

Д. К. Фомин^{1✉}, Е.В. Рыжкова¹

Генерация случайных чисел как ключевой фактор обеспечения безопасности информационных систем

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: denisermake2005@gmail.com

Аннотация. В статье рассмотрена генерация случайных чисел как один из базовых элементов защиты информационных систем. Показано, что устойчивость криптографических алгоритмов зависит не только от математических свойств шифров и протоколов, но и от качества случайных данных, применяемых при создании ключей, одноразовых значений, идентификаторов сессий и параметров электронной подписи. Цель работы состоит в уточнении роли генераторов случайных чисел в практических задачах информационной безопасности и выделении основных требований к их применению. В качестве метода использован сравнительно-аналитический обзор нормативных документов, открытых рекомендаций и типовых сценариев использования случайности в цифровых системах. Рассмотрены источники энтропии, криптографически-стойкие генераторы псевдослучайных чисел, ошибки инициализации и повторного использования значений. В результате сформулированы практические требования к генерации случайных чисел: достаточная энтропия, непредсказуемость, уникальность, контроль состояния генератора и использование проверенных программных интерфейсов.

Ключевые слова: генератор случайных чисел, энтропия, криптография, ключи, аутентификация, информационная безопасность

D. K. Fomin^{1✉}, E. V. Ryzhkova¹

Random number generation as a key factor in ensuring security of information systems

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: denisermake2005@gmail.com

Abstract. The article considers random number generation as one of the basic elements of information system protection. It is shown that the strength of cryptographic algorithms depends not only on the mathematical properties of ciphers and protocols, but also on the quality of random data used to create keys, nonces, session identifiers and digital signature parameters. The purpose of the paper is to clarify the role of random number generators in practical information security tasks and to identify the main requirements for their use. The study is based on a comparative and analytical review of standards, public recommendations and typical scenarios in which randomness is used in digital systems. Entropy sources, cryptographically secure pseudorandom number generators, initialization errors and reuse of values are considered. As a result, practical requirements are formulated: sufficient entropy, unpredictability, uniqueness, generator state control and the use of trusted software interfaces.

Keywords: random number generator, entropy, cryptography, keys, authentication, information security

Введение

При обсуждении информационной безопасности внимание сосредоточено на алгоритмах шифрования, протоколах передачи данных и способах аутентификации. Однако на практике эти механизмы начинают работать только после появления ключей, одноразовых значений, идентификаторов и других параметров, которые должны быть неизвестны злоумышленнику. Именно здесь возникает задача генерации случайных чисел. Она кажется вспомогательной, но фактически связывает математическую стойкость криптографии с реальной работой программного обеспечения и оборудования.

Случайное число в системе защиты не является обычным «произвольным» значением. Для имитационного моделирования или игр достаточно последовательности, которая выглядит равномерной. Для криптографии этого мало: атакующий не должен иметь возможности восстановить прошлые значения, предсказать будущие значения или существенно сузить область перебора. Поэтому в российских документах по информационной безопасности отдельно рассматриваются криптографические алгоритмы, режимы их применения, процедуры контроля и требования к средствам защиты информации [1-6].

Актуальность темы связана с тем, что современные информационные системы постоянно создают временные секреты. Сеансовые ключи в защищенном соединении, токены восстановления пароля, идентификаторы веб-сессий, соли для хэширования паролей и параметры цифровой подписи должны быть уникальными и непредсказуемыми.

Цель работы – рассмотреть генерацию случайных чисел как ключевой фактор обеспечения безопасности информационных систем и показать, какие свойства генератора имеют практическое значение.

Методы и материалы

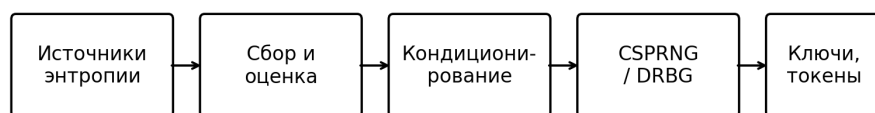
Основной нормативной базой для анализа являются российские стандарты и документы в области криптографической защиты информации. ГОСТ 34.10-2018 описывает процессы формирования и проверки электронной цифровой подписи, ГОСТ Р 34.11-2012 устанавливает алгоритм хэширования, а ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 определяют блочные шифры и режимы их работы [1-4]. Для более общего контекста информационной безопасности использованы стандарты системы менеджмента информационной безопасности и нормативные требования к защите информации в государственных, персональных и критически важных информационных системах [5-13]. Теоретическая часть дополнена учебными и научными изданиями по криптографии и криптографическим методам защиты информации [14-16].

Дополнительно учтены документы серии NIST SP 800-90, так как в них подробно раскрываются вопросы построения генераторов случайных битов. В SP 800-90A рассматриваются детерминированные генераторы, SP 800-90B посвящен источникам энтропии и их оценке, а SP 800-90C описывает общие конструкции генераторов случайных битов [17-19]. При рассмотрении прикладного уровня также

использованы рекомендации по управлению веб-сессиями, поскольку идентификатор сессии является одним из практических примеров значения, которое должно быть достаточно длинным, уникальным и непредсказуемым [20].

Результаты

Генерация случайных чисел в информационной системе может быть представлена как цепочка этапов. Сначала система получает неопределенность из физических или программно-аппаратных источников: шумы оборудования, события ввода-вывода, состояние операционной системы, аппаратные генераторы. Затем эти данные оцениваются с точки зрения энтропии, проходят обработку и используются для инициализации криптографически-стойкого генератора псевдослучайных чисел. Уже после этого генератор выдает значения для конкретных задач: ключей, токенов, одноразовых чисел и идентификаторов. Общая схема такого процесса приведена на рис. 1.



Контроль качества: достаточная энтропия, уникальность, непредсказуемость, отсутствие повторов

Рис. 1. Общая схема получения случайных данных

Из схемы видно, что качество итогового значения определяется не только алгоритмом генератора, но и начальным материалом. Даже хороший криптографический генератор не исправит ситуацию, если он был инициализирован предсказуемым зерном. Например, если зерно зависит только от времени запуска программы, числа возможных вариантов становится значительно меньше, чем предполагает длина выдаваемого ключа. Для атакующего это означает не полный перебор всего пространства ключей, а проверку ограниченного набора вероятных состояний.

В практических системах чаще всего используется не поток «истинных» случайных чисел, а криптографически-стойкий псевдослучайный генератор. Это нормальная инженерная схема: физический источник дает сравнительно небольшой объем энтропии, а детерминированный генератор расширяет его до необходимого количества битов. Важным условием является то, что выходные данные генератора не должны раскрывать его внутреннее состояние. Даже если злоумышленник увидел часть выданных значений, он не должен вычислить предыдущие или будущие значения.

Наиболее заметная область применения случайности – генерация криптографических ключей. Ключ должен быть настолько непредсказуемым, чтобы его поиск сводился к полному перебору огромного пространства вариантов. Если же генератор систематически выдает значения из небольшой области, фактическая

стойкость алгоритма уменьшается. В этом смысле длина ключа и качество генерации не заменяют друг друга: длинный ключ, выбранный из предсказуемой последовательности, не обеспечивает ожидаемого уровня защиты.

Для российских схем электронной подписи случайность также имеет принципиальное значение. В ГОСТ 34.10-2018 формирование подписи основано на операциях в группе точек эллиптической кривой, а в ГОСТ Р 34.11-2012 определена хэш-функция, применяемая в том числе в процессах формирования и проверки электронной цифровой подписи [1, 2]. При создании подписи используется закрытый ключ и для каждой операции формируется случайное или псевдослучайное целое число, которое должно удовлетворять установленным требованиям. Если такое значение окажется предсказуемым или будет повторно использовано, стойкость подписи снижается, а риск компрометации ключевой информации возрастает. Поэтому для российских алгоритмов электронной подписи важны не только корректные параметры эллиптической кривой и применение хэш-функции, но и надежная генерация случайных значений при формировании подписи [1, 7].

Сравнение основных требований к генераторам случайных чисел представлено в табл. 1. Таблица показывает, что требования имеют не только теоретический характер: каждое из них связано с конкретным видом атаки или эксплуатационной ошибки.

Нарушение хотя бы одного требования способно изменить весь уровень защищенности системы.

Для прикладного разработчика практический вывод достаточно простой: нельзя использовать генераторы общего назначения там, где создаются секреты. Генератор для моделирования или статистических задач может давать внешне равномерную последовательность, но это не означает криптографическую стойкость. В задачах защиты информации следует применять системные источники случайности, криптографические библиотеки и программные интерфейсы, рассчитанные именно на создание ключей, токенов, идентификаторов сессий и иных критичных значений [17, 18, 20].

Таблица 1. Основные требования к генерации случайных чисел

Требование	Смысл	Риск при нарушении	Практическое решение
Достаточная энтропия	Наличие реальной неопределенности в исходных данных	Сужение пространства перебора ключей и токенов	Использование системных и аппаратных источников энтропии
Непредсказуемость	Невозможность вычислить будущие значения по известным выходам	Предсказание идентификаторов, ключей или одноразовых значений	Применение CSPRNG/DRBG вместо обычных генераторов

Окончание табл.1

Требование	Смысл	Риск при нарушении	Практическое решение
Уникальность	Отсутствие повторов там, где значение должно использоваться один раз	Повтор попсо, повтор параметров подписи, повтор сеансовых ключей	Контроль повторов и корректное обновление состояния генератора
Корректная инициализация	Непредсказуемое зерно и правильный момент запуска генератора	Одинаковые последовательности после перезапуска или клонирования системы	Инициализация из доверенного источника случайности ОС
Контроль состояния	Проверка отказов источника энтропии и генератора	Незаметная деградация качества случайных данных	Тесты работоспособности и обработка ошибок генератора

Обсуждение

Главная особенность рассматриваемой темы состоит в том, что ошибки генерации случайных чисел трудно заметить обычным тестированием. Если программа выдала токен нужной длины, тест может считаться пройденным. Но внешний вид строки не показывает, сколько в ней реальной неопределенности. Статистически «красивое» распределение также не гарантирует криптографической стойкости: последовательность может выглядеть равномерной и при этом быть полностью воспроизводимой для того, кто знает зерно или алгоритм.

В российской практике значение корректной генерации случайных данных связано не только с криптографическими стандартами, но и с общими требованиями к защите информационных систем. Нормативные документы по защите государственных информационных систем, персональных данных и значимых объектов критической информационной инфраструктуры требуют применения организационных и технических мер безопасности, а криптографические механизмы являются частью таких мер [8-13]. Это показывает, что генератор случайных чисел нельзя рассматривать как второстепенную деталь программы: ошибка в нем способна повлиять на ключи, электронную подпись, идентификаторы пользователей и устойчивость всей системы защиты.

На рис. 2 показана типовая логика последствий слабой генерации случайных чисел. Она применима как к серверным системам, так и к пользовательским приложениям. Повтор ключей или одноразовых параметров бьет по криптографическим протоколам; предсказуемые идентификаторы создают риск захвата сессии; недостаточная энтропия зерна облегчает перебор.

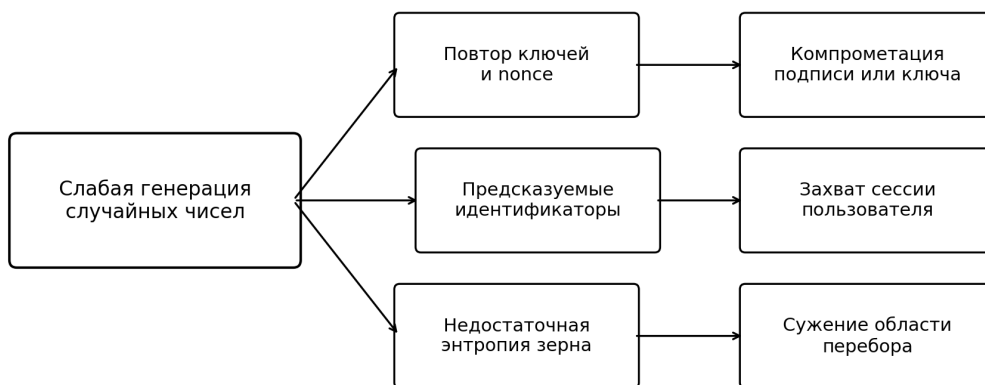


Рис. 2. Типичные последствия слабой генерации случайных чисел

В идеальном случае источник случайности основан на физическом процессе, который невозможно точно предсказать. Но информационная система не всегда может напрямую использовать такой источник в требуемом объеме и с нужной скоростью. Поэтому на практике более важна не противоположность «истинное – псевдослучайное», а правильно построенная цепочка: надежный источник энтропии, корректная обработка, стойкий генератор и безопасное применение результата.

Заключение

Генерация случайных чисел является одним из ключевых факторов обеспечения безопасности информационных систем. Она влияет на криптографические ключи, параметры защищенных соединений, идентификаторы сессий, одноразовые коды, цифровую подпись и другие элементы защиты. При этом качество случайности определяется не одной функцией, а всей цепочкой: источником энтропии, процедурой инициализации, алгоритмом генератора, контролем состояния и корректным использованием результата.

В ходе анализа установлено, что основными требованиями к генераторам случайных чисел являются достаточная энтропия, непредсказуемость, уникальность критических значений, корректная инициализация и контроль отказов. Нарушение этих требований приводит к практическим рискам: снижению стойкости ключей, предсказанию токенов, повтору параметров подписи, захвату сессий и сужению пространства перебора. Поэтому использование проверенных криптографических генераторов и системных источников случайности должно рассматриваться как обязательное условие безопасной разработки.

Дальнейшее развитие темы может быть связано с анализом качества генераторов в конкретных программных средах, сравнением поведения генераторов в обычных и виртуализированных системах, а также с изучением аппаратных и квантовых источников случайности. Практическая значимость работы заключается в том, что сформулированные требования могут использоваться при проектировании и про-

верке информационных систем, где случайные данные применяются для защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ 34.10–2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М. : Стандартинформ, 2018.
2. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – М. : Стандартинформ, 2013.
3. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М. : Стандартинформ, 2016.
4. ГОСТ Р 34.13–2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М. : Стандартинформ, 2016.
5. ГОСТ Р ИСО/МЭК 27001–2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М. : Стандартинформ, 2021.
6. ГОСТ Р ИСО/МЭК 27002–2021. Информационная технология. Методы и средства обеспечения безопасности. Свод практических правил по мерам информационной безопасности. – М. : Стандартинформ, 2021.
7. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
10. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
11. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
12. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
13. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
14. Бабаш А. В., Шанкин Г. П. Криптография. – М. : СОЛОН-Пресс, 2007. – 512 с.
15. Агибалов Г. П., Грушо А. А. Криптология. – Томск : Изд-во НТЛ, 2006. – 256 с.
16. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М. : ДМК Пресс, 2000. – 448 с.
17. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators : NIST SP 800-90A Rev. 1. – Gaithersburg : NIST, 2015.
18. Turan M. S., Barker E., Kelsey J., McKay K., Baish M., Boyle M. Recommendation for the Entropy Sources Used for Random Bit Generation : NIST SP 800-90B. – Gaithersburg : NIST, 2018.
19. Barker E., Kelsey J., McKay K., Roginsky A., Sönmez Turan M. Recommendation for Random Bit Generator Constructions : NIST SP 800-90C. – Gaithersburg : NIST, 2025.
20. OWASP Foundation. Session Management Cheat Sheet. – URL: https://cheatsheet-series.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html (дата обращения: 06.05.2026).

© Д. К. Фомин, Е. В. Рыжкова, 2026