda R.O., Hart P.E.* Pattern Classification and Scene Analysis. New York, NY: Wiley-Intersci. Publ., 1973. xvii, 482 p.

8. *Райхлин В.А.* Конструктивное моделирование систем. Казань: Фэн, 2005. 303 с.

9. *Дружинин В.В., Конторов Д.С.* Проблемы системологии (проблемы теории сложных систем). М.: Сов. радио, 1976. 296 с.

10. *Тейз А., Грибомон П., Юлен Г. и др.* Логический подход к искусственному интеллекту: от модальной логики к логике баз данных. М.: Мир, 1998. 494 с.

11. *Абазина Е.С., Ерунов А.А.* Цифровая стеганография: состояние и перспективы // Сист. упр., связи и безопасн. 2016. № 2. С. 182–201.

12. *Дрюченко М.А., Сирота А.А.* Блочный алгоритм стеганографического скрытия информации в видео на основе универсальных сжимающих преобразований // DSPA: Вопр. примен. цифр. обраб. сигн. 2017. Т. 7, № 3. С. 78–82.

13. *Коржик В.И., Федянин И.А., Копылова О.Д.* Синтез высокоскоростных стегоалгоритмов, устойчивых к «слепому» стегоанализу // ВЗИ. 2014. № 2. С. 51–56.

14. *Сирота А.А., Дрюченко М.А., Митрофанова Е.Ю.* Нейросетевые алгоритмы создания цифровых водяных знаков на основе гетероассоциативных сжимающих преобразований // Киберн. и высок. технол. XXI в. 2014. С. 68–78.

15. *Шелухин О.И., Олейникова Т.В.* Оценка эффективности стеганографического скрытия цифровых водяных знаков в видеопоследовательностях за счет дифференциальной разности энергий областей изображения // Наукоемк. технол. в космич. исслед. земли. 2016. № 2. С. 70–76.

16. *Wang Z., Zhang X.* Secure cover selection for steganography // IEEE Access. 2019. V. 7. P. 57857–57867. https://doi.org/10.1109/ACCESS.2019.2914226.

17. *Cachin C.* An information-theoretic model for steganography // Inf. Comput. 2004. V. 192, No 1. P. 41–56. https://doi.org/10.1016/j.ic.2004.02.003.

18. *ГОСТ 28147-89.* Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Госстандарт СССР, 1989.

19. *ГОСТ 34.12-2018.* Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2018.

20. *Advanced Encryption Standard (AES).* Ser.: Federal Information Processing Standards Publication. FIPS 197. Upd. 1. Gaithersburg, MD: Natl. Inst. Stand. Technol., 2023. vii, 38 p. https://doi.org/10.6028/NIST.FIPS.197-upd1.

21. *Coutinho S.C.* The Mathematics of Ciphers: Number Theory and RSA Cryptography. New York, NY: AK Peters/CRC Press, 1999. 198 p. https://doi.org/10.1201/9781439863893.

22. *Иванов М.А., Матвейчиков И.В., Скитев А.А., Стрельченко П.А.* Способ сокрытия информации в последовательности псевдослучайных чисел // REDS: Телекоммун. устр. и сист. 2016. Т. 6, № 3. С. 355–359.

23. *Вильховский Д.Э.* Обзор методов стеганографического анализа изображений в работах зарубежных авторов // Матем. структ. и моделир. 2020. № 4 (56). С. 75–102.

24. *Сирота Д.А., Дрюченко М.А., Иванков А.Ю.* Стегоанализ цифровых изображений с использованием методов поверхностного и глубокого машинного обучения: известные подходы и новые решения // Вестн. ВГУ. Сер.: Сист. анализ и информ. технол. 2021. № 1. С. 33–52.

25. *Raikhlin V.A., Vershinin I.S., Gibadullin R.F., Pystogov S.V.* Reliable recognition of masked binary matrices. Connection to information security in map systems // Lobachevskii J. Math. 2013. V. 34, No 4. P. 319–325. https://doi.org/10.1134/S1995080213040112.

26. *Raikhlin V.A., Vershinin I.S., Gibadullin R.F.* The elements of associative steganography theory // Moscow Univ. Comput. Math. Cybern. 2019. V. 43, No 1. P. 40–46. https://doi.org/10.3103/S0278641919010072.

27. *Vershinin I.S., Gibadullin R.F., Pystogov S.V., Raikhlin V.A.* Associative steganography. Durability of associative protection of information // Lobachevskii J. Math. 2020. V. 41, No 3. P. 440–450. https://doi.org/10.1134/S1995080220030191.

28. *Vershinin I.S., Gibadullin R.F., Pystogov S.V., Raikhlin V.A.* Associative steganography of text messages // Moscow Univ. Comput. Math. Cybern. 2021. V. 45, No 1. P. 1–11. https://doi.org/10.3103/S0278641921010076.

29. *Raikhlin V.A., Gibadullin R.F., Vershinin I.S.* Is it possible to reduce the sizes of stegomessages in associative steganography? // Lobachevskii J. Math. 2022. V. 43, No 2. P. 455–462. https://doi.org/10.1134/S1995080222050201.

30. *Schneier B.* Cryptographic design vulnerabilities // IEEE Comput. 1998. V. 31, No 9. P. 29–33.

31. *Shinge S.R., Patil R.* An encryption algorithm based on ASCII value of data // Int. J. Comput. Sci. Inf. Technol. 2014. V. 5, No 6. P. 7232–7234.

32. *Ker D.A.* A capacity result for batch steganography // IEEE Signal Process. Lett. 2007. V. 14, No 8. P. 525–528. https://doi.org/10.1109/LSP.2006.891319.

33. *Matsumoto M., Nishimura T.* Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator // ACM Trans. Model. Computer Simul. (TOMACS). 1998. V. 8, No 1. P. 3–30. https://doi.org/10.1145/272991.272995.

34. *Hegadi R., Patil A.P.* A statistical analysis on in-built pseudo random number generators using NIST test suite // Proc. 2020 5th Int. Conf. on Computing, Communication and Security (ICCCS). Patna: IEEE, 2020. P. 1–6. https://doi.org/10.1109/ICCCS49678.2020.9276849.

35. *Maurer U.M.* A universal statistical test for random bit generators // J. Cryptol. 1992. V. 5, No 2. P. 89–105. https://doi.org/10.1007/BF00193563.

36. *Sadique Uz Zaman J.K.M., Ghosh R.* Review on fifteen statistical tests proposed by NIST // J. Theor. Phys. Cryptogr. 2012. V. 1. P. 18–31.

37. *Gyarmati K.* On a pseudorandom property of binary sequences // Ramanujan J. 2004. V. 8, No 3. P. 289–302. https://doi.org/10.1007/s11139-004-0139-z.

38. *Matsumoto M., Saito M., Nishimura T., Hagita M.* CryptMT stream cipher version 3 // eSTREAM, ECRYPT Stream Cipher Project, Report. V. 28. 2007.

39. *Вершинин И.С.* Стойкость ассоциативной защиты распределенных объектов картографии // Нелин. мир. 2011. Т. 9, № 12. С. 822–825.

40. *Probert T.* MapInfo Professional v10. 5 // GeoInformatics. 2010. V. 13, No 6. P. 62.

41. *Вершинин И.С.* Уточнение критерия избыточности помехоустойчивого сокрытия информации в рамках ассоциативной стеганографии // Информ. и безопасн. 2016. Т. 19, № 4. С. 511–514.

42. *Гибадуллин Р.Ф., Вершинин И.С., Райхлин В.А.* Стегостойкость и вычислительная стойкость ассоциативной стеганографии // Мет. моделир.-VII. 2019. С. 23–38.

43. *Райхлин В.А., Вершинин И.С., Классен Р.К., Гибадуллин Р.Ф., Пыстогов С.В.* Конструктивное моделирование процессов синтеза. Казань: Фэн, 2020. 248 с.

44. *Вершинин И.С., Гибадуллин Р.Ф., Пыстогов С.В.* Программа управления ассоциативно защищенными картографическими базами данных «Security Map Cluster». Свидетельство о государственной регистрации программы для ЭВМ № 2016611421. Россия, 2016.

45. *Вершинин И.С., Гибадуллин Р.Ф.* Программа ассоциативной защиты файлов «Stego». Свидетельство о государственной регистрации программы для ЭВМ № 2021613638. Россия, 2021.

46. *Shannon C.E.* Communication theory of secrecy systems // Bell Syst. Tech. J. 1949. V. 28, No 4. P. 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.

References

1. Anokhin P.K. Ideas and facts in the development of the theory of functional systems. *Psikhol. Zh.*, 1984, vol. 5, no. 2, pp. 107–118.
   URL: https://spkurdyumov.ru/evolutionism/idei-i-fakty-v-razrabotke-teorii-funkcionalnyx-sistem.

2. Raikhlin V.A., Medvedev A.S., Motyagin V.G. Problems in the development of matrix compilers. *Vychisl. Sist.*, 1981, no. 89, pp. 69–83. (In Russian)

3. Raikhlin V.A. Operating logical and storing arrays. Application and design. *Avtom. Telemekh.*, 1983, no. 11, pp. 161–171. (In Russian)

4. Raikhlin V.A., Medvedev A.S., Motyagin V.G., Il'in A.V., Schwartzman M.I. On the study of the efficiency of equipping midrange universal computers with associatve matrix processors. *Upr. Sist. Mash.*, 1985, no. 3, pp. 23–28. (In Russian)

5. Raikhlin V.A. *Ob ispol'zovanii apparata dvumernogo assotsiativnogo poiska v protsesse raspoznavaniya* [On the Use of a Two-Dimensional Associative Search Apparatus in the Recognition Process]. Kazan, KAI, 1991, pp. 38–54. (In Russian)

6. Raikhlin V.A. Analysis of the performance of processor matrices in binary pattern recognition. *Avtometriya*, 1996, no. 5, pp. 97–103. (In Russian)

7. Duda R.O., Hart P.E. *Pattern Classification and Scene Analysis*. New York, NY, Wiley-Intersci. Publ., 1973. xvii, 482 p.

8. Raikhlin V.A. *Konstruktivnoe modelirovanie sistem* [Constructive Modeling of Systems]. Kazan, Fen, 2005. 303 p. (In Russian)

9. Druzhinin V.V., Kontorov D.S. *Problemy sistemologii (problemy teorii slozhnykh sistem)* [Problems of Systems Science (Problems of the Theory of Complex Systems)]. Moscow, Sov. Radio, 1976. 296 p. (In Russian)

10. Thayse A., Gribomont P., Hulin G., et al. *Logicheskii podkhod k iskusstvennomu intellektu: ot modal'noi logiki k logike baz dannykh* [A Logic Based Approach to Artificial Intelligence: From Modal Logic to Deductive Databases]. Moscow, Mir, 1998. 494 p. (In Russian)

11. Abazina E.S., Yerunov A.A. Digital steganography: Status and development outlook. *Sist. Upr., Svyazi Bezop.*, 2016, no. 2, pp. 182–201. (In Russian)

12. Dryuchenko M.A., Sirota A.A. Block video steganography algorithm based on universal compressing transformations. *DSPA: Vopr. Primen. Tsifrovoi Obrab. Signalov*, 2017, vol. 7, no. 3, pp. 78–82. (In Russian)

13. Korzhik V.I., Fedyanin I.A., Kopylova O.D. Synthesis of high-speed steganographic algorithms resistant to blind steganalysis. *VZI*, 2014, no. 2, pp. 51–56. (In Russian)

14. Sirota A.A., Dryuchenko M.A., Mitrofanova E.Yu. Neural network algorithms for creating digital watermarks based on heteroassociative compressive transformations. In: *Kibernetika i vysokie tekhnologii XXI veka* [Cybernetics and High Technology of the 21st Century], 2014, pp. 68–78. (In Russian)

15. Sheluhin O.I., Oleynikova T.V. Evaluating the effectiveness of hiding digital watermark in video sequences due to the energy difference between the discrete cosine transform coefficients. *H&ES Res.*, 2016, no. 2, pp. 70–76. (In Russian)

16. Wang Z., Zhang X. Secure cover selection for steganography. *IEEE Access*, 2019, vol. 7, pp. 57857–57867. https://doi.org/10.1109/ACCESS.2019.2914226.

17. Cachin C. An information-theoretic model for steganography. *Inf. Comput.*, 2004, vol. 192, no. 1, pp. 41–56. https://doi.org/10.1016/j.ic.2004.02.003.

18. State Standard 28147-89. Information processing systems. Cryptographic protection. Cryptographic transformation algorithm. Moscow, Gosstandart SSSR, 1989. (In Russian)

19. State Standard 34.12-2018. Information technology. Cryptographic data security. Block ciphers. Moscow, Standartinform, 2018. (In Russian)

20. Advanced Encryption Standard (AES). Ser.: Federal Information Processing Standards Publication. FIPS 197. Upd. 1. Gaithersburg, MD, Natl. Inst. Stand. Technol., 2023. vii, 38 p. https://doi.org/10.6028/NIST.FIPS.197-upd1.

21. Coutinho S.C. *The Mathematics of Ciphers: Number Theory and RSA Cryptography*. New York, NY, AK Peters/CRC Press, 1999. 198 p. https://doi.org/10.1201/9781439863893.

22. Ivanov M.A., Matveichikov I.V., Skitev A.A., Strel'chenko P.A. Hiding information in pseudorandom number sequences. *REDS: Telekommun. Ustroistva Sist.*, 2016, vol. 6, no. 3, pp. 355–359. (In Russian)

23. Vil'khovskii D.E. A review of image steganalysis methods in foreign publications. *Mat. Strukt. Model.*, 2020, no. 4 (56), pp. 75–102. (In Russian)

24. Sirota A.A., Dryuchenko M.A., Ivankov A. Steganalysis of digital images by means of shallow and deep machine learning: Existing approaches and new solutions. *Proc. Voronezh State Univ. Ser.: Syst. Anal. Inf. Technol.*, 2021, no. 1, pp. 33–52. (In Russian)

25. Raikhlin V.A., Vershinin I.S., Gibadullin R.F., Pystogov S.V. Reliable recognition of masked binary matrices. Connection to information security in map systems. *Lobachevskii J. Math.*, 2013, vol. 34, no. 4, pp. 319–325. https://doi.org/10.1134/S1995080213040112.

26. Raikhlin V.A., Vershinin I.S., Gibadullin R.F. The elements of associative steganography theory. *Moscow Univ. Comput. Math. Cybern.*, 2019, vol. 43, no. 1, pp. 40–46. https://doi.org/10.3103/S0278641919010072.

27. Vershinin I.S., Gibadullin R.F., Pystogov S.V., Raikhlin V.A. Associative steganography. Durability of associative protection of information. *Lobachevskii J. Math.*, 2020, vol. 41, no. 3, pp. 440–450. https://doi.org/10.1134/S1995080220030191.

28. Vershinin I.S., Gibadullin R.F., Pystogov S.V., Raikhlin V.A. Associative steganography of text messages. *Moscow Univ. Comput. Math. Cybern.*, 2021, vol. 45, no. 1, pp. 1–11. https://doi.org/10.3103/S0278641921010076.

29. Raikhlin V.A., Gibadullin R.F., Vershinin I.S. Is it possible to reduce the sizes of stegomessages in associative steganography? *Lobachevskii J. Math.*, 2022, vol. 43, no. 2, pp. 455–462. https://doi.org/10.1134/S1995080222050201.

30. Schneier B. Cryptographic design vulnerabilities. *IEEE Comput.*, 1998, vol. 31, no. 9, pp. 29–33.

31. Shinge S.R., Patil R. An encryption algorithm based on ASCII value of data. *Int. J. Comput. Sci. Inf. Technol.*, 2014, vol. 5, no. 6, pp. 7232–7234.

32. Ker D.A. A capacity result for batch steganography. *IEEE Signal Process. Lett.*, 2007, vol. 14, no. 8, pp. 525–528. https://doi.org/10.1109/LSP.2006.891319.

33. Matsumoto M., Nishimura T. Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Model. Computer Simul. (TOMACS)*, 1998, vol. 8, no. 1, pp. 3–30. https://doi.org/10.1145/272991.272995.

34. Hegadi R., Patil A.P. A statistical analysis on in-built pseudo random number generators using NIST test suite. *Proc. 2020 5th Int. Conf. on Computing, Communication and Security (ICCCS)*. Patna, IEEE, 2020, pp. 1–6. https://doi.org/10.1109/ICCCS49678.2020.9276849.

35. Maurer U.M. A universal statistical test for random bit generators. *J. Cryptol.*, 1992, vol. 5, no. 2, pp. 89–105. https://doi.org/10.1007/BF00193563.

36. Sadique Uz Zaman J.K.M., Ghosh R. Review on fifteen statistical tests proposed by NIST. *J. Theor. Phys. Cryptogr.*, 2012, vol. 1, pp. 18–31.

37. Gyarmati K. On a pseudorandom property of binary sequences. *Ramanujan J.*, 2004, vol. 8, no. 3, pp. 289–302. https://doi.org/10.1007/s11139-004-0139-z.

38. Matsumoto M., Saito M., Nishimura T., Hagita M. CryptMT stream cipher version 3. eSTREAM, ECRYPT Stream Cipher Project, Report. Vol. 28. 2007.

39. Vershinin I.S. Durability of the associative protection of distributed cartographic objects. *Nelineinyi Mir*, 2011, vol. 9, no. 12, pp. 822–825. (In Russian)

40. Probert T. MapInfo Professional v10.5. *GeoInformatics*, 2010, vol. 13, no. 6, p. 62.

41. Vershinin I.S. Refinement of the redundancy criterion for noise-resistant hiding of information in associative steganography. *Inf. Bezop.*, 2016, vol. 19, no. 4, pp. 511–514. (In Russian)

42. Gibadullin R.F., Vershinin I.S., Raikhlin V.A. Steganographic and computational strength of associative steganography. In: *Metody modelirovaniya-VII* [Methods of Modeling-VII], 2019, pp. 23–38. (In Russian)

43. Raikhlin V.A., Vershinin I.S., Klassen R.K., Gibadullin R.F., Pystogov S.V. *Konstruktivnoe modelirovanie protsessov sinteza* [Constructive Modeling of Synthesis Processes]. Kazan, Fen, 2020. 248 p. (In Russian)

44. Vershinin I.S., Gibadullin R.F., Pystogov S.V. State Registration Certificate for Software No. 2016611421. "Security Map Cluster" program for managing associative protected cartographic databases. Russia, 2016. (In Russian)

45. Vershinin I.S., Gibadullin R.F. State Registration Certificate for Software No. 2021613638. "Stego" program for associative protection of files. Russia, 2021.

46. Shannon C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 1949, vol. 28, no. 4, pp. 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.

Информация об авторах

Игорь Сергеевич Вершинин, доктор технических наук, доцент, заведующий кафедрой «Компьютерные системы», Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ

E-mail: *ISVershinin@kai.ru*

ORCID: https://orcid.org/0000-0001-5166-2862

Руслан Фаршатович Гибадуллин, кандидат технических наук, доцент, доцент кафедры «Компьютерные системы», Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ

E-mail: *RuslanGibadullin@vk.com*

ORCID: https://orcid.org/0000-0001-9359-911X

Вадим Абрамович Райхлин, доктор физико-математических наук, профессор, профессор кафедры «Компьютерные системы», Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ

E-mail: *rajhlin.cs@kstu-kai.ru*

Author Information

Igor S. Vershinin, Dr. Sci. (Engineering), Associate Professor, Head of Department of Computer Systems, Kazan National Research Technical University named after A.N. Tupolev – KAI

E-mail: *ISVershinin@kai.ru*

ORCID: https://orcid.org/0000-0001-5166-2862

Ruslan F. Gibadullin, Cand. Sci. (Engineering), Associate Professor, Department of Computer Systems, Kazan National Research Technical University named after A.N. Tupolev – KAI

E-mail: *RuslanGibadullin@vk.com*

ORCID: https://orcid.org/0000-0001-9359-911X

Vadim A. Raikhlin, Dr. Sci. (Physics and Mathematics), Full Professor, Department of Computer Systems, Kazan National Research Technical University named after A.N. Tupolev – KAI

E-mail: *rajhlin.cs@kstu-kai.ru*

Поступила в редакцию 2.08.2025 Received August 2, 2025

Принята к публикации 14.09.2025 Accepted September 14, 2025