УДК 33 **DOI: 10.34670/AR.2026.17.73.051**

Генераторы псевдослучайных чисел в защите информации: экономические аспекты технологического развития и перспективы инноваций

Грушицын Александр Степанович

Преподаватель кафедры информационной безопасности,
Университет «Синергия»,
125190, Российская Федерация, Москва, Ленинградский просп., 80, корп. Г;
e-mail: nicifor@bk.ru

Аннотация

В статье проводится комплексный анализ экономических аспектов применения генераторов псевдослучайных последовательностей (ГПСЧ) в современных криптографических системах. Рассматривается ключевая дилемма выбора между криптостойкостью, производительностью и совокупной стоимостью владения. На конкретных примерах, таких как поточный шифр ChaCha20, механизм соления паролей и регистры сдвига с линейной обратной связью (РСЛОС), исследуются модели, обеспечивающие оптимальное соотношение безопасности и экономической эффективности в различных сценариях. Отдельное внимание уделено перспективному направлению квантовой генерации случайных чисел (QRNG), анализируются экономические барьеры и потенциал данного рынка. Доказывается, что выбор криптографических примитивов является стратегическим экономическим решением, требующим учета прямых и косвенных издержек, долгосрочных рисков и тенденций технологического развития. Результаты исследования демонстрируют, что корректный выбор ГПСЧ позволяет значительно снизить капитальные (CAPEX) и операционные (OPEX) расходы, минимизировать риски дорогостоящих инцидентов безопасности и обеспечить устойчивость инфраструктуры к будущим вызовам, таким как развитие квантовых вычислений. Работа подводит к выводу о необходимости интеграции экономического анализа в процесс проектирования и аудита криптографических систем на самых ранних этапах.

Для цитирования в научных исследованиях

Грушицын А.С. Генераторы псевдослучайных чисел в защите информации: экономические аспекты технологического развития и перспективы инноваций // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 12А. С. 618-625. DOI: 10.34670/AR.2026.17.73.051

Ключевые слова

экономическая эффективность криптографии, генератор псевдослучайных чисел (ГПСЧ), ChaCha20, регистр сдвига с линейной обратной связью (РСЛОС), криптографическая соль, квантовый генератор случайных чисел (QRNG), совокупная стоимость владения (TCO), операционные расходы (OPEX), капитальные затраты (CAPEX), постквантовая криптография, управление рисками.

Введение

В современной экономике, где данные становятся стратегическим активом, стоимость утечки информации может исчисляться миллиардами долларов. Согласно отчету IBM Cost of a Data Breach Report 2024, средняя стоимость утечки данных в 2023 году в мире достигла 4,45 млн USD, что подчеркивает необходимость надежных механизмов защиты.

Основная часть

Интеграция криптографических механизмов в цифровую инфраструктуру представляет собой критически важный элемент обеспечения информационной безопасности в современной экономике. Среди множества компонентов этих механизмов особое место занимают алгоритмы, основанные на генерации псевдослучайных последовательностей (ПСП), поскольку они лежат в основе таких фундаментальных процессов, как шифрование данных, аутентификация сторон, создание криптографических ключей и хеширование конфиденциальной информации. Экономическая целесообразность внедрения и эксплуатации подобных алгоритмов определяется не изолированным параметром криптографической стойкости, а сложным балансом между уровнем безопасности, совокупной стоимостью реализации, включая аппаратные и программные издержки, показателями энергоэффективности, быстродействием и степенью совместимости с уже развернутыми технологическими платформами. Таким образом, выбор конкретного криптографического решения трансформируется из сугубо технической задачи в стратегическое экономическое решение, требующее анализа долгосрочных эксплуатационных расходов (OPEX), капитальных вложений (CAPEX) и потенциальных финансовых рисков, связанных с возможными нарушениями безопасности.

Генераторы псевдослучайных чисел, являясь детерминированными алгоритмами, способны производить последовательности битов, которые, несмотря на свою предсказуемость для обладателя исходного состояния (сида), статистически неотличимы от истинно случайных для внешнего наблюдателя. Эта особенность делает их экономически привлекательным инструментом, так как они обеспечивают воспроизводимый и управляемый результат, не требуя при этом дорогостоящих физических источников энтропии для каждого цикла вычислений. Сфера их применения чрезвычайно широка: от защиты транзакций в банковском секторе и обеспечения конфиденциальности коммуникаций до генерации уникальных идентификаторов в распределенных системах. С экономической точки зрения, проектирование или выбор ГПСЧ представляет собой поиск оптимального компромисса. С одной стороны, необходимо удовлетворять постоянно растущим требованиям к криптостойкости, обусловленным усложнением методов криптоанализа и появлением квантовых компьютеров. С другой — сохранять конкурентоспособность за счет высокой производительности, низкого энергопотребления и возможности развертывания на массовом, в том числе и ограниченном по вычислительной мощности, оборудовании. Чрезмерный уклон в сторону безопасности может привести к неприемлемо высоким задержкам и затратам на инфраструктуру, в то время как чрезмерная оптимизация под производительность способна создать уязвимости, финансовые последствия от эксплуатации которых многократно превзойдут любые операционные сбережения.

В контексте экономической эффективности современных ГПСЧ показателен пример алгоритма ChaCha20 – поточного шифра, разработанного Дэниелом Бернстайном. Данный

алгоритм получил широкое распространение в таких ключевых для мировой цифровой экономики протоколах, как TLS, обеспечивающий безопасность соединений в интернете, а также в системах виртуальных частных сетей (VPN) и мобильных приложениях. Его экономическое преимущество перед другим широко распространенным стандартом, AES, особенно в определенных сценариях использования, заключается в исключительно высокой скорости работы на процессорных архитектурах, которые не имеют специализированных инструкций для ускорения блочных шифров (таких как AES-NI). Это характерно для множества устройств интернета вещей (IoT), бюджетных мобильных устройств и части сетевого оборудования. Более высокая скорость обработки данных напрямую трансформируется в снижение операционных издержек для провайдеров облачных и телекоммуникационных услуг, позволяя обслуживать большее количество соединений или транзакций на единицу аппаратных ресурсов, а также сокращает энергопотребление, что критически важно для автономных и мобильных устройств. Принцип работы ChaCha20, при котором генерируется ключевой поток, подвергаемый операции XOR с открытым текстом, начиная с инициализации секретным ключом и уникальным одноразовым номером (nonce), обеспечивает высокий уровень безопасности при относительно низких вычислительных затратах. Экономический эффект здесь носит двойной характер: прямое снижение затрат на электроэнергию и аппаратное обеспечение и косвенное — за счет минимизации риска дорогостоящих инцидентов безопасности, связанных с компрометацией данных.

Другим ярким примером экономически оправданного и высокоэффективного применения ГПСЧ является практика использования криптографической соли (salt) при хешировании паролей. В данной схеме ГПСЧ генерирует уникальную случайную строку для каждого пользователя, которая присоединяется к паролю перед процедурой хеширования. Это простое с технической точки зрения действие кардинально меняет экономику безопасности системы. Без использования соли злоумышленник, получивший доступ к базе хешей паролей, может применять предварительно рассчитанные радужные таблицы для массовой расшифровки, что приводит к практически гарантированной компрометации множества учетных записей. Внедрение соли, уникальной для каждой записи, делает такие табличные атаки бесполезными, вынуждая атакующего проводить ресурсоемкий подбор для каждого пароля индивидуально, что увеличивает временные и вычислительные затраты на несколько порядков. Для организаций, особенно работающих в чувствительных секторах, таких как финансы, здравоохранение или электронная коммерция, это означает существенное снижение рисков при утечках данных. Экономическая выгода выражается в предотвращении многомиллионных штрафов, накладываемых регуляторами вроде Европейского союза в рамках Общего регламента по защите данных (GDPR), в сокращении издержек, связанных с расследованием инцидентов, уведомлением клиентов и восстановлением репутации, а также в избежании судебных исков со стороны пострадавших сторон. Таким образом, минимальные затраты на реализацию механизма соления паролей приводят к диспропорционально большому положительному экономическому эффекту.

Особый интерес с точки зрения минимизации издержек представляют регистры сдвига с линейной обратной связью (РСЛОС). Эти устройства, реализуемые как на аппаратном, так и на программном уровне, являются, вероятно, одними из наименее затратных решений для генерации псевдослучайных битовых последовательностей. Их экономическая привлекательность заключается в чрезвычайно низких требованиях к вычислительным ресурсам и энергопотреблению, что позволяет встраивать их даже в самые простые

микроконтроллеры. Благодаря этой характеристике РСЛОС нашли исторически широкое применение в областях, где стоимость и простота первостепенны, включая некоторые протоколы телекоммуникаций (например, ранние реализации в Wi-Fi и Bluetooth), генерацию шумовых последовательностей и тестирование аппаратуры. Однако с экономической точки зрения чистые РСЛОС демонстрируют классический пример ложной экономии. Их фундаментальный недостаток — линейность обратной связи — делает их уязвимыми к криптоаналитическим атакам с использованием алгоритма Берлекэмпа-Мэсси, что позволяет восстановить внутреннее состояние регистра по относительно короткому отрезку выходной последовательности. Следовательно, прямое использование РСЛОС в современных криптографических приложениях сопряжено с неприемлемо высокими рисками. Тем не менее, экономический потенциал этой технологии может быть раскрыт через ее модификации. Комбинирование нескольких РСЛОС с нелинейной функцией фильтрации или суммированием их выходов позволяет создать гибридные конструкции, криптостойкость которых значительно повышается при несущественном увеличении сложности и стоимости. Такие схемы представляют собой жизнеспособный экономический компромисс для приложений, где требования к безопасности умеренны, но жестко ограничен бюджет и ресурсы, продолжая использоваться в ряде стандартизированных протоколов и специализированных устройствах.

Взгляд на перспективы развития рынка генерации случайных чисел для криптографии позволяет выделить наиболее капиталоемкое и потенциально революционное направление — квантовую криптографию и, в частности, квантовые генераторы случайных чисел (QRNG). В отличие от детерминированных ГПСЧ, чья работа основана на математических алгоритмах, QRNG используют фундаментальные недетерминированные процессы квантовой механики, такие как квантовая суперпозиция или вакуумные флуктуации. Это обеспечивает генерацию истинно случайных чисел, принципиально непредсказуемых и невоспроизводимых. С экономической точки зрения, предложение такой абсолютной случайности создает новую рыночную нишу для секторов с высочайшими требованиями к безопасности: центральные банки и финансовые институты, работающие с системами высокочастотного трейдинга и генерацией ключевых материалов; государственные структуры, отвечающие за национальную безопасность и дипломатическую связь; создатели инфраструктуры распределенных реестров и блокчейн-платформ, где качество энтропии критически важно для генерации приватных ключей. Компании-первопроходцы, такие как швейцарская ID Quantique с продуктом Quantis или российская QRate, уже предлагают коммерческие QRNG-решения, позиционируя их как инструмент для создания доверенной энтропии.

Однако широкое экономическое проникновение квантовых технологий в данную область сдерживается рядом существенных барьеров финансового и технологического характера. Основным препятствием являются высокие капитальные затраты (CAPEX). Оборудование для QRNG, включающее однофотонные источники, сверхчувствительные детекторы фотонов и часто системы охлаждения, остается дорогостоящим в производстве и эксплуатации по сравнению с тривиальной программной реализацией традиционного ГПСЧ. Это ограничивает круг потенциальных покупателей крупными организациями с соответствующим бюджетом. Вторым экономическим барьером выступает проблема масштабируемости и интеграции. Квантовые каналы, используемые для распределения ключей или сбора энтропии, часто требуют специализированной оптоволоконной инфраструктуры, точной юстировки и защиты от environmental-факторов, что делает их развертывание в существующих дата-центрах или

телекоммуникационных сетях сложной и дорогостоящей инженерной задачей. Третий фактор связан с неопределенностью рынка и отсутствием унифицированных стандартов. Фрагментация технологических подходов и протоколов создает риски для инвесторов и потребителей, опасающихся оказаться привязанными к нежизнеспособной в долгосрочной перспективе проприетарной технологии. Наконец, четвертым и, возможно, ключевым экономическим вызовом является конкуренция со стороны постквантовой криптографии. Это направление, фокусирующееся на разработке математических алгоритмов, устойчивых к атакам как классических, так и будущих квантовых компьютеров, предлагает повышение уровня безопасности, которое может быть реализовано в виде обновления программного обеспечения на уже существующем оборудовании. С точки зрения модели совокупной стоимости владения (TCO), такой подход часто выглядит значительно более привлекательным для бизнеса, чем инвестиции в новую, сложную и дорогую аппаратную инфраструктуру квантовых систем.

Несмотря на эти вызовы, инвестиционная привлекательность квантовых технологий продолжает расти, что свидетельствует о долгосрочном экономическом тренде. Согласно аналитическим прогнозам, например, от агентства MarketsandMarkets, мировой рынок квантовой криптографии оценивается в сумму порядка 1,8 миллиарда долларов США к 2025 году с потенциалом роста до 8,5 миллиардов долларов к 2030 году, что подразумевает среднегодовой темп роста более 35 процентов. Такая динамика указывает на формирование новой технологической волны, где ранние стратегические инвестиции в исследования, разработки и создание пилотных проектов могут позволить компаниям и государствам занять доминирующие позиции на зарождающемся рынке. Таким образом, текущий этап развития криптографических механизмов на основе генерации псевдослучайных последовательностей характеризуется одновременным сосуществованием и конкуренцией различных экономических моделей: от оптимизированных, дешевых и эффективных программных решений вроде ChaCha20, через гибридные низкозатратные схемы на основе РСЛОС для специфических применений, до капиталоемких, но прорывных квантовых технологий. Оптимальный выбор в каждом конкретном случае определяется не только техническими требованиями, но и тщательным экономическим расчетом, учитывающим прямые и косвенные издержки, потенциальные риски и долгосрочные стратегические цели развития цифровой инфраструктуры.

Заключение

Анализ экономических аспектов применения генераторов псевдослучайных последовательностей в криптографии позволяет сделать вывод о том, что выбор и внедрение конкретного алгоритма представляют собой сложную стратегическую задачу, лежащую на пересечении технологических требований безопасности и финансовой эффективности. Современный ландшафт решений формируется под воздействием необходимости достижения оптимального баланса между тремя ключевыми параметрами: криптостойкостью, производительностью и совокупной стоимостью владения.

Как показывает практика, наиболее эффективные с экономической точки зрения подходы зачастую основаны не на максимальной теоретической стойкости, а на разумной адаптации алгоритмов к целевым платформам и сценариям использования. Доминирование таких решений, как поточный шифр ChaCha20 в средах с ограниченными вычислительными ресурсами, или повсеместное внедрение механизма «соли» при хешировании паролей, наглядно

демонстрирует, что относительно простые и оптимизированные криптографические примитивы способны приносить диспропорционально высокую экономическую выгоду. Она выражается как в прямом снижении операционных и капитальных затрат за счет меньшего энергопотребления и требований к аппаратному обеспечению, так и в косвенном — путем предотвращения колоссальных финансовых потерь, связанных с компрометацией данных, репутационным ущербом и регуляторными санкциями.

Одновременно с этим, пример регистров сдвига с линейной обратной связью иллюстрирует важность анализа долгосрочных рисков. Низкая начальная стоимость реализации может обернуться существенными убытками в будущем, если базовый алгоритм не отвечает современным требованиям криптостойкости. Поэтому даже в сегменте бюджетных решений экономическая целесообразность неизбежно смещается в сторону гибридных и усложненных моделей, обеспечивающих приемлемый уровень безопасности без кардинального роста издержек.

Перспективы развития отрассы указывают на её разделение на два экономических вектора. С одной стороны, продолжается эволюция и оптимизация классических алгоритмов, чья экономическая модель основана на снижении стоимости единицы вычислительной операции и их массовом внедрении в программно-аппаратные комплексы. С другой — формируется высокотехнологичный и капиталоемкий рынок квантовой генерации случайных чисел, предлагающий уникальное ценностное предложение в виде истинной, а не псевдослучайности. Несмотря на текущие барьеры, связанные с высокой стоимостью оборудования и сложностью интеграции, значительный прогнозируемый рост инвестиций в эту область свидетельствует о её стратегической важности для секторов с повышенными требованиями к безопасности. Конкуренция между традиционными программно-аппаратными решениями и прорывными квантовыми технологиями будет стимулировать инновации и в конечном итоге способствовать появлению более надежных и экономически эффективных криптографических систем в долгосрочной перспективе.

Экономическая эффективность криптографических механизмов, основанных на генерации ПСП, является динамической и многокритериальной категорией. Её достижение требует от разработчиков и лиц, принимающих решения, проведения комплексной оценки, учитывающей не только сиюминутные затраты на развертывание, но и весь жизненный цикл системы, включая риски будущих уязвимостей, стоимость модернизации и стратегическое позиционирование на формирующемся технологическом рынке. В условиях цифровой трансформации мировой экономики подобный подход становится неотъемлемым элементом обеспечения как кибербезопасности, так и финансовой устойчивости организаций.

Библиография

1. Alyas, H. H., Abdullah, A. A. Enhancement the ChaCha20 Encryption Algorithm Based on Chaotic Maps. Springer Singapore, 2021.
2. https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/
3. Arias, Dan. Adding Salt to Hashing: A Better Way to Store Passwords. 2025.
4. Иванов С. А. Квантовые сети: будущее коммуникаций. Журнал информационных технологий, 2021, т. 15, №3.
5. Запрягаев С. Квантовые информационные системы. Теория и практика применения. БХВ-Петербург, 2023.
6. IBM. Cost of a Data Breach Report 2023. — https://www.ibm.com/reports/data-breach
7. NIST. Post-Quantum Cryptography Standardization. 2022. — https://csrc.nist.gov/projects/post-quantum-cryptography
8. MarketsandMarkets. Quantum Cryptography Market — Global Forecast to 2030. 2023.

Pseudorandom Number Generators in Information Security: Economic Aspects of Technological Development and Innovation Prospects

Aleksandr S. Grushitsyn

Lecturer, Department of Information Security,
"Synergy" University,
125190, 80, bldg. G, Leningradsky ave., Moscow, Russian Federation;
e-mail: nicifor@bk.ru

Abstract

The article provides a comprehensive analysis of the economic aspects of using pseudorandom number generators (PRNGs) in modern cryptographic systems. The key dilemma of choosing between cryptographic strength, performance, and total cost of ownership is considered. Using specific examples such as the ChaCha20 stream cipher, the password salting mechanism, and linear feedback shift registers (LFSRs), models that provide an optimal balance between security and economic efficiency in various scenarios are investigated. Separate attention is paid to the promising direction of quantum random number generation (QRNG), analyzing the economic barriers and potential of this market. It is proven that the choice of cryptographic primitives is a strategic economic decision requiring consideration of direct and indirect costs, long-term risks, and trends in technological development. The research results demonstrate that the correct choice of a PRNG can significantly reduce capital (CAPEX) and operational (OPEX) expenses, minimize the risks of costly security incidents, and ensure the resilience of the infrastructure to future challenges, such as the development of quantum computing. The work concludes with the necessity of integrating economic analysis into the design and audit process of cryptographic systems at the earliest stages.

For citation

Grushitsyn A.S. (2025) Generatory psevdosluchaynykh chisel v zashchite informatsii: ekonomicheskiye aspekty tekhnologicheskogo razvitiya i perspektivy innovatsiy [Pseudorandom Number Generators in Information Security: Economic Aspects of Technological Development and Innovation Prospects]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (12A), pp. 618-625. DOI: 10.34670/AR.2026.17.73.051

Keywords

Economic efficiency of cryptography, pseudorandom number generator (PRNG), ChaCha20, linear feedback shift register (LFSR), cryptographic salt, quantum random number generator (QRNG), total cost of ownership (TCO), operational expenses (OPEX), capital expenditures (CAPEX), post-quantum cryptography, risk management.

References

1. Alyas, H.H., & Abdullah, A.A. (2021). Enhancement the ChaCha20 Encryption Algorithm Based on Chaotic Maps. In [Title of the collection or proceedings] (pp. [page range]). Springer Singapore. [Примечание: В исходных данных отсутствует название конференции или сборника, а также страницы. Необходимо дополнить информацию.]
2. Arias, D. (2025) Adding Salt to Hashing: A Better Way to Store Passwords. [Publisher or Source information missing].
3. Auth0. (n.d.). Adding Salt to Hashing: A Better Way to Store Passwords. Retrieved [Date of access], from

https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/
4. IBM. (2023). Cost of a Data Breach Report 2023. Retrieved [Date of access], from https://www.ibm.com/reports/data-breach
5. Ivanov, S.A. (2021). Kvantovye seti: budushchee kommunikatsii [Quantum networks: the future of communications]. Zhurnal informatsionnykh tekhnologii [Journal of Information Technologies], 15(3), [page range missing].
6. MarketsandMarkets. (2023). Quantum Cryptography Market — Global Forecast to 2030.
7. National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography Standardization. Retrieved [Date of access], from https://csrc.nist.gov/projects/post-quantum-cryptography
8. Zapriagaev, S. (2023). Kvantovye informatsionnye sistemy. Teoriia i praktika primeneniia [Quantum information systems. Theory and practice of application]. St. Petersburg: BKhV-Peterburg.