www.volsu.ru

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В БЕЗОПАСНОСТИ И ТЕЛЕКОММУНИКАЦИЯХ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2025.3.1

УДК 004.056.5
ББК 32.972.53

ИССЛЕДОВАНИЕ ПРИНЦИПОВ ЦИФРОВОГО СКРЕМБЛИРОВАНИЯ ДАННЫХ

Надежда Николаевна Ермакова

Старший преподаватель, кафедра телекоммуникационных систем,
Волгоградский государственный университет
ermakova.nadezhda@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Современное общество невозможно представить без телекоммуникационных систем, в которых ежедневно передаются колоссальные объемы данных. Надежность и безопасность этой информации имеют ключевое значение – как для государственных структур и коммерческих организаций, так и для частных пользователей. В процессе передачи данных по цифровым каналам возникает ряд проблем, связанных с искажениями сигнала, нарушением синхронизации и возможностью несанкционированного доступа. Одним из эффективных инструментов повышения устойчивости и корректности передачи является цифровое скремблирование данных. С развитием телекоммуникационных технологий и возрастанием требований к безопасности информационных систем методы скремблирования начали использоваться не только в инженерных целях, но и как элемент комплексной защиты данных. Современные стандарты связи включают скремблеры как обязательный компонент физического уровня. При этом в сфере информационной безопасности наблюдается тенденция интеграции принципов скремблирования с криптографическими механизмами для дополнительного уровня защиты. Цель научной работы – исследовать принципы цифрового скремблирования данных и определить его роль в обеспечении информационной безопасности. Основными задачами исследования являются обзор основных принципов скремблирования и классификация типов алгоритмов, современных подходов к защите данных, оценка эффективности различных алгоритмов скремблирования, включая сравнительный анализ их устойчивости и применимости; проведение экспериментальных исследований и сравнение эффективности методов скремблирования данных. Результаты работы могут быть применены при разработке и проектировании систем передачи управляющих и телеметрических данных в промышленных и распределенных сетях,

© Ермакова Н.Н., 2025

где требуется высокая надежность, синхронность и устойчивость к помехам. Реализованные схемы скремблеров могут служить основой для дальнейших исследований по оптимизации алгоритмов кодирования и защите цифровых каналов связи.

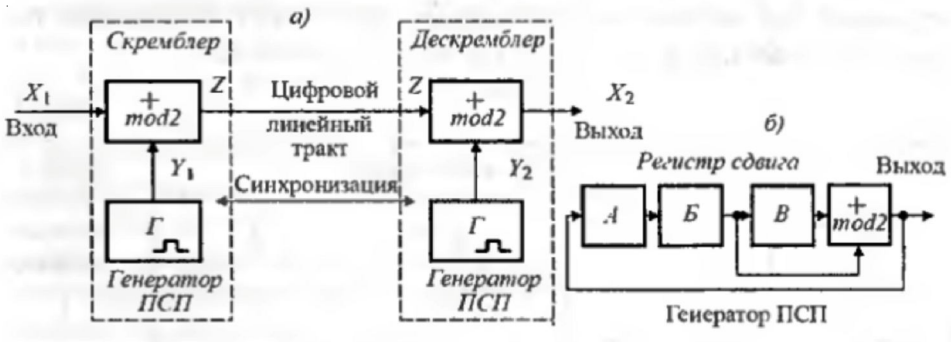
Ключевые слова: цифровое скремблирование, защита данных, аддитивный скремблер, блочный скремблеры, эффективность, ошибки и устойчивость.

Цифровое скремблирование представляет собой процесс преобразования последовательности двоичных данных с целью устранения закономерностей в потоке и повышения его статистической равномерности. В отличие от шифрования, скремблирование не предназначено для скрытия содержимого информации, а обеспечивает оптимальные свойства сигнала для передачи по каналу связи. Главная задача скремблирования – предотвращение возникновения длинных однотипных последовательностей битов, которые могут нарушать синхронизацию приемного оборудования и снижать качество передачи [1; 2]. Длительные серии одинаковых символов уменьшают количество переходов в сигнале, что затрудняет выделение тактовых импульсов и может приводить к ошибкам восстановления данных.

Скремблирование реализуется с использованием генераторов псевдослучайных последовательностей, чаще всего на основе линейных регистров сдвига с обратной связью (LFSR). Каждый бит исходного потока модифицируется в соответствии с состоянием генератора, что обеспечивает псевдослучайное распределение символов и сохранение обратимости процесса. Это позволяет приемнику восстановить исходные данные при известном алгоритме и начальных параметрах генератора. На рисунке представлена общая схема скремблера – дескремблера.

Использование скремблирования положительно сказывается на характеристиках цифрового канала связи. Преобразованный поток данных приобретает более равномерное распределение нулей и единиц, что улучшает спектральные свойства сигнала и снижает вероятность возникновения помех [3]. Одновременно уменьшается вероятность появления длинных последовательностей одинаковых битов, что повышает устойчивость каналов к сбоям синхронизации и снижает количество ошибок передачи. С практической точки зрения это обеспечивает стабильную работу сетевых протоколов и повышает надежность систем передачи данных. Скремблирование создает условия для корректной синхронизации, стабильной передачи информации и упрощает последующее применение методов кодирования и защиты данных.

Была выполнена практическая реализация двух скремблеров в среде MATLAB/Simulink: аддитивного (синхронного) LFSR и блочного (frame-based) типа. Линейный (синхронный) скремблер на основе LFSR, при котором и передающий, и принимающий скремблеры изначально синхронизированы и используют одинаковое начальное состояние регис-



Скремблер – дескремблер

тра. Блочный (frame-based) скремблер, осуществляющий скремблирование данных по кадрам фиксированной длины, что позволяет сравнить его эффективность и особенности работы относительно линейного варианта. Проведены эксперименты с различными объемами данных, выполнены измерения скорости, пропускной способности и энтропии потока. Полученные результаты представлены в таблицах 1–3.

На основе полученных результатов можно сделать сравнение аддитивного LFSR-скремблера и блочного скремблера по трем основным критериям: производительность (скорость работы), пропускная способность и энтропия (степень «случайности» выходного потока. Блочный скремблер оказывается более производительным (выше скорость и пропускная способность) при обработке больших данных, а также обеспечивает лучшую энтропию на малых объемах. Аддитивный LFSR быстрее на небольших данных, но уступает на больших выборках. Если требуется высокая производительность и устойчивое качество при работе с большими массивами, блочный скремблер предпочтителен. Если важна простота реализации и эффективность на малых данных, аддитивный LFSR также вполне допустим. Оба типа обеспечивают достаточную степень скремблирования для цифровых систем, однако блочный скремблер дает чуть лучшие результаты по пропускной способности и максимальной энтропии.

Современные подходы к защите данных строятся на комбинации методов различного уровня: от низкоуровневого скремблирования и кодирования до высокоуровневого шифрования и управления доступом. Скремблирование в этой системе играет роль базового механизма, повышающего устойчивость каналов свя-

Таблица 1

Сравнение средней скорости работы, с

Кол-во битов	Аддитивный LFSR	Блочный
10	0.091	0.094
1000	0.102	0.105
10000	0.213	0.208
50000	0.725	0.681
100000	1.334	1.248

Таблица 2

Сравнение пропускной способности, кбит/с

Кол-во битов	Аддитивный LFSR	Блочный
10	0.11	0.11
1000	9.83	9.63
10000	46.92	48.17
50000	68.96	73.51
100000	74.98	80.10

Таблица 3

Результаты энтропии, бит/символ

Кол-во битов	Аддитивный LFSR	Блочный
10	0.68404	0.84535
1000	0.7963	0.78452
10000	0.8058	0.80965
50000	0.81038	0.80805
100000	0.81205	0.80964

зи и формирующего основу для эффективной работы других средств защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Голиков, А. М. Исследование методов аналогового скремблирования : учеб.-метод. пособие по лаборатор. работе / А. М. Голиков. Томск : ТУСУР, 2019. 25 с. Электрон. текстовые дан. – Режим доступа: https://studfile.net/preview/16875615/

2. Кривоногов, А. С. Алгоритм идентификации вида скремблирования бинарных данных / А. С. Кривоногов, Е. О. Кривоногова // Известия высших учебных заведений России. Радиоэлектроника. – 2017. – № 6. – С. 10–14. – Электрон. текстовые дан. – Режим доступа: https://re.eltech.ru/jour/article/view/197

3. Маглицкий, Б. Н. Космические и наземные системы радиосвязи : учеб. пособие. Новосибирск : Изд-во СибГУТИ, 2013. 300 с.

REFERENCES

1. Golikov A.M. *Issledovaniye metodov analogovogo skremblirovaniya: ucheb.-metod. posobiye po laborator. rabote* [Research of Analog Scrambling Methods. Educational and Methodological Manual for Laboratory Work]. Tomsk, TUSUR, 2019. 25 p. URL: https://studfile.net/preview/16875615/

2. Krivonogov A.S., Krivonogova E.O. Algoritm identifikatsii vida skremblirovaniya binarnyh dannyh [Algorithm for Identifying the Type of Binary Data Scrambling]. *Izvestiya vysshih uchebnyh zavedeniy Rossii. Radioelektronika* [Journal of Russian Universities. Radioelectronics], 2017, no. 6, pp. 10-14. URL: https://re.eltech.ru/jour/article/view/197

3. Maglitsky B.N. *Kosmicheskiye i nazemnye sistemy radiosvyazi: ucheb. posobiye* [Space and Terrestrial Radio Communication Systems. Textbook]. Novosibirsk, Izd-vo SibGUTI, 2013. 300 p.

RESEARCH ON THE PRINCIPLES OF DIGITAL DATA SCRAMBLING

Nadezhda N. Ermakova

Senior Lecturer, Department of Telecommunications Systems,
Volgograd State University
ermakova.nadezhda@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Modern telecommunications are fundamental to society, transmitting vast amounts of data daily. Information reliability and security are crucial for all users. Digital transmission faces challenges: signal distortion, synchronization loss, and unauthorized access. Digital scrambling enhances transmission stability and correctness. A key trend is integrating scrambling with cryptographic mechanisms for layered defense. This research investigates digital scrambling principles and their role in information security. Objectives include reviewing scrambling fundamentals and classifying algorithm types, analyzing modern integrated data protection approaches, and comparatively evaluating algorithm effectiveness, stability, and applicability. Theoretical analysis is supplemented by experimental studies comparing method performance effectiveness. Results are applicable in designing control and telemetry systems for industrial and distributed networks requiring high reliability, synchronization, and interference resistance. Implemented scrambler schemes provide a foundation for future research into optimizing coding algorithms and securing digital channels against evolving threats. The work bridges theoretical scrambling analysis with practical security implementation, addressing current needs for robust data integrity and confidentiality in critical infrastructure. Scrambling transforms data sequences to eliminate patterns, preventing synchronization failure and reducing error propagation. This property is essential for modern high-speed networks. The comparative evaluation focuses on parameters like autocorrelation, balance, and linear complexity. Experimental modeling assesses bit error rate performance under various channel conditions. The conclusion defines optimal scrambling applications within broader cryptographic system architectures.

Key words: digital scrambling, data protection, additive scramblers, block scramblers, efficiency, errors and resilience.