9. Skoba, A. N., Mikhaylov, V. K., Ayesh, Akhmed Nafea Ayesh. Reshenie zadachi obespecheniya optimalnoy effektivnosti funktsionirovaniya raspredelennykh sistem obrabotki informatsii [Solving the problem of ensuring the optimal efficiency of functioning of distributed information processing systems]. *Inzhenernyy vestnik Dona* [Engineering Journal of Don], 03.06.2021, no. 6. Available at: www.ivdon.ru/ru/magazine/archive/n6y2021/7053.

10. Chor, B., Rivest, R. A Krapsack-type pubkie key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, 1988, vol. 34, pp. 901–909.

11. Osipyan, V. O., Litvinov, K. I., Bagdasaryan, R. Kh., Lukashchik, E. P., Sinitsa, S. G., Zhuk, A. S. Development of information security system mathematical models by the solutions of the multigrade diophantine equation systems. *International Conference Proceeding Series, Association for Computing Machinery*, 2019.

УДК 004.421.5

## ВАРИАНТ РЕАЛИЗАЦИИ СХЕМЫ ПРЕОБРАЗОВАНИЯ ВХОДНОГО ПОТОКА ДАННЫХ АСИММЕТРИЧНЫМ МЕТОДОМ НА БАЗЕ КЛЕТОЧНЫХ АВТОМАТОВ[1]

*Статья поступила в редакцию 24.08.2021, в окончательном варианте – 09.09.2021.*

***Кулешова Елена Александровна***[2], Юго-Западный государственный университет, 305004, Россия, г. Курск, ул. Челюскинцев, 19, корпус Б,
аспирант, ORCID: 0000−0002−8270−564X, e–mail: lena.kuleshova.94@mail.ru

В настоящее время известны такие приложения теории клеточных автоматов, как симметричное шифрование, сжатие данных, обработка цифровых изображений и некоторые другие. Также существуют исследования, предполагающие возможность построения системы с открытым ключом на базе клеточных автоматов, однако данная задача пока не была решена. В данной статье предлагается вариант схемы преобразования входного потока данных асимметричным методом на базе клеточных автоматов. Предложена схема преобразования, основанная на последовательном изменении битов исходного файла согласно инструкциям в ключе. Открытым параметром в данном случае будет являться число столбцов информационной матрицы, а закрытый ключ будет состоять из матрицы шифрования и правила обхода матрицы данных. В целях повышения стойкости и поддержания высокой скорости обработки потока данных предложена математическая модель преобразования данных на базе клеточных автоматов с использованием расширенного ключа, определяющего индивидуальную окрестность обрабатываемого бита данных с учетом положения данного бита в матрице исходных данных. Для верификации математической модели был разработан программный модуль для анализа индивидуальных цепочек в блоках данных, позволяющий сопоставить блоки данных в виде бинарных матриц. Практическая значимость предложенного решения заключается в том, что полученные результаты можно использовать в исследовательских целях и в возможности применения полученных решений для развития методов криптографического преобразования данных.

**Ключевые слова:** информационная безопасность, потоковая передача данных, клеточные автоматы, асимметричное шифрование, системы защиты конфиденциальной информации

## A VARIANT OF IMPLEMENTATION OF THE SCHEME FOR CONVERSION OF THE INPUT DATA FLOW BY THE ASYMMETRIC METHOD ON THE BASIS OF CELLULAR AUTOMATA

*The article was received by the editorial board on 24.08.2021, in the final version – 09.09.2021.*

***Kuleshova Elena A.***, Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,
postgraduate student, ORCID: 0000−0002−8270−564X, e-mail: lena.kuleshova.94@mail.ru

At present, such applications of the theory of cellular automata as symmetric encryption, data compression, digital image processing, and some others are known. There are also studies suggesting the possibility of building a public key system based on cellular automata, but this problem has not yet been solved. This article proposes a variant of the scheme for transforming the input data stream by an asymmetric method based on cellular automata. The proposed conversion scheme is based on the sequential change of the bits of the source file according to the instructions in the key. The public parameter in this case will be the number of columns of the information matrix, and the private key will consist of the encryption matrix and the rule for traversing the data matrix. In order to increase the stability and maintain a high processing speed of data streams, a mathematical model of data transformation based on cellular automata with the use of an extended key, which determines the individual neighborhood of the processed data bit, taking into account the position of this bit in the initial data matrix, is proposed. To verify the mathematical model, a software module was developed for the analysis of individual chains in data blocks, which makes it possible

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-31-90069.

[2] Научный руководитель – Добрица Вячеслав Порфирьевич, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19, корпус Б, доктор физико-математических наук, профессор, e-mail: dobritsa@mail.ru

to compare data blocks in the form of binary matrices. The practical significance of the proposed solution lies in the fact that the results obtained can be used for research purposes and in the possibility of using the obtained solutions for the development of methods for cryptographic data transformation.

**Keywords:** information security, data streaming, cellular automata, asymmetric encryption, confidential information protection systems

**Graphical annotation (Графическаяаннотация)**


**Введение.** Идея клеточных автоматов была предложена Дж. Фон Нейманом и К. Цусе в конце 40-х годов. Изначально клеточные автоматы рассматривались как универсальная вычислительная среда для построения алгоритмов и моделирования физических процессов, эквивалентная по собственным возможностям машине Тьюринга [1]. С начала 70-х годов в Берлине начали регулярно проводиться международные конференции по параллельной обработке информации на клеточных автоматах. В это же время получила известность игра «Жизнь», основанная на двумерных клеточных автоматах. В 1983 г. британский математик С. Вольфрам начинает работу над моделью клеточных автоматов, которую впоследствии применял в криптографии и гидродинамике. В области симметричного шифрования стоит выделить работы [2, 3], а также работы [4–6], в которых рассмотрена задача обратимости клеточных автоматов.

Описание клеточного автомата с целевой функцией было представлено в работе в работе [7], данная идея получила развитие в работах [8, 9], в которых было предложено определение усовершенствованного клеточного автомата на разбиении и описана модель клеточного автомата с плавающим окном. При использовании клеточного автомата с плавающим окном обработка (шифрование) начинается с первого блока (зависит от входных параметров и режима обработки), далее итеративный процесс повторяется по порядку до обработки всех блоков [10]. Основываясь на исследования, проведенных в данной работе было принято решение о введение локального правила обработки блоков на основе конечного набора шаблонов, что предполагает сокращение времени шифрования без потери стойкости шифра. Каждый шаблон задает индивидуальную окрестность информационным битам. Функция обновления работает с ячейкой тогда и только тогда, когда существует соответствие между состояниями ее соседей и заданным шаблоном.

**Схема преобразования данных.** Предложенная схема преобразования основана на последовательном изменении битов исходного файла согласно инструкциям в ключе. Открытым параметром является число столбцов информационной матрицы – эта информация передается по открытому каналу связи. Закрытый ключ состоит из матрицы шифрования и правила обхода матрицы данных. Схема работы системы обработки двоичного потока данных представлена на рисунке 1.

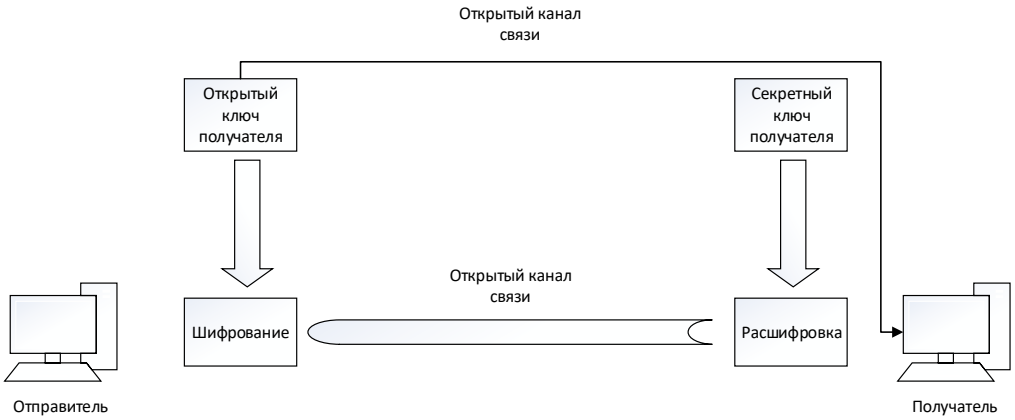



Рисунок 1 – Схема работы системы обработки двоичного потока данных

В качестве основы алгоритма возьмем модель клеточного автомата, в которой элементы системы определяются согласно заданной окрестности. В качестве блока будет рассматриваться элемент информационной матрицы. Вводится правило локальной обработки элементов матрицы на основе конечного набора шаблонов. Каждый шаблон задает индивидуальную окрестность информационным битам. Функция обновления работает с ячейкой тогда и только тогда, когда существует соответствие между состояниями ее соседей и шаблоном. Основываясь на исследованиях, приведенных в статье [11], введем два серьезных ограничения: все шаблоны в композиции имеют такую же окрестность, что и конечный результат их композиции, и все шаблоны имеют одинаковую форму. Эти простые ограничения позволяют создавать прозрачную и эффективную в части использования вычислительных ресурсов реализацию.

**Материалы и методы.** По результатам проведенных исследований, определено, что системы преобразования данных с применением как открытого, так и закрытого ключа обладают своими преимуществами и недостатками. Именно поэтому, чтобы создать устойчивую систему, обладающую всеми преимуществами, необходимо объединить асимметричный метод с симметричным, получив гибридную систему.

В качестве асимметричной части разрабатываемой системы будем использовать метод RSA, так как он зарекомендовал себя, как надежный и простой в реализации метод. Симметричной частью разрабатываемого приложения будет являться метод шифрования на базе клеточных автоматов [12].

Для описания работы метода рассмотрим работу с бинарной матрицей. В качестве закрытого ключа выступает так называемая квадратная шифр-матрица, которая задается бинарным файлом. Она является шаблоном, задающим индивидуальную битам матрицы данных. Размерность P матрицы (формула 1) шифрования определим, как целую часть от корня из количества бит в файле матрицы:

$$P = \left\lfloor \sqrt{s(x) \cdot 8} \right\rfloor, \tag{1}$$

где $s(X)$ – размер исходного файла в байтах.

Далее определяем размерность сегмента матрицы данных. Число столбцов информационной матрицы $N_1$ является открытым параметром шифрования.

Рекомендуется принимать $N_1 >$ P, так как открытый параметр задает ширину рабочей части матрицы. Соблюдение данной рекомендации максимизирует число индивидуальных окрестностей, так как шифр-матрица работает по всей ширине и повышает криптостойкость преобразования [13].

Метод формирования индивидуальной окрестности состоит в том, что на каждый информационный бит (n – номер столбца, m – номер строки) накладывается окрестность. На примере окрестности Мура w-го порядка можем определить координаты центра по формулам 2–3:

$$x = m \bmod (P - w) + \left\lfloor \frac{w}{2} \right\rfloor + 1; \tag{2}$$

$$y = n \bmod (P - w) + \left\lfloor \frac{w}{2} \right\rfloor + 1. \tag{3}$$

Далее в соответствии с правилом обхода матрицы производим шифрование на клеточном уровне с учетом индивидуальной окрестности. Базовый уровень защиты данных предполагает однократный обход элементов матрицы по выбранному маршруту, продвинутый уровень защиты - два варианта обхода. Таким образом, клеточным автоматом с индивидуальной окрестностью называют совокупность (формула 4):

$$CA_{OM} =< Z^n, (N_1, \ldots, N_n), A, X(p_1, \ldots, p_n), P > . \tag{4}$$

где $Z^n$ – размерность клеточного автомата $(n = 2)$;

$(N_1, \ldots, N_n)$ – размер сегмента матрицы данных, при этом $N_1$ является открытым параметром шифрования;

$X(p_1, \ldots, p_n)$ – шифр-матрица;

$A = \{0,1\}$ – значение битов данных;

$P$ – размерность матрицы шифрования.

Рассмотрим метод шифрования разработанной системы на примере окрестности Мура первого порядка.

1. Определяем размерность матрицы шифрования исходя из соображений, что она квадратная и максимально учитывает секретный ключ. Шифр-матрица является шаблоном, в соответствии с которым задается индивидуальная окрестность информационного бита по формуле 5:

$$P = \begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & ? & p_{23} \\ p_{31} & p_{32} & p_{33} \end{bmatrix}. \quad (5)$$

Закрытый ключ получателя записывается в матрицу ключа *P*. Принцип записи отображен в таблице 1.

Таблица 1 – Принцип записи ключа в матрицу *P*

| Элемент матрицы | $p_{11}$ | $p_{12}$ | $p_{13}$ | $p_{21}$ | $p_{22}$ | $p_{23}$ | $p_{31}$ | $p_{32}$ | $p_{33}$ |
|---|---|---|---|---|---|---|---|---|---|
| Порядковый номер бита | 1 | 2 | 3 | 4 | | 5 | 6 | 7 | 8 |

2. Определим размерность сегмента матрицы данных. Построим матрицу *N* размером *n x m*. Число столбцов матрицы $N_1$ является в данном случае открытым параметром (рекомендуется $N_1$>P), формула 6:

$$N = \begin{bmatrix} a_{11} & a_{12} & a_{13} & & a_{1m} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2m} \\ a_{31} & a_{32} & a_{33} & & \\ & \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nm} \end{bmatrix}. \quad (6)$$

При этом $a_{11}, a_{12,} \ldots, a_{nm}$ соответствуют битам файла $s_1, s_{2,} \ldots, s_i$. Если размер файла $S < n \cdot m$, тогда заполним пустые элементы матрицы нулями, количество таких элементов вычисляется по формуле 7:

$$x = n \cdot m - S. \quad (7)$$

Другими словами, последний сегмент матрицы может быть дополнен нулевыми битами (хвостом) для полноты прямоугольного сегмента [14, 15]. Остальные сегменты не нуждаются в дополнении, так как размерность матрицы в соответствии с предложенным методом кратна восьми [16]. Для обратимости шифрования и исключения «хвоста» можно использовать криптографические хеш-функции от числа добавленных элементов, в таком случае целесообразно использовать произвольную цепочку бит [17]. При дешифровании это позволит определить количество бит, которые не будут учитываться при работе программного модуля.

3. Формируем матрицу зашифрованного текста $N^*$. При наложении окрестности, центральный элемент которой вычисляется по формуле 8, нумерация строк и столбцов матрицы начинается с нуля. Для элементов $a_{ij}$ последовательно (в соответствие с правилом обхода матрицы данных) применяются следующие действия: сравниваются окрестности элемента матрицы $N^*$ и центрального элемента шаблона $P$. Если элементы окрестности $L_{p_{22}}$ центрального элемента ключа не совпадают с аналогичными элементами окрестности $L_{a_{ij}}$ элемента матрицы $N^*$, то значение элемента остается прежним, в противном случае для элемента применяется операция сложения по модулю два с единичными битами:

$$a_{ij} = \begin{cases} a_{ij} \oplus 1, \forall\, p_{ij} = 1, p_{ij} = a_{ij} \\ a_{ij} \oplus 0, \forall\, p_{ij} = 1, p_{ij} \neq a_{ij} \end{cases} \quad (8)$$

4. Элементы полученной матрицы записываются в пустой файл и собираются в соответствии с правилом сбора сегментов данных.

При обратном преобразовании важно производить инверсный обход элементов матрицы.

**Оценка распределения цепочек выходных бит.** Для оценки равномерности распределения бит, полученных в ходе верификации математической модели без использования разработанного программного средства, сформируем матрицу, являющуюся разностью исходной и зашифрованной матрицы, воспользуемся программным модулем для анализа индивидуальных цепочек в блоках данных, позволяющим сопоставить блоки данных в виде бинарных матриц. В ходе экспериментальных исследований проведен анализ индивидуальных цепочек с учетом смещения относительно начала файла и размерностей бинарных фрагментов. На рисунке 2 представлен график распределения битовой последовательности, сформированный на основе исходной и зашифрованной матриц.

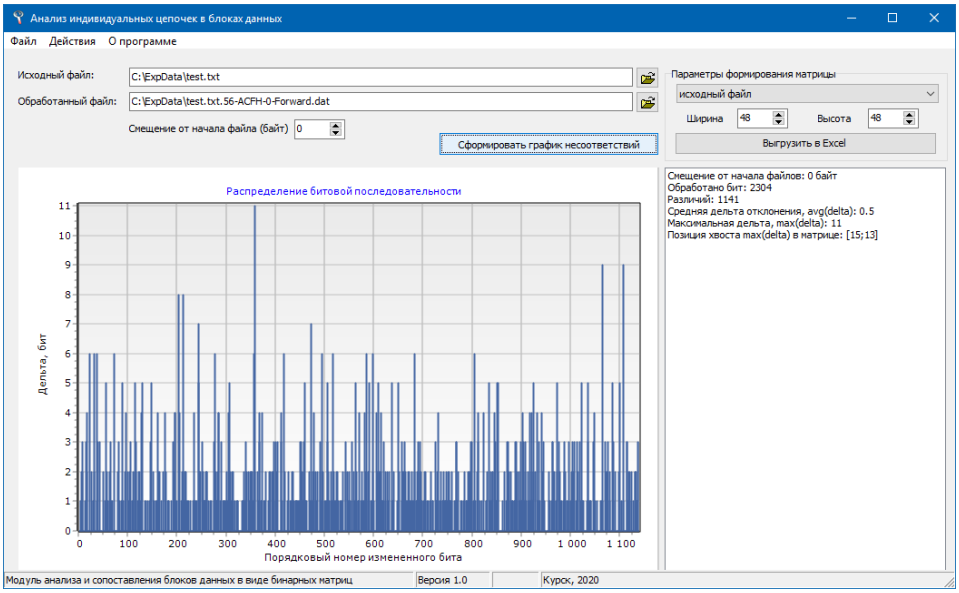
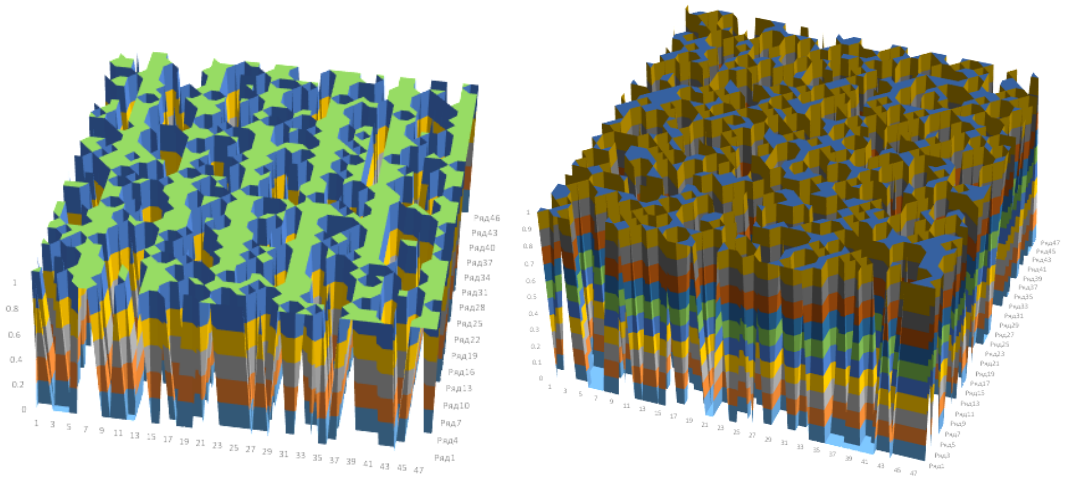



Рисунок 2 – Распределение битовой последовательности

Упрощенная визуализация матрицы в виде поверхности показана на рисунке 3. Здесь точки отличия приподнимаются от основного уровня и демонстрируют расстановку единичных бит. На схеме показан фрагмент матрицы 48 х 48 (инструмент для анализа позволяет производить выгрузку любых размерностей, в том числе с учетом смещения относительно начала файла). Наклонные грани показывают равномерный переход между состояниями и используются для лучшей визуализации. В ходе экспериментальных исследований сопоставлены классический метод обработки потока данных на базе клеточного автомата (оригинальный, рис. 3а) и метод, предложенный в данной статье (модифицированный, рис. 3б). Явно прослеживаются зависимости и неравномерность распределения бит на рисунке 3а.

Произведем выгрузку матрицы, полученной с применением модифицированного метода обработки битовой последовательности на базе клеточных автоматов (рис. 3б). Как и ожидалось, в соответствии с графиком распределения битовой последовательности, показавшим величину максимальной дельты, равной 11 бит, и средний показатель 6 бит, форма выгрузки демонстрирует более равномерное распределение данных, что значительно усложняет задачу распознавания контента.



а) б)

Рисунок 3 – Внешний вид матрицы данных

Для качественного анализа распределения изменений в ходе обработки сформируем графическое представление суперпозиции, отражающей отличие матриц с привязкой к координатам. Значением элемента матрицы будут значения {–1, 0, 1}. Мы видим, что оба варианта позволяют достичь достаточно равномерного распределения изменений на битовом уровне по обе стороны плоскости исходных данных в виде поверхности (рис. 4).

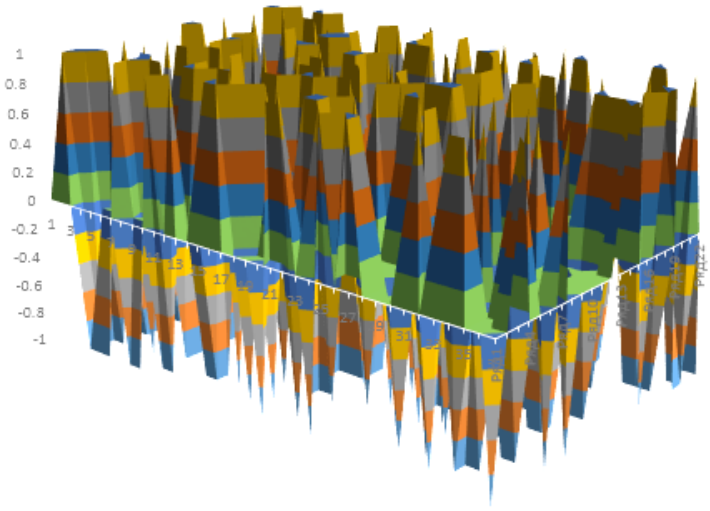


Рисунок 4 – Фрагмент суперпозиции матриц

Из полученных результатов следует, что обработанная матрица содержит не менее 45 % изменений на уровне бит и 100 % изменений на уровне байт, что условиях соответствия положения бит до и после обработки исключает доступ к защищенным данным со стороны злоумышленника без обратного преобразования, предполагающего знание или подбор ключевых параметров. Число вариантов формирования индивидуальной окрестности зависит от параметров ключа, а именно – от размера шифрующей матрицы и растет в экспоненциальной зависимости. Учитывая тот факт, что злоумышленнику, обладающему открытой частью ключа, кроме подбора матрицы-шифра требуется поиск вариантов обхода информационных бит, который может быть комбинированным, делаем вывод о высоком уровне криптостойкости.

**Обсуждение и выводы.** В ходе экспериментальных исследований сопоставлены классический метод обработки потока данных на базе клеточного автомата (оригинальный) и метод, предложенный в данной статье (модифицированный). Оба метода рассматривались в разрезе скорости обработки одним потоком, равномерности распределения бит и значения максимальной дельты между инвертированными элементами матриц. Для объективности результатов с учетом длины потока данных группа экспериментов разделена на два этапы обработки последовательностей менее 10 Мб (графика, документы, аудиофайлы), и превышающих это значение (видео-контент, архивы и т.д.). Все эксперименты проводились на одном и том же оборудовании.

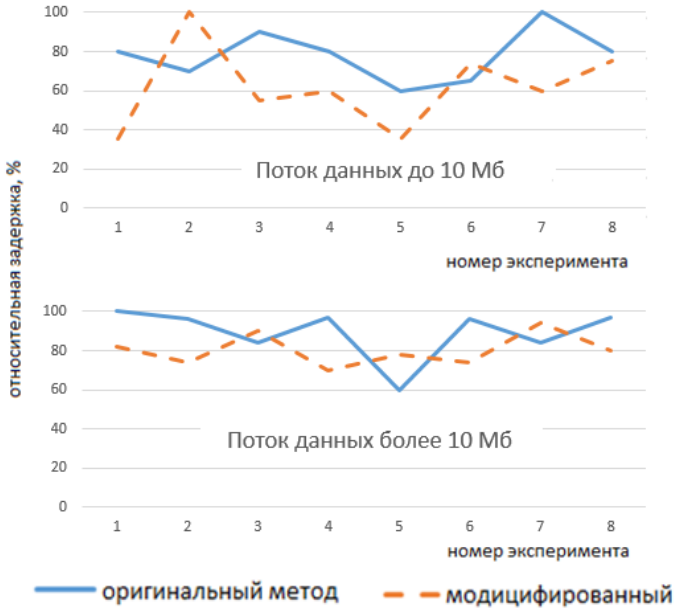



Рисунок 5 – Относительные задержки с привязкой к методу преобразования

Из рисунка 5 видно, что быстродействие модифицированного метода остается на уровне оригинального, а при обработке больших потоков данных имеет меньшие отклонения от средней величины. Это позволяет прогнозировать время обработки и учитывать при подборе аппаратной части.

Матрицы, обработанные обоими методами, по числу инверсий входят в доверительный интервал 40–60 %, что показано на рисунке 6.

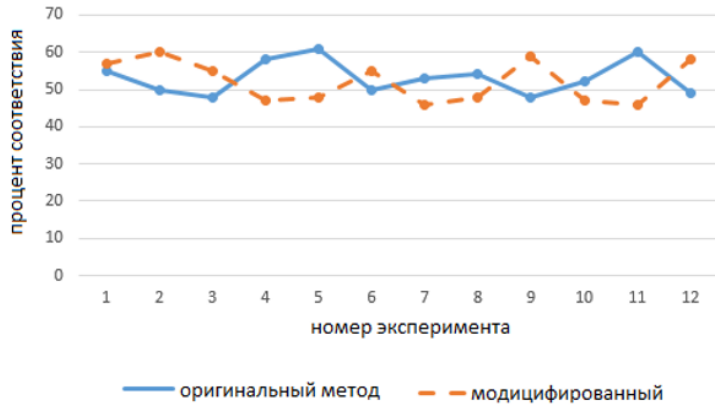



Рисунок 6 – Статистика инверсий

Оценка равномерности внесенных изменений по всем экспериментам показала изменений данных на уровне байта, значение максимальной дельты не превышает 11 бит, в то время как средний показатель составляет 5–6 бит (рис. 7).

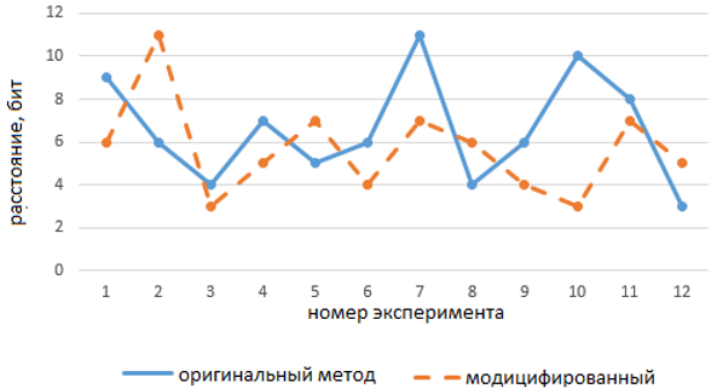



Рисунок 7 – Значений отклонений инвертированных бит (дельта)

Значение этого статистического параметра показало изменение потока данных на уровне байта, из которого можно сделать вывод о том, что оба метода не дают возможности распознать исходный контент без обратного преобразования.

**Выводы.** В данной статье предложен вариант схемы преобразования потоков данных, основанный на сочетании асимметричного шифрования и клеточных автоматов, который позволяет создать устойчивую к атакам систему защиты конфиденциальной информации.

Основным отличием предложенной схемы преобразования данных на основе клеточного автомата является использование открытого параметра, который передается по открытому каналу связи. Открытым параметром является число столбцов информационной матрицы. Также стоит отметить, что закрытый ключ в данном случае является составным и включает в себя не только матрицу шифрования, но и правила обхода матрицы данных, которые в свою очередь подразумевают два уровня защиты (базовый и продвинутый).

Проведен ряд экспериментальных исследований, которые показали, что обработанная матрица содержит не менее 45 % изменений на уровне бит и 100 % изменений на уровне байт, что в условиях соответствия положения бит до и после обработки исключает доступ к защищенным данным со стороны злоумышленника без обратного преобразования, предполагающего знание или подбор ключевых параметров, что подтверждает полноту и корректность полученных решений.

Практическая значимость данной работы заключается в возможности применения полученных решений для развития методов криптографического преобразования. Данный метод имеет перспективы повышения быстродействия за счет интеграции вычислительных серверов в масштабе вычислительной системы.

**Библиографический список**

1. Тоффоли, Т. Машины клеточных автоматов / Т. Тоффоли, Н. Марголус. – Москва : Мир, 1991. – 280 с.
2. Wuensche, A. Cellular automata encryption: the reverse algorithm, Z-parameter and chain-rules / A. Wuensche // Parallel Processing Letters. – 2009. – Vol. 19, № 2. – P. 283–297.
3. Ключарёв, П. Г. Блочные шифры, основанные на обобщённых клеточных автоматах / П. Г. Ключарёв // Наука и образование. – 2012. – № 12. – С. 27.
4. Kari, J. Reversibility and surjectivity problems of cellular automata / J. Kari // Journal of Computer and System Science. – 1994 – № 48(1). – P. 149–182.
5. Achkoun, K. SPF-CA: A new cellular automata based block cipher using key-dependent S-boxes / K. Achkoun, H. Khadija, C. Hanin, et al. // Journal of Discrete Mathematical Sciences and Cryptography. – 2019. – № 23. – P. 1–16.
6. Achkoun, K. SPF-CA-1.2: An enhanced version of cellular automata based block cipher system / K. Achkoun, C. Hanin, A. Sadak, et al. // International Journal of Computer Mathematics: Computer Systems Theory. – 2021. – № 2, vol. 6. – P. 1–17.
7. Росошек, С. К. Криптосистемы клеточных автоматов / С. К. Росошек, С. И. Боровков, О. О. Евсютин // Прикладная дискретная математика. – 2008. – № 1. – С. 43–49.
8. Добрица, В. П. Усовершенствование клеточного автомата на разбиении / В. П. Добрица, М. А. Ефремов, Д. М. Зарубин, А. А. Асютиков // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения : сб. тр. 1 Всероссийской научно-практической конференции. – Курск, 2017. – С. 224–227.
9. Franti, E. Cellular Automata Encryption System / E. Franti, M. Dascalu // Proceedings of the Fifth International Conference on Engineering Computational Technology. – Civil-Comp Press, Stirlingshire, UK, 2021. – P. 283–297.
10. Марухленко, А. Л. Вариант организации многопоточной обработки конфиденциальных данных на базе клеточных автоматов / А. Л. Марухленко, А. В. Плугатарев, М. О. Таныгин, Л. О. Марухленко, Д. О. Бобынцев // Известия Юго-Западного государственного университета. – 2019.– Т. 23, № 3. – С. 100–112.
11. Lira, E. A reversible system based on hybrid toggle radius-4 cellular automata and its application as a block cipher / E. Lira, H. Macêdo, D. Lima, et al. // Natural Computing. – 2021. – № 2. – P. 1–34.
12. Кулешова, Е. А. Программа для многопоточного шифрования на базе клеточных автоматов / Е. А. Кулешова, А. Л. Марухленко, В. П. Добрица, М. О. Таныгин, Л. О. Марухленко // Свидетельство о регистрации программы для ЭВМ RU 2019664789, 13.11.2019. – Заявка № 2019663418 от 29.10.2019. – Режим доступа: https://www.elibrary.ru/item.asp?id=41364754, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 03.03.2021).
13. Марухленко, А. Л. Анализ потенциальных уязвимостей и современных методов защиты многопользовательских ресурсов / А. Л. Марухленко, М. О. Марухленко, Е. Е. Конорева, М. О. Таныгин // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения : II Всероссийская научно-практическая конференция. – Курск : ЮЗГУ, 2018. – С. 136–140.
14. Марухленко, А. Л. Вариант разграничения доступа к информационным ресурсам на основе неявной аутентификации / А. Л. Марухленко, А. В. Плугатарев, М. О. Таныгин, Л. О. Марухленко, М. Ю. Шашков // Известия Юго-Западного государственного университета. – 2020. – Т. 24, № 2. – С. 108–121.
15. Марухленко, А. Л. Комплексная оценка информационной безопасности объекта с применением математической модели для расчета показателей риска / А. Л. Марухленко, А. В. Плугатарев, М. О. Марухленко, М. А. Ефремов // Известия Юго-Западного государственного университета. – 2018. – Т. 8, № 4 (29). – С. 34–40.
16. Kumaresan, G. An Analytical Study of Cellular Automata and its Applications in Cryptography / G. Kumaresan, N. Gopalan // International Journal of Computer Network and Information Security. – 2017. – № 12. – P. 45–54.
17. Зотов, Я. А. Использование клеточных автоматов в симметричной криптосистеме / Я. А. Зотов // Вопросы кибербезопасности. – 2015. – Т. 11, № 3. – С. 43–45.

**References**

1. Toffoli, T., Margolus, N. *Mashiny kletochnykh avtomatov* [Machines of cellular automata]. Moscow, Mir Publ., 1991. 280 p.
2. Wuensche, A. Cellular automata encryption: the reverse algorithm, Z-parameter and chain-rules. *Parallel Processing Letters*, 2009, vol. 19, no. 2, pp. 283–297.
3. Klyucharyov, P. G. Blochnyye shifry, osnovannyye na obobshchonnykh kletochnykh avtomatakh [Block ciphers based on generalized cellular automata]. *Nauka i obrazovaniye* [Science and education], 2012, no. 12, p. 27.
4. Kari, J. Reversibility and surjectivity problems of cellular automata. *Journal of Computer and System Science*, 1994, no. 48 (1), pp. 149–182.

5. Achkoun, K., Khadija, H., Hanin C. et al. SPF-CA: A new cellular automata based block cipher using key-dependent S-boxes. *Journal of Discrete Mathematical Sciences and Cryptography*, 2019, no. 23, pp. 1–16.

6. Achkoun, K., Hanin, C., Sadak, A. et al. SPF-CA-1.2: An enhanced version of cellular automata based block cipher system. *International Journal of Computer Mathematics: Computer Systems Theory,* 2021, no. 2, vol. 6, pp. 1–17.

7. Rososhek, S. K., Borovkov, S. I., Evsyutin, O. O. Kriptosistemy kletochnykh avtomatov [Cryptosystems of cellular automata]. *Prikladnaya diskretnaya matematika* [Applied discrete mathematics], 2008, no. 1, pp. 43-49.

8. Dobritsa, V. P., Efremov, M. A., Zarubin, D. M., Asyutikov, A. A. Usovershenstvovaniye kletochnogo avtomata na razbiyenii [Improvement of a cellular automaton on a partition]. *Infokommunikatsii i kosmicheskiye tekhnologii: sostoyaniye, problemy i puti resheniya : sbornik trudov 1 Vserossiyskoy nauchno-prakticheskoy konferentsii* [Infocommunications and space technologies: state, problems and solutions : collection of works of the 1st All-Russian Scientific and Practical Conference]. Kursk, 2017, pp. 224–227.

9. Franti, E., Dascalu, M. Cellular Automata Encryption System. *Proceedings of the Fifth International Conference on Engineering Computational Technology*. Civil-Comp Press, Stirlingshire, UK, 2021, pp. 283–297.

10. Marukhlenko, A. L., Plugatarev, A. V., Tanygin, M. O., Marukhlenko, L. O., Bobintsev, D. O. Variant organizatsii mnogopotochnoy obrabotki konfidentsialnykh dannykh na baze kletochnykh avtomatov [A Variant of the Organization of Multithreaded Processing of Confidential Data Based on Cellular Automata]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta* [Bulletin of the Southwest State University], 2019, vol. 23, no. 3, pp. 100–112.

11. Lira, E., Macêdo, H., Lima, D. et al. A reversible system based on hybrid toggle radius-4 cellular automata and its application as a block cipher. *Natural Computing*, 2021, no. 2, pp. 1–34.

12. Kuleshova, E. A., Marukhlenko, A. L., Dobritsa V. P., Tanygin, M. O., Marukhlenko L. O. *Programma dlya mnogopotochnogo shifrovaniya na baze kletochnykh avtomatov* [A Program for Multithreaded Encryption Based on Cellular Automata]. Certificate of registration of a computer program RU 2019664789, 11.13.2019. Application no. 2019663418 dated October 29, 2019. Available at: https://www.elibrary.ru/item.asp?id=41364754 (accessed 03.16.2021).

13. Marukhlenko, A. L., Marukhlenko, L. O., Konoreva, E. E., Tanygin, M. O. Analiz potentsialnykh uyazvimostey i sovremennykh metodov zashchity mnogopolzovatelskikh resursov [Analysis of Potential Vulnerabilities and Modern Methods of Protecting Multi-User Resources]. *Infokommunikatsii i kosmicheskiye tekhnologii: sostoyaniye, problemy i puti resheniya : II Vserossiyskaya nauchno-prakticheskaya konferentsiya* [Infocommunications and Space Technologies: State, Problems and Solutions : II All-Russian Scientific and Practical Conference]. Kursk, 2018, pp. 136–140.

14. Marukhlenko, A. L., Plugatarev, A. V., Tanygin, M. O., Marukhlenko, L. O., Shashkov, M. Yu. Variant razgranicheniya dostupa k informatsionnym resursam na osnove neyavnoy autentifikatsii [Variant of Differentiation of Access to Information Resources Based on Implicit Authentication]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta* [Bulletin of the Southwest State University], 2020, vol. 24, no. 2, pp. 108–121.

15. Marukhlenko, A. L., Plugatarev, A. V., Marukhlenko, L. O., Efremov, M. A. Kompleksnaya otsenka informatsionnoy bezopasnosti obekta s primeneniyem matematicheskoy modeli dlya rascheta pokazateley riska [Comprehensive Assessment of the Information Security of an Object Using a Mathematical Model for Calculating Risk Indicators]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta* [Bulletin of the Southwest State University], 2018, vol. 8, no. 4 (29), pp. 34–40.

16. Kumaresan, G., Gopalan, N. An Analytical Study of Cellular Automata and its Applications in Cryptography. *International Journal of Computer Network and Information Security*, 2017, no. 12, pp. 45–54.

17. Zotov, Ya. A. Ispolzovaniye kletochnykh avtomatov v simmetrichnoy kriptosisteme [The use of cellular automata in a symmetric cryptosystem]. *Voprosy kiberbezopasnosti* [Issues of cybersecurity], 2015, vol. 11, no. 3, pp. 43–45.