



Ә.Қ. Жүнісхан¹, Қ.С. Сақан^{1,2}, М.Д. Джакипбеков³

¹Farabi University, Алматы, Қазақстан

²Institute of Information and Computational Technologies CS MSHE RK,
Алматы, Қазақстан

³National Defense University of the Republic of Kazakhstan, Астана, Қазақстан
E-mail: assel.zhuniskhan@gmail.com

ПРИМЕНЕНИЕ ДИНАМИЧЕСКИХ ХАОТИЧЕСКИХ ФУНКЦИЙ В КРИПТОГРАФИИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Аннотация. В статье представлен обзор современных подходов к применению динамических хаотических функций в криптографии. Рассмотрены основные свойства хаотических систем, обеспечивающие возможность их использования для защиты информации, включая чувствительность к начальным условиям, эргодичность, нелинейность и псевдослучайность. Проведен анализ существующих направлений использования хаотических отображений в криптографических алгоритмах, таких как генерация псевдослучайных последовательностей, симметричное шифрование, защита изображений и легковесная криптография для устройств Интернета вещей. Отмечены основные преимущества и ограничения хаотических криптосистем, а также перспективы их дальнейшего развития в условиях появления постквантовых вычислений.

Ключевые слова: хаотические системы, динамические функции, хаотические отображения, генерация ключей, псевдослучайные последовательности, информационная безопасность.

Введение.

Развитие цифровых технологий сопровождается постоянным увеличением объемов передаваемой и хранимой информации, что требует совершенствования методов ее защиты. Традиционные криптографические алгоритмы обеспечивают высокий уровень безопасности благодаря использованию сложных математических задач, однако развитие вычислительной техники и появление квантовых вычислений стимулируют поиск новых подходов к построению криптографических механизмов [1].

Одним из перспективных направлений является применение методов теории хаоса. Исследования в данной области ведутся с конца XX века, когда было установлено сходство между свойствами хаотических динамических систем и требованиями, предъявляемыми к криптографическим алгоритмам [2,3,4]. В частности, хаотические системы обладают высокой



чувствительностью к начальным условиям, демонстрируют сложное непериодическое поведение и способны генерировать последовательности, близкие по своим характеристикам к случайным [5]. Эти особенности делают их привлекательными для построения генераторов псевдослучайных чисел, систем шифрования и механизмов формирования криптографических ключей [6].

Несмотря на значительное количество опубликованных работ, вопрос практического применения хаотических систем в криптографии остается актуальным. Современные исследования направлены не только на разработку новых схем шифрования, но и на оценку их криптографической стойкости с учетом требований современной теории криптографии [6].

Целью данной работы является анализ современных подходов к использованию динамических хаотических функций в криптографии, а также выявление перспективных направлений их дальнейшего развития.

Материалы и методы.

Основные свойства динамических хаотических систем. Под хаотической системой понимают нелинейную динамическую систему, поведение которой определяется детерминированными законами, но при этом характеризуется высокой степенью сложности и непредсказуемости. Хаотическое поведение возникает вследствие многократного применения нелинейных преобразований и проявляется даже при отсутствии внешних случайных воздействий [7,8].

Возможность применения хаотических систем в криптографии обусловлена рядом свойств.

Чувствительность к начальным условиям. Одним из основных признаков хаоса является существенное различие траекторий системы при незначительном изменении начальных параметров. Даже минимальное изменение начального значения приводит к экспоненциальному расхождению последовательностей. Данное свойство соответствует криптографическому требованию лавинного эффекта, согласно которому незначительное изменение ключа должно приводить к существенному изменению результата шифрования [9].

Нелинейность. Хаотические отображения являются нелинейными функциями, что существенно усложняет анализ их поведения и повышает устойчивость к различным методам криптоанализа. Нелинейность обеспечивает реализацию свойства confusion, сформулированного К. Шенноном как одного из базовых принципов криптографической защиты информации [10].

Эргодичность. Эргодичность означает способность траектории хаотической системы со временем посещать практически все допустимые состояния фазового пространства. Благодаря этому обеспечивается равномерное распределение генерируемых значений и улучшаются статистические характеристики формируемых последовательностей [11].



Псевдослучайность. Последовательности, генерируемые хаотическими системами, обладают свойствами, близкими к случайным последовательностям. Это позволяет использовать их для генерации ключевого материала и псевдослучайных чисел, необходимых в криптографических приложениях [12].

Наиболее распространенными хаотическими отображениями, применяемыми в криптографии, являются логистическое отображение, отображение Тента, отображение Хенона и система Лоренца [5].

Логистическое отображение описывается выражением:

$$x_{n+1} = rx_n(1 - x_n), \quad (1)$$

где x_n принадлежит интервалу $(0;1)$, а параметр r определяет режим функционирования системы.

Благодаря простоте реализации логистическое отображение получило широкое распространение в ранних хаотических криптосистемах. Однако последующие исследования показали наличие ряда ограничений, связанных с конечной точностью вычислений и возможностью восстановления параметров системы [13].

В современных разработках все чаще используются многомерные и гиперхаотические системы, обладающие более сложной динамикой и значительно большим пространством состояний [14]. Применение гиперхаотических систем позволяет повысить криптографическую стойкость за счет использования нескольких положительных показателей Ляпунова и более сложных механизмов формирования ключевых последовательностей.

Таблица 1 – Сравнение наиболее распространенных хаотических отображений

Хаотическая система	Размерность	Основные свойства	Преимущества	Недостатки
Logistic Map	1D	Чувствительность к начальным условиям	Простота реализации	Ограниченное пространство ключей
Tent Map	1D	Хорошая равномерность распределения	Высокая скорость вычислений	Уязвимость при конечной точности
Henon Map	2D	Нелинейность и сложная динамика	Более высокая стойкость	Повышенная вычислительная сложность
Arnold Cat Map	2D	Пространственное перемешивание	Эффективна для изображений	Ограниченная область применения
Lorenz System	3D	Сложная хаотическая динамика	Большое пространство состояний	Высокие вычислительные затраты



Хаотическая система	Размерность	Основные свойства	Преимущества	Недостатки
Hyperchaotic Systems	4D и выше	Несколько положительных показателей Ляпунова	Высокая криптостойкость	Сложность реализации

Как показывают современные обзоры, наблюдается постепенный переход от одномерных отображений к многомерным и гиперхаотическим системам, обеспечивающим более высокий уровень безопасности [13, 15].

Применение динамических хаотических функций в криптографии.

Благодаря своим свойствам динамические хаотические системы нашли применение в различных направлениях криптографии. Наиболее активно хаотические отображения используются для генерации псевдослучайных последовательностей, построения симметричных криптосистем, защиты мультимедийных данных и разработки легковесных алгоритмов для устройств с ограниченными вычислительными ресурсами [16].

Генерация псевдослучайных последовательностей.

Генераторы псевдослучайных чисел являются одним из ключевых компонентов большинства криптографических систем. Они используются при формировании ключей шифрования, генерации случайных параметров протоколов аутентификации и создании одноразовых ключевых последовательностей.

Хаотические отображения обладают рядом характеристик, необходимых для построения эффективных генераторов случайных чисел. В частности, высокая чувствительность к начальным условиям позволяет получать существенно различные последовательности даже при незначительном изменении параметров системы. Кроме того, хаотические последовательности характеризуются высокой энтропией и хорошими статистическими свойствами [17].

Наиболее распространенными решениями являются генераторы, основанные на логистическом отображении, отображении Тента и их модификациях. Однако исследования последних лет показывают, что применение только одномерных хаотических карт не всегда обеспечивает требуемый уровень криптографической стойкости. В связи с этим активно развиваются гибридные схемы, объединяющие несколько хаотических отображений или использующие гиперхаотические системы [18].

Одним из важных направлений исследований является прохождение генерируемыми последовательностями стандартных статистических тестов NIST SP 800-22, позволяющих оценивать качество случайности выходных данных. Современные гиперхаотические генераторы демонстрируют результаты, сопоставимые с традиционными криптографическими генераторами случайных чисел.

Применение хаоса в симметричном шифровании.



Одним из наиболее распространенных направлений использования хаотических функций является симметричное шифрование данных. Основная идея заключается в использовании хаотических последовательностей для формирования ключевого потока либо для организации процессов перестановки и подстановки элементов открытого текста [4, 12].

Большинство хаотических алгоритмов реализуют два базовых механизма криптографической защиты:

- перестановку (permutation);
- диффузию (diffusion).

На этапе перестановки выполняется изменение порядка расположения элементов данных. Далее производится этап диффузии, в ходе которого изменяются значения элементов информации с использованием хаотически сформированных последовательностей [4, 9].

Использование хаотических функций позволяет повысить степень нелинейности алгоритма и усложнить восстановление исходных данных без знания секретных параметров системы. Кроме того, хаотические отображения могут применяться для динамической генерации S-блоков, являющихся важнейшими компонентами современных блочных шифров [19].

В отличие от статических таблиц подстановок, используемых в традиционных алгоритмах, динамические S-блоки могут изменяться в процессе работы алгоритма, что затрудняет проведение линейного и дифференциального криптоанализа.

Защита изображений и мультимедийных данных. Одной из наиболее активно развивающихся областей применения хаотической криптографии является защита цифровых изображений. Это связано с тем, что изображения обладают значительным объемом данных и высокой корреляцией между соседними пикселями, что требует применения специализированных методов защиты [10, 14].

Типичная схема хаотического шифрования изображений включает два этапа:

- 1) Перестановка пикселей.
- 2) Диффузия значений пикселей.

На этапе перестановки изменяется пространственное расположение пикселей изображения. Для этого часто используются отображение Арнольда, отображение Хенона и различные двумерные хаотические карты [14].

На этапе диффузии значения пикселей изменяются с использованием хаотически сгенерированных последовательностей. В результате даже незначительное изменение исходного изображения приводит к существенным изменениям зашифрованных данных.

Современные исследования демонстрируют высокую эффективность гиперхаотических систем при защите изображений. Использование нескольких независимых хаотических последовательностей позволяет



повысить устойчивость алгоритмов к статистическому анализу и атакам на основе известных открытых текстов.

Следует отметить, что большинство современных публикаций в области хаотической криптографии посвящено именно шифрованию изображений, медицинских данных и мультимедийного контента.

Легковесная криптография для устройств Интернета вещей. Развитие технологий Интернета вещей (IoT) обусловило необходимость создания криптографических алгоритмов, пригодных для работы на устройствах с ограниченными вычислительными ресурсами [20].

К таким устройствам относятся:

- беспроводные сенсоры;
- RFID-метки;
- встроенные контроллеры;
- устройства промышленного Интернета вещей.

Для подобных систем важными характеристиками являются:

- низкое энергопотребление;
- минимальные требования к памяти;
- высокая скорость выполнения операций.

Хаотические функции обладают рядом преимуществ, позволяющих использовать их в качестве основы легковесных криптографических решений. В большинстве случаев реализация хаотических отображений требует выполнения ограниченного числа арифметических операций, что снижает вычислительные затраты по сравнению с традиционными алгоритмами.

Таблица 2 – Современные направления применения хаотических функций в криптографии

Направление	Используемые хаотические системы	Основные показатели эффективности
Генерация псевдослучайных чисел	Logistic, Tent, Chebyshev	Энтропия, NIST SP 800-22
Потоковое шифрование	Logistic, Henon, Lorenz	Скорость генерации ключевого потока
Блочное шифрование	Hyperchaotic systems	Лавинный эффект, нелинейность
Шифрование изображений	Arnold, Lorenz, Hyperchaotic	NPCR, UACI, Entropy
Защита IoT	Multi-chaos systems	Энергопотребление, время выполнения
Гибридные схемы с ИИ	Hyperchaos + AI	Адаптивность и устойчивость

Современные исследования показывают, что наибольшее количество публикаций посвящено шифрованию изображений, IoT и гибридным схемам на основе гиперхаоса. Современные исследования демонстрируют



возможность совместного применения хаотических механизмов с легковесными криптографическими примитивами. Особый интерес представляют схемы, в которых хаотические системы используются для генерации ключевого материала и случайных параметров, а непосредственное шифрование осуществляется с использованием стандартизованных алгоритмов.

Подобный подход позволяет сочетать преимущества хаотических систем с доказанной криптографической стойкостью современных алгоритмов защиты информации.

Результаты и обсуждения.

Сравнительный анализ существующих подходов. На основании проведенного обзора можно выделить основные направления использования динамических хаотических функций в криптографии, их преимущества и ограничения [11–20].

Таблица 3 – Сравнение основных направлений применения хаотических функций в криптографии

Направление применения	Основные преимущества	Основные недостатки
Генерация псевдослучайных чисел	Высокая скорость генерации, большое пространство параметров	Зависимость от точности вычислений
Потоковые шифры	Простота реализации, высокая производительность	Возможность восстановления параметров при неудачном выборе карты
Блочные шифры с хаотическими S-блоками	Повышенная нелинейность, динамическая структура	Усложнение реализации
Шифрование изображений	Высокая эффективность для мультимедийных данных	Ограниченная область применения
Легковесная криптография для IoT	Низкие вычислительные затраты	Недостаточная изученность криптостойкости

Проведенный анализ (Таблица 3) показывает, что наиболее перспективными направлениями применения хаотических функций являются генерация псевдослучайных последовательностей и легковесная криптография для устройств Интернета вещей. В данных областях хаотические системы позволяют обеспечить приемлемый уровень безопасности при относительно невысоких вычислительных затратах.

В то же время широкое практическое внедрение хаотических криптосистем сдерживается отсутствием строгих математических доказательств стойкости, характерных для современных стандартизованных криптографических алгоритмов.



Таблица 4 – Тенденции развития хаотической криптографии (2021–2025 гг.)

Период	Основное направление исследований	Характерные особенности
2021–2022	Классические хаотические карты	Logistic, Henon, Tent
2022–2023	Многослойные схемы шифрования	Перестановка и диффузия
2023–2024	Гиперхаотические системы	Увеличение пространства ключей
2024–2025	IoT и легковесная криптография	Минимизация вычислительных затрат
2025–2026	Интеграция с ИИ и постквантовыми решениями	Адаптивные и гибридные системы

Анализ публикаций последних лет показывает рост интереса к гиперхаотическим системам, многокарточным (multi-chaos) схемам, интеграции хаоса с искусственным интеллектом и решениям для Интернета вещей [15, 18, 20].

Проблемы и перспективы развития хаотической криптографии. Несмотря на значительное количество исследований, посвященных применению динамических хаотических функций в криптографии, их широкое практическое внедрение сталкивается с рядом ограничений. Одной из основных проблем является влияние конечной точности вычислений на поведение хаотических систем. В отличие от теоретических моделей, функционирующих в непрерывном пространстве состояний, реальные вычислительные устройства используют конечное число разрядов для представления данных. В результате возможно появление периодических циклов и снижение уровня хаотичности генерируемых последовательностей [6, 11].

Другим существенным недостатком является отсутствие строгих математических доказательств криптографической стойкости большинства хаотических алгоритмов. Современные стандартизованные криптографические системы, такие как AES, SHA-3 и алгоритмы постквантовой криптографии, основываются на хорошо изученных математических задачах, безопасность которых подтверждается многолетними исследованиями. В большинстве хаотических схем оценка стойкости осуществляется преимущественно на основе статистических тестов и экспериментальных исследований [6, 11, 13].

Кроме того, эффективность хаотических криптосистем существенно зависит от выбора параметров используемой динамической системы. Некорректный выбор начальных условий или управляющих коэффициентов может привести к возникновению предсказуемых режимов функционирования и снижению уровня безопасности [6].

Несмотря на указанные ограничения, результаты современных исследований свидетельствуют о сохранении высокого интереса к хаотической криптографии. В настоящее время наиболее активно развиваются следующие направления:



- использование гиперхаотических систем высокой размерности;
- разработка многослойных криптографических схем на основе нескольких хаотических отображений;
- применение хаотических функций в легковесной криптографии для устройств Интернета вещей;
- создание динамических S-блоков и генераторов псевдослучайных чисел;
- интеграция хаотических механизмов с технологиями искусственного интеллекта;
- использование хаотических систем совместно с постквантовыми криптографическими алгоритмами [15, 18–20].

Особый интерес представляет возможность применения хаотических функций в качестве дополнительного механизма формирования ключевого материала и генерации случайных последовательностей для постквантовых криптографических схем. Такой подход позволяет объединить преимущества хаотических динамических систем и современных криптографических примитивов, обладающих доказанной стойкостью к атакам квантовых вычислителей [18, 20].

Заключение.

В работе проведен обзор современных подходов к применению динамических хаотических функций в криптографии. Рассмотрены основные свойства хаотических систем, включая чувствительность к начальным условиям, нелинейность, эргодичность и псевдослучайность, определяющие возможность их использования для защиты информации.

Показано, что хаотические функции находят применение в генераторах псевдослучайных чисел, симметричных алгоритмах шифрования, системах защиты изображений и легковесных криптографических решениях для устройств Интернета вещей. Анализ современных исследований свидетельствует о постепенном переходе от простых одномерных хаотических отображений к многомерным и гиперхаотическим системам, обеспечивающим более высокий уровень криптографической стойкости.

Установлено, что наиболее перспективными направлениями развития являются использование гиперхаотических систем, создание гибридных криптографических схем и интеграция хаотических механизмов с постквантовыми алгоритмами защиты информации. При этом дальнейшие исследования должны быть направлены на разработку методов формального доказательства безопасности хаотических криптосистем и оценку их устойчивости к современным методам криптоанализа.

Таким образом, динамические хаотические функции представляют собой перспективный инструмент построения криптографических механизмов нового поколения и могут использоваться для повышения эффективности и безопасности систем защиты информации в условиях дальнейшего развития цифровых технологий.

**СПИСОК ЛИТЕРАТУРЫ**

1. Shannon C.E. Communication Theory of Secrecy Systems // Bell System Technical Journal. – 1949. – Vol. 28, No. 4. – P. 656–715.
2. Matthews R. On the Derivation of a Chaotic Encryption Algorithm // Cryptologia. – 1989. – Vol. 13, No. 1. – P. 29–42.
3. Baptista M.S. Cryptography with Chaos // Physics Letters A. – 1998. – Vol. 240. – P. 50–54.
4. Fridrich J. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps // International Journal of Bifurcation and Chaos. – 1998. – Vol. 8, No. 6. – P. 1259–1284.
5. Kocarev L. Chaos-Based Cryptography: A Brief Overview // IEEE Circuits and Systems Magazine. – 2001. – Vol. 1, No. 3. – P. 6–21.
6. Alvarez G., Li S. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems // International Journal of Bifurcation and Chaos. – 2006. – Vol. 16, No. 8. – P. 2129–2151.
7. Strogatz S.H. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry and Engineering. – Boulder: Westview Press, 2018. – 498 p.
8. Devaney R.L. An Introduction to Chaotic Dynamical Systems. – New York: CRC Press, 2018. – 336 p.
9. Hua Z., Zhou Y. Dynamic Chaotic System for Image Encryption // Signal Processing. – 2020. – Vol. 175. – Article 107629.
10. Wang X., Zhang H., Bao X. A Novel Hyperchaotic Image Encryption Algorithm Based on DNA Encoding and Chaos // Multimedia Tools and Applications. – 2021. – Vol. 80. – P. 19687–19712.
11. Farhan A.K., Ali A.H., Hasson N.K. Chaos-Based Cryptography: A Survey on Present State and Future Directions // Journal of Information Security and Applications. – 2021. – Vol. 59. – Article 102837.
12. Abd El-Latif A.A., Niu X., Wang L. Efficient Chaos-Based Cryptosystem for Secure Communications // IEEE Access. – 2022. – Vol. 10. – P. 25248–25261.
13. Alawida M., Samsudin A., Teh J.S. A Survey on Chaos-Based Cryptosystems: Implementations and Applications // Mathematics. – 2022. – Vol. 10, No. 18. – Article 3308.
14. Zhang Y., Li C., Ou R. Survey on Image Encryption Techniques Using Chaotic Maps in Spatial Transform and Spatiotemporal Domains // International Journal of Network Security. – 2022. – Vol. 24, No. 5. – P. 835–850.
15. Bhatia S., Sood S.K. Lightweight Chaos-Based Security Mechanisms for Internet of Things: A Review // Journal of King Saud University – Computer and Information Sciences. – 2023. – Vol. 35, No. 6. – P. 101622.
16. Hameed A., Mahmood A., Khalaf O. A Review of Chaotic Maps Used for Generating Secure Random Keys // BIO Web of Conferences. – 2024. – Vol. 119. – Article 00070.



17. Naskar P., Roy S. Robust Chaotic Tent Map-Based Cryptographically Secure Pseudorandom Number Generator // arXiv. – 2024. – arXiv:2408.05580.
18. Wang J., Liu Y., Chen X. Hyperchaotic Systems in Modern Cryptography: Recent Advances and Challenges // Entropy. – 2025. – Vol. 27, No. 3. – Article 215.
19. Zhang L., Wu H. Dynamic S-Box Construction Using Hyperchaotic Systems for Symmetric Encryption // Electronics. – 2025. – Vol. 14, No. 11. – Article 2198.
20. Kumar R., Sharma P. Chaos-Based Lightweight Cryptography for IoT Devices: Current Trends and Future Perspectives // Peer-to-Peer Networking and Applications. – 2025. – Vol. 18. – P. 1452–1471.

Әсел Жүнісхан, докторант, Farabi University, Алматы, Қазақстан, assel.zhuniskhan@gmail.com

Қайрат Сақан, PhD, Institute of Information and Computational Technologies CS MSHE RK, Алматы, Қазақстан, kairat_sks@mail.ru

Марат Джакипбеков, профессор, полковник, National Defence University of the Republic of Kazakhstan, Астана, Қазақстан, kazei.72@mail.ru

КРИПТОГРАФИЯДАҒЫ ДИНАМИКАЛЫҚ ХАОТИКАЛЫҚ ФУНКЦИЯЛАРДЫ ҚОЛДАНУ: ҚАЗІРГІ ЖАҒДАЙЫ ЖӘНЕ ДАМУ БОЛАШАҒЫ

Аңдатпа. Мақалада криптографияда динамикалық хаостық функцияларды қолданудың заманауи тәсілдеріне шолу жасалған. Ақпаратты қорғау мақсатында пайдалануға мүмкіндік беретін хаостық жүйелердің негізгі қасиеттері, атап айтқанда бастапқы шарттарға сезімталдық, эргодикалылық, сызықтық еместік және жалған кездейсоқтық қарастырылған. Жалған кездейсоқ тізбектерді генерациялау, симметриялық шифрлау, кескіндерді қорғау және Заттар интернеті құрылғыларына арналған жеңілдетілген криптография сияқты криптографиялық алгоритмдерде хаостық бейнелеулерді қолданудың негізгі бағыттарына талдау жүргізілген. Сонымен қатар хаостық криптожүйелердің негізгі артықшылықтары мен шектеулері, сондай-ақ посткванттық есептеулердің пайда болуы жағдайындағы олардың одан әрі даму перспективалары айқындалған.

Түйінді сөздер: ақпаратты қорғау, хаостық жүйелер, динамикалық функциялар, хаостық бейнелеулер, кілттерді генерациялау, жалған кездейсоқ тізбектер, ақпараттық қауіпсіздік.



Assel Zhuniskhan, doctoral student, Farabi University, Almaty, Kazakhstan, assel.zhuniskhan@gmail.com

Sakan Kairat, PhD, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, kairat_sks@mail.ru

Marat Dzhakipbekov, professor, Colonel, National Defence University of the Republic of Kazakhstan, Astana, Kazakhstan, kazei.72@mail.ru

APPLICATION OF DYNAMIC CHAOTIC FUNCTIONS IN CRYPTOGRAPHY: CURRENT STATE AND PROSPECTS FOR DEVELOPMENT

Abstract. This paper presents a review of modern approaches to the application of dynamic chaotic functions in cryptography. The main properties of chaotic systems that enable their use for information protection, including sensitivity to initial conditions, ergodicity, nonlinearity, and pseudorandomness, are considered. An analysis of existing applications of chaotic maps in cryptographic algorithms is carried out, including pseudorandom sequence generation, symmetric encryption, image protection, and lightweight cryptography for Internet of Things devices. The main advantages and limitations of chaos-based cryptosystems are identified, and the prospects for their further development in the era of post-quantum computing are discussed.

Keywords: information protection, chaotic systems, dynamic functions, chaotic maps, key generation, pseudorandom sequences, information security.

Поступила: 01 июля 2026 года

Рецензирована: 03 августа 2026 года

Принята: 18 августа 2026 года