УДК: 519.86, 004.94, 004.056, 004.89 DOI: 10.65599/III7273

DDoS-АТАКИ: ИСТОРИЧЕСКИЙ АНАЛИЗ, СТАТИСТИЧЕСКАЯ ДИНАМИКА

Дж.Ш. Рахматов

Центр инновационного развития науки и цифровых технологий НАНТ

Статья анализирует эволюцию распределённых атак отказа в обслуживании (DDoS) от первых демонстрационных экспериментов до современных многоуровневых угроз, инициируемых IoT-ботнетами и облачными сервисами. Показан экспоненциальный рост мощности атак и усложнение их структуры. Предложена гибридная модель прогнозирования, объединяющая логистическую динамику и марковские процессы, что позволяет описывать как количественную эскалацию, так и вероятностные переходы между типами атак. Практическая значимость заключается в рекомендациях по внедрению интеллектуальных систем защиты на основе машинного обучения и нечеткой логики, обеспечивающих устойчивость цифровой инфраструктуры в условиях роста киберугроз.

Ключевые слова: *DDoS-атаки, IoT-ботнеты, логистическая модель, марковская цепь, кибербезопасность, машинное обучение, нечёткая логика.*

DDoS-ҲУҶУМҲО: ТАҲЛИЛИ ТАРИХӢ, ДИНАМИКАИ ОМОРӢ

Дж.Ш. Рахматов

Мақола эволютсияи ҳамлаҳои DDoS-ро аз таҷрибаҳои ибтидоӣ то таҳдидҳои мураккаби муосир, ки аз ботнетҳои IoT ва хизматрасониҳои абрӣ сарчашма мегиранд, таҳлил мекунад. Афзоиши экспоненсиалии иқтидори ҳамлаҳо ва мураккабшавии сохтори онҳо нишон дода мешавад. Модели гибридии пешгӯӣ пешниҳод шудааст, ки динамикаи логистикиро бо занҷирҳои Марков муттаҳид мекунад ва ҳам афзоиши миқдорӣ ва ҳам гузаришҳои эҳтимолиро байни намудҳои ҳамлаҳо инъикос менамояд. Арзиши амалӣ дар тавсияҳо оид ба истифодаи системаҳои муҳофизати мутобиқшаванда, ки омӯзиши мошинӣ ва мантиқии норавшанро муттаҳид месозанд, ифода меёбад.

Калидвожаҳо*: ҳамлаҳои DdoS, ботнетҳои IoT, модели логистикӣ, занҷирҳои Марков, амнияти киберӣ, омӯзиши мошинӣ, мантиқии норавшан.*

DDoS-ATTACKS: HISTORICAL ANALYSIS, STATISTICAL DYNAMICS

J.Sh. Rahmatov

The paper analyzes the evolution of Distributed Denial of Service (DDoS) attacks, from early demonstrations to modern multi-layered threats driven by IoT botnets and cloud services. It highlights the exponential growth in attack power and the increasing complexity of their structure. A hybrid forecasting model is introduced, combining logistic dynamics with Markov chains to capture both quantitative escalation and probabilistic transitions between attack types. The practical contribution lies in recommendations for adaptive defense systems based on machine learning and fuzzy logic, aimed at ensuring resilience of digital infrastructure under escalating cyber threats.

Keywords: *DDoS attacks, IoT botnets, Logistic growth model, Markov chains, Cybersecurity, Machine learning, Fuzzy logic.*

Введение

За последние два десятилетия распределённые атаки отказа в обслуживании (Distributed Denial of Service, DDoS) стали одной из главных угроз цифровой инфраструктуре. Даже кратковременные перебои могут иметь серьёзные последствия для экономики и политики [1, 4, 5]. Эволюция атак показывает переход от локальных экспериментов к действиям организованных групп, использующих ботнеты и IoT-устройства [6, 9]. Статистическая динамика фиксирует рост мощности атак до терабит в секунду, что требует новых методов моделирования и прогнозирования [2, 14, 15]. Современные методы противодействия всё чаще опираются на гибридные технологии: машинное обучение, поведенческий анализ, адаптивные системы фильтрации, основанные на нечеткой логике, а также распределённые подходы на основе блокчейн [3, 7, 8, 10, 11, 12]. Также проблемы кибербезопасности и модели развития эпидемий были изучены в работах [14-17].

Цель данной работы — провести комплексный анализ DDoS-атак в трёх взаимосвязанных измерениях: историческом, статистическом и технологическом. Научная новизна заключается в интеграции ретроспективного анализа с формальными моделями динамики атак и предложением гибридного подхода к противодействию, сочетающего методы машинного обучения и нечеткой логики.Таким образом, статья призвана не только систематизировать накопленный опыт, но и предложить оригинальные решения для повышения устойчивости цифровых систем в условиях эскалации киберугроз.

Исторический анализ DDoS-атак

Эволюция DDoS-атак демонстрирует закономерный переход от локальных экспериментов к глобальным кибероперациям. Первые задокументированные случаи конца 1990-х – начала 2000-х годов носили демонстрационный характер: атаки на крупные интернет-порталы осуществлялись с помощью примитивных скриптов и имели ограниченную мощность [6] (табл. 1).

В период 2003–2010 гг. наступила «эра ботнетов». Массовое распространение вредоносных программ позволило формировать распределённые сети заражённых компьютеров, что превратило DDoS в инструмент киберпреступности. В этот же период появились специализированные программы, доступные даже непрофессионалам, а мощность атак достигла сотен мегабит и гигабит в секунду, угрожая банковским и государственным системам [9].

Ключевым рубежом стала атака ботнета Mirai в 2016 году, использовавшего уязвимые IoT-устройства. Она привела к масштабным перебоям в работе глобальных сервисов и впервые продемонстрировала мощность свыше 1 Тбит/с, обозначив новую фазу угроз [4], [6].

Современный этап (2017–2025 гг.) характеризуется дальнейшим ростом мощности атак до 3–4 Тбит/с, усложнением их структуры и политизацией. Появление сервисов «DDoS-as-a-Service» сделало атаки доступными широкому кругу злоумышленников, а использование облачных технологий и многоуровневых методов превратило их в инструмент кибервойн и геополитического давления [13], [14].

Таблица 1– Ключевые этапы эволюции DDoS-атак

Период	Характеристика этапа	Технологии / примеры	Мощность атак	Целевые объекты	Особенности / контекст
1999–2002	Первые атаки на порталы	Скрипты, flood-инструменты	Десятки Мбит/с	Крупные интернет-порталы	Демонстрационный характер
2003–2010	Эра ботнетов, коммерциализация	Trinoo, LOIC, DDoS-for-ransom	Сотни Мбит/с – Гбит/с	Банки, гос. сайты	Вымогательство, первые политические мотивы
2016	IoT-революция, Mirai	IoT-устройства, Mirai	>1 Тбит/с	Dyn, Twitter, Netflix	Массовые перебои, глобальный резонанс
2017–2025	Современный этап	DDoS-as-a-Service, облачные атаки	3–4 Тбит/с и выше	Критическая инфраструктура, облачные сервисы	Политизация, использование в кибервойнах

Таким образом, историческая динамика отражает переход от хаотичных экспериментов к высокотехнологичным и целенаправленным операциям, напрямую связанным с развитием цифровых технологий и ростом уязвимости глобальной инфраструктуры.

Выводы исторического анализа. Эволюция DDoS-атак демонстрирует закономерный переход от хаотичных экспериментов к систематизированным и высокотехнологичным операциям. Каждое новое поколение атак связано с технологическим скачком: от персональных компьютеров к ботнетам, от ботнетов к IoT, а сегодня — к облачным и распределённым системам (табл. 1).

Статистическая динамика DDoS-атак

За последние два десятилетия мощность DDoS-атак выросла экспоненциально: от десятков мегабит в начале 2000-х до сотен гигабит в 2010-х. Атака ботнета Mirai в 2016 году превысила 1 Тбит/с, а к 2025 году зафиксированы случаи свыше 3–4 Тбит/с [2], [4], [6], [14], [15]. Прогнозы указывают на достижение 5–6 Тбит/с к 2030 году с тенденцией к насыщению.

Структура атак усложняется: volumetric остаются доминирующими, но растёт доля прикладных атак, а протокольные эксплойты сохраняют значимость [2], [5]. Для описания динамики применяются логистические модели и марковские процессы, позволяющие прогнозировать как рост интенсивности, так и вероятностные переходы между типами атак [3], [12], [14].

Таким образом, статистическая динамика отражает нелинейный рост, глобальное распространение и усложнение структуры, что требует адаптивных моделей прогнозирования и интеллектуальных систем защиты.

Таблица 2 – Статистическая динамика DDoS-атак

Показатель	Характеристика	Примеры / данные	Прогноз (2026–2030)
Мощность атак	Экспоненциальный рост	2000-е: десятки Мбит/с; 2010-е: сотни Гбит/с; 2016: >1 Тбит/с; 2025: 3–4 Тбит/с	До 5–6 Тбит/с, насыщение к 2030 г.
География	Глобальный характер	Азия, Восточная Европа	Рост активности в Африке и Латинской Америке
Типология	Разнообразие форм	Volumetric, Application-layer, Protocol exploits	Доминирование сложных атак на прикладном уровне
Моделирование	Формальные модели	Логистическая динамика, марковские процессы	Адаптивные модели с ML-параметрами
Закономерности	Сокращение длительности атак	«Тяжёлый хвост» распределения мощности	Рост кратковременных, но сверхмощных атак

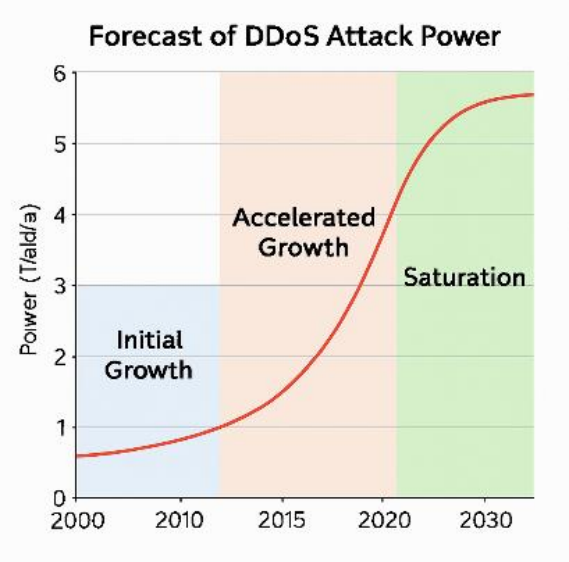

Рисунок 1– График прогноза динамики мощности DDoS-атак до 2030 года

График на Рис. 1 демонстрирует три фазы эволюции мощности атак:

Фаза начального роста (2000–2010) — линейное увеличение до ~0.5 Тбит/с, обусловленное ограниченными ресурсами и примитивными инструментами;

Фаза экспоненциального роста (2011–2025) — резкий скачок мощности до 3–4 Тбит/с, вызванный распространением IoT-ботнетов и облачных платформ;

Фаза насыщения (2026–2030) — замедление роста до 5–6 Тбит/с, отражающее физические ограничения и усиление систем защиты.

Ключевые точки:

- 2016 — атака Mirai (>1 Тбит/с), переход к фазе экспоненциального роста;
- 2025 — пик мощности 3–4 Тбит/с;
- 2030 — прогнозируемое насыщение на уровне 5–6 Тбит/с.

Эта визуализация подтверждает необходимость перехода от статических средств защиты к адаптивным системам, способным учитывать как количественную эскалацию, так и структурные трансформации угроз.

Региональные особенности распространения DDoS-атак

Анализ географии DDoS-атак показывает, что их распределение по регионам мира носит неравномерный характер и тесно связано с уровнем цифровизации, доступностью уязвимых устройств и политической напряжённостью.

1. Азия и Восточная Европа — эпицентры активности: высокая концентрация атак наблюдается в странах Азии (Китай, Индия, Вьетнам) и Восточной Европы (Россия, Украина, Польша), где массово используются уязвимые IoT-устройства и дешёвые хостинговые ресурсы; в этих регионах часто фиксируются volumetric-атаки, направленные на перегрузку сетевой инфраструктуры, а также атаки с политическим подтекстом [19].

2. Северная Америка и Западная Европа — цели высокотехнологичных атак: в США, Канаде, Великобритании и Германии преобладают сложные прикладные и протокольные атаки, направленные на облачные сервисы, финансовые платформы и государственные ресурсы; здесь наблюдается активное развитие систем защиты, включая ML-механизмы, edge-фильтрацию и блокчейн-интеграцию [20].

3. Африка и Латинская Америка — растущие зоны риска: в этих регионах пока фиксируется низкая интенсивность атак, но прогноз указывает на рост активности в связи с расширением цифровой инфраструктуры и слабой киберзащитой; особенно уязвимы государственные порталы, образовательные платформы и телекоммуникационные узлы [18].

Таким образом можно подчеркнуть, что региональный анализ подтверждает, что DDoS-угрозы эволюционируют не только по мощности и структуре, но и по географическому охвату. Это требует разработки локализованных стратегий защиты, учитывающих специфику инфраструктуры, типы атак и уровень зрелости киберсреды в каждом регионе.

Научная новизна и вклад

Работа объединяет исторический анализ DDoS-атак с формальными моделями их статистической динамики, что позволяет выявить закономерности эволюции угроз и связать их с современными тенденциями.

Гибридная модель прогнозирования включает два взаимодополняющих компонента:

1.Логистическая динамика роста числа атак

$$\frac{dN(t)}{dt} = \alpha N(t) - \beta N(t)^2$$

где $N(t)$ — количество атак в момент времени, α — скорость появления новых атак, β — коэффициент противодействия.

-Параметр α отражает интенсивность генерации угроз и может оцениваться на основе статистики прироста числа атак (например, ежегодные отчёты CERT, Arbor Networks).

-Параметр β характеризует эффективность мер защиты и насыщение инфраструктуры, оцениваемое по снижению успешных атак.

Практическая ценность заключается в возможности регулярной калибровки этих параметров на основе реальных данных, что делает модель адаптивной и применимой в SIEM-системах.

2.Марковская модель переходов между типами атак

$$P = \begin{bmatrix} 0.6 & 0.3 & 0.1 \\ 0.2 & 0.6 & 0.2 \\ 0.1 & 0.3 & 0.6 \end{bmatrix}$$

где элементы матрицы P_{ij} отражают вероятности трансформации volumetric-атак в прикладные или протокольные, а также обратные переходы.

Элементы матрицы переходов P определяются эмпирически на основе частотного анализа статистики инцидентов. Три состояния марковской цепи соответствуют трём доминирующим типам атак: объёмным (volumetric, S_1), прикладным (application-layer, S_2) и протокольным (protocol, S_3). Вероятность перехода p^l_j вычисляется как относительная частота: $p^l_j = n^l_j / n^l$, где n^l_j — число зафиксированных переходов из типа i в тип j за анализируемый период, а n^l — общее число наблюдений атак типа i. Источниками данных служат ежегодные отчёты Cloudflare, Akamai и CERT-организаций, содержащие долю и смену категорий атак по периодам. Условие стохастичности строк ($\sum_j p^l_j = 1$) гарантирует корректность вероятностной интерпретации. Для учёта динамики угроз матрица P пересчитывается по скользящему временному окну длиной 3–5 лет, что обеспечивает актуальность параметров модели и позволяет своевременно отражать изменения в структуре атак.

- Вероятности P_{ij} подлежат регулярному обновлению на основе статистики инцидентов (например, отчёты Cloudflare, Akamai).
- Использование скользящего окна (3–5 лет) позволяет учитывать динамику изменения структуры атак.
- Пример: рост прикладных атак в 2020–2025 гг. увеличил вероятность перехода volumetric → application до 0.35, что отражает тенденцию к усложнению угроз.

Совместное использование логистической и марковской моделей обеспечивает прогнозирование не только интенсивности атак, но и их структурных трансформаций. Практическая ценность заключается в возможности адаптивного обновления параметров α, β, P_{ij} на основе реальных данных, что делает модель применимой в интеллектуальных системах защиты, интегрирующих машинное обучение и нечеткую логику.

Таким образом, статья вносит вклад в развитие методов прогнозирования DDoS-угроз, предлагая оригинальное решение для анализа их количественной динамики и вероятностной трансформации, а также формируя основу для построения устойчивой цифровой инфраструктуры.

Таблица 3 – Примеры параметров логистической и марковской моделей для разных периодов

Период	**Параметр α (скорость появления атак)**	**Параметр β (эффект противодействия)**	**Пример вероятностей переходов (P_{ij})**	**Интерпретация**
2000–2005	0.05–0.08	0.02–0.03	Volumetric → Application: 0.15; Volumetric → Protocol: 0.05	Низкая интенсивность атак, слабая защита, доминирование volumetric-форм
2010–2015	0.10–0.12	0.04–0.05	Volumetric → Application: 0.25; Application → Protocol: 0.10	Рост ботнетов, усиление прикладных атак, первые адаптивные фильтры
2016–2020	0.15–0.18	0.05–0.06	Volumetric → Application: 0.30; Protocol → Application: 0.20	Эра IoT-ботнетов, усложнение структуры, появление ML-методов защиты
2021–2025	0.18–0.20	0.06–0.07	Volumetric → Application: 0.35; Application → Protocol: 0.20	Массовые облачные атаки, рост прикладных угроз, внедрение SIEM-систем
Прогноз 2026–2030	0.20–0.22	0.07–0.08	Volumetric → Application: 0.40; Application → Protocol: 0.25	Усиление прикладных и протокольных атак, необходимость международной координации

Примеры значений параметров α, β и вероятностей переходов P_{ij} для разных периодов развития DDoS-атак приведены в таблице 3. Они демонстрируют рост интенсивности атак и усложнение их структуры, а также необходимость регулярной калибровки модели на основе статистики реальных инцидентов. Такой подход позволяет адаптировать прогнозы к изменяющимся условиям и использовать их в интеллектуальных системах защиты.

Модель (рис. 2) включает логистическую динамику роста интенсивности атак и марковскую модель переходов между типами угроз. Интеграция этих компонентов позволяет адаптировать прогнозы к реальным данным и использовать их в интеллектуальных системах защиты, основанных на машинном обучении и нечеткой логике.

Практическое применение:

-Прогноз позволяет заранее адаптировать архитектуру защиты.

-Модель может быть встроена в SIEM-системы для оценки риска.

-Использование адаптивных порогов фильтрации на основе вероятностных переходов.

Рисунок 2 – Схема гибридной модели прогнозирования DDoS-атак.

Заключение

Проведённое исследование показало, что DDoS-атаки представляют собой динамично развивающийся феномен, тесно связанный с технологическими изменениями и глобальными процессами цифровизации. Исторический анализ выявил закономерный переход от примитивных скриптов к ботнетам, от ботнетов к IoT-экосистемам, а затем к облачным и распределённым платформам, что сопровождается экспоненциальным ростом мощности атак. Статистическая динамика подтверждает нелинейный характер эскалации угроз и усложнение их структуры, требующее применения адаптивных моделей прогнозирования. Предложенная гибридная модель, основанная на сочетании логистической динамики и марковских процессов, обеспечивает возможность предсказания как количественных параметров атак, так и их вероятностных трансформаций. Практическая значимость работы заключается в обосновании необходимости перехода к интеллектуальным системам защиты, интегрирующим машинное обучение, нечеткую логику и распределённые технологии. В перспективе 2026–2030 гг. ожидается усиление прикладных и протокольных атак, что делает актуальным формирование международно-координированных стратегий кибербезопасности и развитие устойчивых архитектур цифровой инфраструктуры.

Рецензент: Акрамов М.Б. – к.ф.-м.н., доцент, зав.лабораторией Центра инновационного развития науки и цифровых технологий НАНТ.

Литература

1. Parihar V.C., Prasad S.N., Kounte M.R., Sai Prabhu K.B. Mitigating the Threat of DDoS Attacks: Emerging Strategies and Algorithms // Intelligent Control, Robotics, and Industrial Automation. RCAAI 2024. Lecture Notes in Electrical Engineering. Vol. 1492. Singapore: Springer, 2026. P. — DOI: 10.1007/978-981-95-2901-8_33.

2. Yin D., Zhang L., Yang K. A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework // IEEE Access. 2018. Vol. 6. P. 24694–24705. DOI: 10.1109/ACCESS.2018.2831284.

3. Ibrahim El Sayed A., Abdelaziz M., Hussein M., Elbayoumy A.D. DDoS Mitigation in IoT Using Machine Learning and Blockchain Integration // IEEE Networking Letters. 2024. Vol. 6, No. 2. P. 152–155. DOI: 10.1109/LNET.2024.3377355.

4. Pandey N., Mishra P.K. A Survey on DDoS Attacks on Network and Application Layer in IoT // Advanced Network Technologies and Intelligent Computing. CCIS. Vol. 1534. Cham: Springer, 2022. DOI: 10.1007/978-3-030-96040-7_19.

5. Hussain F., Hussain R., Hassan S.A., Hossain E. Machine Learning in IoT Security: Current Solutions and Future Challenges // IEEE Communications Surveys & Tutorials. 2020. Vol. 22, No. 3. P. 1686–1721. DOI: 10.1109/COMST.2020.2986444.

6. Kolias C., Kambourakis G., Stavrou A., Voas J. DDoS in the IoT: Mirai and Other Botnets // Computer. 2017. Vol. 50, No. 7. P. 80–84. DOI: 10.1109/MC.2017.201.

7. Rehman Z., Gondal I., Ge M., Dong H., Gregory M., Tari Z. Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception // Computers & Security. 2024. Vol. 139. 103685. DOI: 10.1016/j.cose.2023.103685.
8. Chaira M., Belhenniche A., Chertovskih R. Enhancing DDoS Attacks Mitigation Using Machine Learning and Blockchain-Based Mobile Edge Computing in IoT // Computation. 2025. Vol. 13. 158. DOI: 10.3390/computation13070158.
9. Ahmed M., Mahmood A.N., Hu J. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. 2016. Vol. 60. P. 19–31. DOI: 10.1016/j.jnca.2015.11.016.
10. Badamasi U., Khaliq S., Babalola O., Shafiu M., Iqbal T. A Deep Learning based approach for DDoS attack detection in IoT-enabled smart environments // Machine Learning. 2020. P. 93–99.
11. Singh A., Gupta B.B. Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms // International Journal on Semantic Web and Information Systems. 2022. Vol. 18, No. 1. DOI: 10.4018/IJSWIS.297143.
12. Jia Y., Zhong F., Alrawais A., Gong B., Cheng X. FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks // IEEE Internet of Things Journal. 2020. Vol. 7, No. 10. P. 9552–9562. DOI: 10.1109/JIOT.2020.2993782.
13. Gelgi M., Guan Y., Arunachala S., Rao M.S.S., Dragoni N. Systematic Literature Review of IoT Botnet DDoS Attacks and Evaluation of Detection Techniques // Sensors. 2024. Vol. 24. 3571. DOI: 10.3390/s24113571.
14. Ilolov M., Kuchakshoev K., Mirshahi M., Rahmatov J.Sh. Nonlinear stochastic equation in epidemiology // Global and Stochastic Analysis. 2023. Vol. 10, No. 3. P. 75–84.
15. Рахматов Дж.Ш. Фишинг и кибератаки: исторический анализ, статистическая динамика и современные методы противодействия // Известия Национальной академии наук Таджикистана. Отд. физ.-мат., хим., геол. и техн. наук. 2025. № 3 (200). С. 67–74.
16. Илолов М., Рахматов Дж.Ш. Применение нечетких дифференциальных уравнений для анализа и прогнозирования кибератак // Доклады Национальной академии наук Таджикистана. 2025. Т. 68. № 8. С. 743–749.
17. Rahmatov J.Sh. Fuzzy Differential Equations: Applications for Analyzing and Predicting Cyberattacks // Journal of Applied Data Analysis and Modern Stochastic Modelling. 2025. Vol. 2, No. 2. P. 53–58.
18. Geo-blocking DDoS attacks. URL: https://vercara.digicert.com/resources/geo-blocking-ddos-attacks (дата обращения: 18.03.2026).
19. NETSCOUT DDoS Threat Intelligence Report 1H 2025. URL: https://www.netscout.com/threatreport/wp-content/uploads/2025/08/NETSCOUT-DDoS-Threat-Intelligence-Report-1H-2025.pdf (дата обращения: 18.03.2026).
20. Cloudflare Radar DDoS Report 2023 Q4. URL: https://radar.cloudflare.com/reports/ddos-2023-q4 (дата обращения: 18.03.2026).

МАЪЛУМОТ ДАР БОРАИ МУАЛЛИФ – СВЕДЕНИЯ ОБ АВТОРЕ – INFORMATION ABOUT AUTHOR

TJ	RU	EN
Раҳматов Ҷамшед Шавкатович	Рахматов Джамшед Шавкатович	Rahmatov Jamshed Shavkatovich
номзади илмҳои физикаю математика, муовини директор оид ба илм	кандидат физико-математических наук, заместитель директора по науке	Candidate of Physical and Mathematical Sciences, Deputy Director for Science
Маркази рушди инноватсионии илм ва технологияҳои рақамӣ, АМИТ	Центр инновационного развития науки и цифровых технологий НАНТ	Center for Innovative Development of Science and Digital Technologies, NAST
E-mail: jamesd007@rambler.ru		