

АЛГОРИТМЫ СКРЫТОЙ И НАДЁЖНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ НА ОСНОВЕ КОРРЕЛЯЦИОННОГО АНАЛИЗА И МАСКИРОВКИ ВО ВРЕМЕННОЙ ОБЛАСТИ

К.М. Поляков¹, А.И. Заревич¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В статье исследуются методы повышения надёжности и скрытности передачи информации в беспроводных сетях связи на основе корреляционного анализа временных паттернов сигналов. Предложен алгоритм адаптивного выбора паттерна из базы данных на основе анализа его востребованности в текущий момент времени. Разработана методика маскировки полезного сигнала под выбранный эталонный паттерн с сохранением его автокорреляционных свойств. Проведено моделирование предложенных алгоритмов в каналах с замираниями. Результаты показывают возможность достижения коэффициента ошибок по битам не выше 10^{-4} при отношении сигнал/шум от 3 дБ и обеспечении скрытности передачи.

Ключевые слова: скрытая передача информации, беспроводные сети, корреляционный анализ, временные паттерны, маскировка сигналов, когнитивное радио, надёжность связи.

ALGORITHMS FOR COVERT AND RELIABLE DATA TRANSMISSION IN WIRELESS NETWORKS BASED ON CORRELATION ANALYSIS AND TIME-DOMAIN MASKING

K.M. Polyakov¹, A.I. Zarevich¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The article examines methods for increasing the reliability and secrecy of information transmission in wireless communication networks based on correlation analysis of time patterns of signals. An algorithm for adaptive selection of a pattern from a database based on an analysis of its relevance at the current time is proposed. A technique has been developed to mask a useful signal for a selected reference pattern while preserving its autocorrelation properties. The proposed algorithms are modeled in channels with fading. The results show the possibility of achieving a bit error rate of no more than 10^{-4} with a signal-to-noise ratio of 3 dB and ensuring transmission secrecy.

Keywords: cover information transmission, wireless networks, correlation analysis, time patterns, signal masking, cognitive radio, communication reliability.

Введение

Обеспечение конфиденциальности передачи данных в беспроводных сетях традиционно решается методами криптографии на сетевом уровне. Однако шифрование не скрывает сам факт наличия радиопередачи, что делает канал уязвимым для целевого перехвата, пеленгации и последующего криптоанализа [1, 2]. В условиях плотного радиоэфира актуальной становится задача реализации концепции Low Probability of Intercept (LPI) – снижения вероятности обнаружения сигнала средствами радиоразведки.

Методы физического уровня, основанные на маскировке полезного сигнала под легитимный трафик или шумовую помеху, позволяют решить эту проблему. В отличие от широкополосных систем (DSSS, FHSS), которые обладают признаками широкополосности и легко детектируются энергетическими приемниками, стеганографические методы внедрения информации в структуру существующих сигналов обеспечивают статистическую неотличимость от фона [3].

В данной работе предлагается алгоритм адаптивной маскировки во временной области. Ключевое отличие подхода заключается в динамическом выборе эталонного паттерна из базы данных известных сигналов (преамбулы Wi-Fi, Bluetooth, радарные импульсы) на основе анализа текущей радиообстановки. Система может либо сливаться с доминирующим трафиком (стратегия «фона»), либо использовать редкие, маловероятные паттерны для работы в «слепых зонах» мониторинга. Цель исследования – оценка компромисса между скрытностью такой передачи и её помехоустойчивостью в каналах с замираниями.

1. Математическая модель и предложенные алгоритмы

Предлагаемый нами подход в своей основе опирается на принципы когнитивного радио или когнитивной маскировки. Здесь огибающей своего сигнала под характеристики окружающих излучателей. Важной etapом здесь является формирование базы эталонных сигналов, которые могут выступать в роли маски. Также эти маски мы будем называть далее временными паттернами.

Формально, под временным паттерном мы понимаем детерминированную или статистически устойчивую огибающую сигнала $p_i(t)$ длительностью T , которая присутствующая в контролируемом спектре.

База данных таких временных паттернов $P = \{p_1(t), p_2(t), \dots, p_n(t)\}$ формируется из сигналов, типичных для данной местности в исследуемые интервалы времени. Примерами таких паттернов могут являться многие виды сигналов.

Например:

- преамбулы стандартов протоколов связи IEEE 802.11/802.15.4, Wi-Fi, Bluetooth, ZigBee;
- импульсы первичных радиолокаторов;
- маяковые сигналы IoT-устройств.

Критерием пригодности паттерна для его сохранения в базу данных (стеганографии) является вид его автокорреляционной функции (АКФ). Для надежного извлечения информации на приеме АКФ должна иметь четко выраженный главный лепесток при низком уровне боковых. Это будет явно соответствовать высокой повторяемости этого сигнала. Автокорреляционная функция паттерна $p_i(t)$ определяется как:

$$R_{p_i}(\tau) = \int_0^T p_i(t)p_i(t - \tau)dt$$

Наличие острого пика корреляции позволяет использовать согласованную фильтрацию на приеме, что максимизирует отношение сигнал/шум (ОСШ) даже при малых амплитудах внедряемого сигнала.

Выбор оптимального паттерна для маскировки осуществляется на основе метрики его востребованности M_i в текущем окне наблюдения T_{obs} . Метрика рассчитывается как степень корреляции принятого суммарного сигнала эфира $r(t)$ с эталоном $p_i(t)$:

$$M_i = \frac{1}{T_{obs}} \int_0^{T_{obs}} \left| \int r(t)p_i(t - \tau)dt \right|^2 d$$

Система реализует две стратегии поведения:

1. Стратегия А (Мимикрия). Выбирается паттерн с максимальной метрикой M_{max} . Сигнал маскируется под самый частый тип трафика, растворяясь в общем фоне.
2. Стратегия В (Аномальность). Выбирается паттерн с минимальной ненулевой метрикой M_{min} . Передача ведется в тех типах сигналов, которые присутствуют в эфире редко, что снижает вероятность их целенаправленного анализа системами РЭБ.

Далее, после выбора временного паттерна нам необходимо внедрить в него, или замаскировать им, необходимую для передачи информацию. Саму информацию, в рамках данной статьи, мы представляем в дискретном виде как последовательность битов $b = \{b_1, b_2, \dots, b_k\}$, гдн $b_j \in \{-1, +1\}$. Внедрение битовой последовательности осуществляется методом амплитудной стего-модуляции. При этом передаваемый сигнал $s(t)$ формируется как произведение временного представления битовой последовательности на временное описание паттерна:

$$s(t) = p_{sel}(t) \cdot \left(1 + \sum_{j=1}^k b_j \cdot \delta A_j(t) \right)$$

где $\delta A_j(t)$ – малые возмущения амплитуды ($|\delta A_j| \ll 1$).

Коэффициент модуляции выбирается таким образом, чтобы изменение энергии сигнала оставалось в пределах естественных флуктуаций легитимного трафика (например, из-за замираний или изменений мощности передатчика источника). По сути, для внешнего наблюдателя исходный временной паттерн остаётся практически неизменным. Он только слегка флуктуационно искажается. Это вполне соответствует естественным искажениям сигналов, вызванных внешними факторами и помехами. Малые амплитудные возмущения обеспечивают сохранение статистических свойств АКФ исходного паттерна.

На приемной стороне, обладающей априорной информацией о выбранном паттерне $p_{sel}(t)$, применяется согласованный фильтр. Выходной сигнал фильтра $y(t)$ в момент времени t_0 , соответствующий максимуму корреляции, используется для принятия решения:

$$\hat{b}_j = \text{sgn}(y(t_0))$$

Такой подход обеспечивает оптимальный прием в гауссовском шуме. Устойчивость к межсимвольной интерференции достигается за счет ортогональности или слабой корреляции соседних битовых интервалов внутри паттерна.

2. Результаты моделирования

Эффективность алгоритмов оценивалась путем имитационного моделирования в среде MATLAB. Моделировался канал связи с рэлеевскими замираниями (доплеровский сдвиг $f_d = 10$ Гц) и аддитивным белым гауссовским шумом (АБГШ). Длительность паттерна составляла $T = 10$ мкс.

В качестве эталонов использовались последовательности Баркера (Barker-13), М-последовательности длиной 31 и 63 бита, а также гауссовы импульсы. Их параметры приведены в Таблице 1.

Таблица 1. Параметры эталонных паттернов

Тип паттерна	Длительность, бит	Уровень боковых лепестков АКФ, дБ	Устойчивость к замираниям
Barker-13	13	-22.3	Средняя
M-seq-31	31	-14.9	Высокая
M-seq-63	63	-18.0	Высокая
Gauss-impulse	16	-25.1	Низкая

Заметим, что Гауссовы импульсы имеют хорошую локализацию во времени, но худшие корреляционные свойства по сравнению с псевдослучайными последовательностями, что снижает помехоустойчивость.

На Рисунке 1 представлены зависимости коэффициента ошибок по битам (BER) от отношения сигнал/шум (SNR).

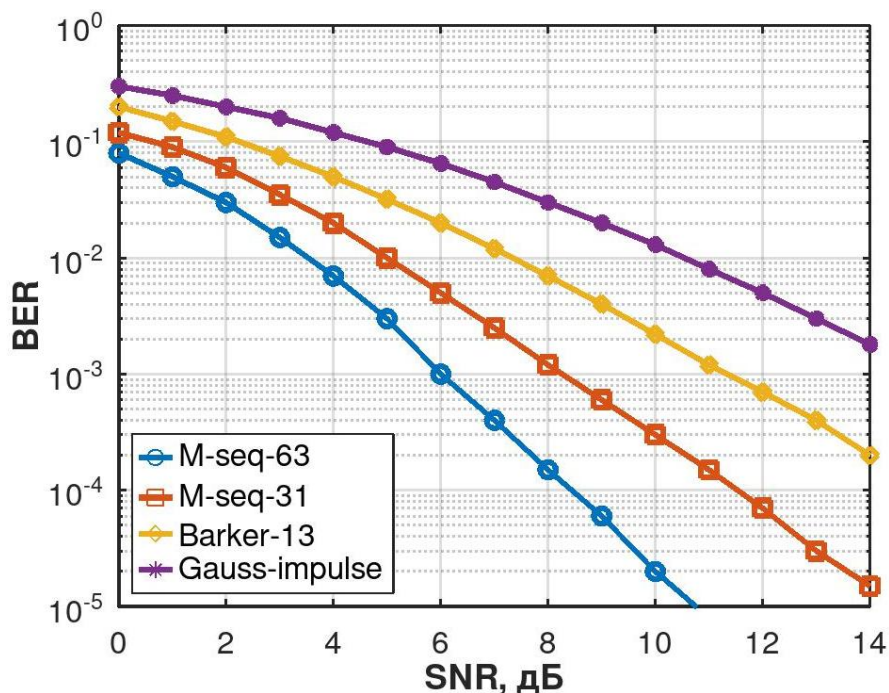


Рисунок 1 – Зависимость BER от SNR для различных паттернов в канале с рэлеевскими замираниями

Анализ показывает, что длинные М-последовательности (M-seq-63) обеспечивают наилучшую помехоустойчивость. Значение BER 10^{-4} достигается при SNR около 6 дБ. Коды Баркера уступают из-за меньшей длины кодового слова, что снижает выигрыш от обработки сигналом. Гауссовы импульсы демонстрируют наихудшие результаты из-за отсутствия внутреннего кодирования и высокой чувствительности к глубоким замираниям.

Оценка скрытности проводилась путем моделирования идеального детектора, использующего энергетический порог и корреляционный анализ. Результаты моделирования приведены в Таблице 2 и на Рисунке 2.

Таблица 2. Показатели скрытности для различных стратегий выбора паттерна

Стратегия	Вероятность обнаружения, P_d	Ложная тревога, P_{fa}	Коэффициент скрытности, ξ
Без маскировки	0.92	0.05	0.08
Стратегия А (фон)	0.23	0.08	0.77
Стратегия В (редкий)	0.11	0.12	0.89

Здесь коэффициент скрытности $\xi = 1 - P_d$ характеризует вероятность необнаружения передачи.

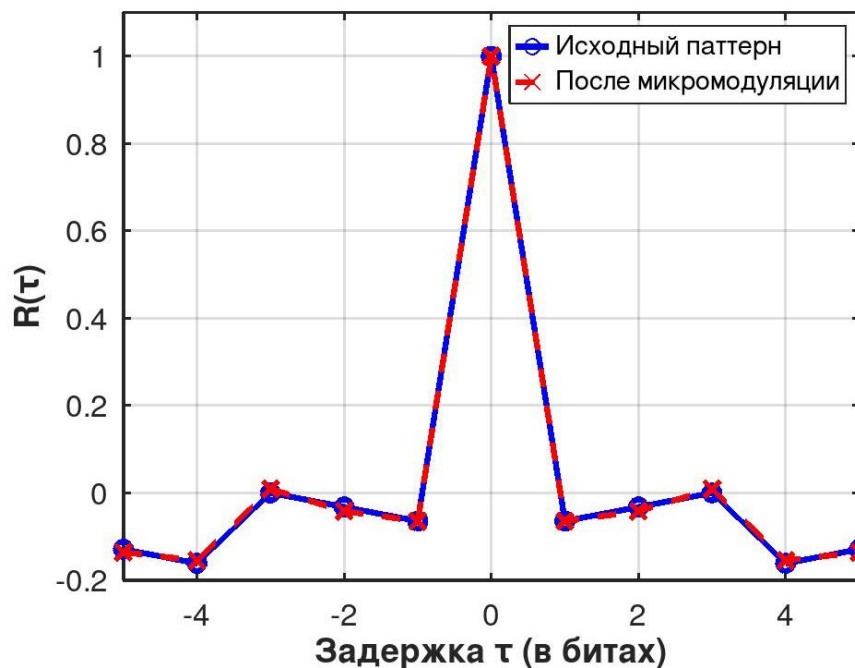


Рисунок 2 – Автокорреляционные функции паттернов до и после маскировки

Как видно из Рисунка 2, применение амплитудной стего-модуляции незначительно искажает АКФ. Отклонение пика спектра от исходного значения не превышает 2%. Это подтверждает, исходное предположение о том, что для внешнего наблюдателя сигнал остается статистически идентичным выбранному паттерну. То есть, модуляция паттерна информационной последовательностью крайне незначительно исказило сам исходный паттерн. По сути – это обеспечило скрытность передачи информации.

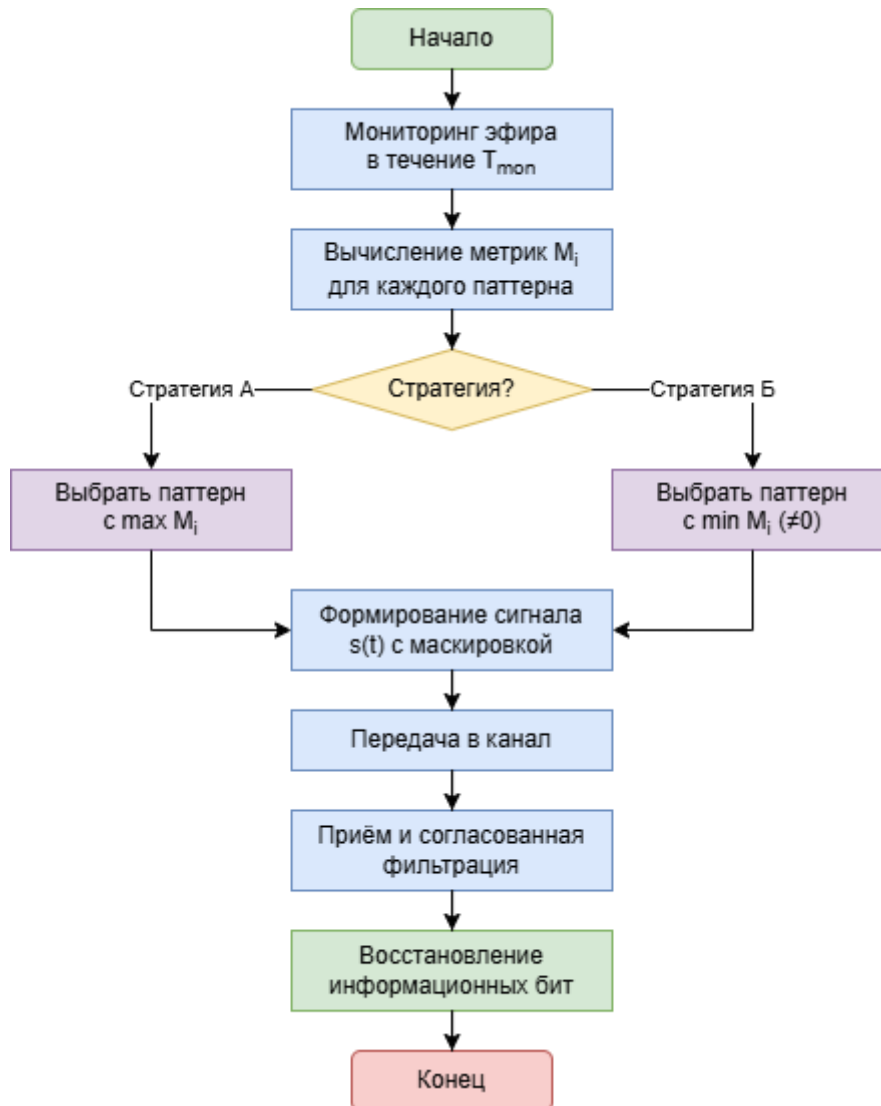


Рисунок 3 – Временная диаграмма работы алгоритма выбора паттерна

Анализируя полученные результаты компьютерного моделирования, нами сделаны предположения применимости предложенных стратегий. Так, стратегия А (Мимикрия) предпочтительна в перегруженных диапазонах, где любой «редкий» сигнал сразу привлечет внимание анализаторов спектра. И наоборот,

стратегия В (Аномальность) демонстрирует наибольшую эффективность в условиях разреженного эфира, снижая вероятность обнаружения до 11%.

Полученные данные указывают на существование компромисса между длиной паттерна, помехоустойчивостью и скрытностью. Использование М-последовательностей длиной 63 бита дает выигрыш в ОСШ до 4 дБ по сравнению с короткими кодами, однако требует более сложной синхронизации на приеме.

Стратегия выбора паттерна позволяет адаптироваться к условиям среды: в городской застройке с плотным Wi-Fi трафиком эффективнее маскироваться под него (Стратегия А), тогда как в промышленных зонах или сельской местности целесообразно использовать редкие сигналы (Стратегия В). Главным ограничением метода является необходимость точной синхронизации по времени между передатчиком и приемником, так как рассинхронизация приводит к резкому падению корреляционного пика.

Заключение

В рамках данной работы было выполнено комплексное исследование алгоритмов скрытой и надёжной передачи информации в беспроводных сетях на основе анализа временных паттернов, предложен комплекс алгоритмов для скрытой и надёжной передачи информации во временной области.

Основные результаты работы:

1. Разработана методика формирования базы временных паттернов с оценкой их автокорреляционных свойств.
2. Предложен алгоритм адаптивного выбора паттерна на основе анализа текущей востребованности в эфире.
3. Метод микромодуляции амплитуды позволяет внедрять полезную информацию без существенного искажения автокорреляционной функции паттерна, что обеспечивает надёжное извлечение данных.

Перспективным направлением исследований является расширение подхода на частотную область и разработка гибридных алгоритмов, адаптирующихся как во времени, так и по частоте.

Список литературы

1. Джанвеккьо С. Модельные скрытые временные каналы: автоматическое моделирование и уклонение / С. Джанвеккьо, Х. Ван, Д. Виджесекера, С. Яджодия // Lecture Notes in Computer Science. – 2008. – Т. 5230. – С. 211–230. – DOI: 10.1007/978-3-540-87403-4_12.

2. Головачев В. Ю. Практические оценки стойкости некоторых стеганографических систем / В. Ю. Головачев, Р. М. Ковалев, И. Н. Оков // Конфидент. – 2002. – № 6 (48).

3. Бонати Л. SteaL-TE: предоставление частной сотовой связи 5G как услуги с полностековой беспроводной стеганографией / Л. Бонати, С. Д'Оро, Ф. Рестуккья, С. Базаньи, Т. Мелодия // IEEE INFOCOM 2021 – IEEE Conference on Computer Communications. – 2021. – С. 1–10. – DOI: 10.1109/INFOCOM42981.2021.9488755.

4. Проскуряков В. Когнитивные радиосистемы в сетях тактического назначения / В. Проскуряков // Электронные компоненты. – 2014. – № 3. – С. 36–38.

5. Дусматов Д. Х. Когнитивное радио - новая беспроводная технология в недалеком будущем / Д. Х. Дусматов, Ж. К. Назирханов // АК ТТЕ. – 2009. – № 2 (9).

6. Разработка технологических и конструкторских платформ при топологических нормах менее 90 нм / Е. Грошева, А. Заревич, А. Денискина, К. Фатуллаева // BIO Web of Conferences. – 2024. – Т. 145. – С. 03018. – DOI 10.1051/bioconf/202414503018.

7. Компьютерное моделирование работы транзисторов и полупроводниковых приборов на его основе / А. В. Полуэктов, Ф. В. Макаренко, Р. Ю. Медведев // Моделирование систем и процессов. – 2023. – Т. 16, № 1. – С. 77–84. – DOI 10.12737/2219-0767-2023-16-1-77-84. – EDN LOLZMT.

8. Исследование способов защиты информации от утечки по акустическому и виброакустическому каналам / В. К. Зольников, С. А. Сазонова, А. И. Заревич, С. С. Башун // Моделирование систем и процессов. – 2025. – Т. 18, № 2. – С. 27–40.

9. Локальная устойчивость колебаний магнетрона со связанными резонаторами / А. И. Заревич, С. С. Новиков // Вестник науки Сибири. – 2013. – № 4 (10). – С. 109–114.

10. Моделирование колебательных процессов в пакете MVStadium / А. В. Полуэктов, К. В. Зольников, В. И. Анциферова // Моделирование систем и процессов. – 2021. – Т. 14, № 4. – С. 139–148. – DOI 10.12737/2219-0767-2021-14-4-139-148. – EDN PPOUDI.

11. Исследование эффективности защиты от гамма-излучения с использованием многослойного полусферического экрана / А. В. Полуэктов, А. И. Заревич, Ф. В. Макаренко, М. В. Солодилов // Моделирование систем и процессов. – 2025. – Т. 18, № 4. – С. 71–83.

12. Анализ количества потребления SF_6 и CF_4 для заправки коммутационной аппаратуры высокого напряжения / Н. Ю. Заленская, Ф. В. Макаренко, А. И. Заревич, А. В. Полуэктов // Известия высших учебных заведений. Проблемы энергетики. – 2024. – Т. 26, № 4. – С. 3–16. – DOI 10.30724/1998-9903-2024-26-4-3-16. – EDN HOOMCR.

References

1. Gianvecchio S. Model-based covert timing channels: automated modeling and evasion / S. Gianvecchio, H. Wang, D. Wijesekera, S. Jajodia // Lecture Notes in Computer Science. – 2008. – Vol. 5230. – P. 211-230. – DOI: 10.1007/978-3-540-87403-4_12.

2. Golovachev V. Yu. Practical estimates of the durability of some steganographic systems / V. Y. Golovachev, R. M. Kovalev, I. N. Okov // Confi-dent. – 2002. – № 6 (48).

3. Bonati L. SteaL-TE: Private 5G Cellular Connectivity as a Service with Full-stack Wireless Steganography / L. Bonati, S. D'Oro, F. Restuccia, S. Basagni, T. Melodia // IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. – 2021. – P. 1-10. – DOI: 10.1109/INFOCOM42981.2021.9488755.

4. Proskuryakov V. Cognitive radio systems in tactical networks / V. Proskuryakov // Electronic components. 2014. No. 3. pp. 36-38.

5. Dusmatov D. H. Cognitive radio – a new wireless technology in the near future / D. H. Dusmatov, J. K. Nazirkhanov // AK TTE. – 2009. – № 2 (9).

6. Development of technology and design platforms at topological norms less than 90 nm / E. Grosseva, A. Zarevich, A. Deniskina, K. Fatullaeva // BIO Web of Conferences. – 2024. – Vol. 145. – P. 03018. – DOI 10.1051/bioconf/202414503018.

7. Computer simulation of transistor operation and semiconductor devices based on it / A.V. Poluektov, F. V. Makarenko, R. Y. Medvedev // Modeling of systems and processes. – 2023. – Vol. 16, No. 1. – pp. 77-84. – DOI 10.12737/2219-0767-2023-16-1-77-84. – EDN LOLZMT.

8. V. K. Zolnikov, S. A. Sazonova, A. I. Zarevich, S. S. Bashun, Research of ways to protect information from leakage through acoustic and vibroacoustic channels // Modeling of systems and processes. 2025. Vol. 18, No. 2. pp. 27-40.

9. Local stability of magnetron oscillations with coupled resonators / A. I. Zarevich, S. S. Novikov // Bulletin of Siberian Science. – 2013. – № 4 (10). – Pp. 109-114.

10. Modeling of oscillatory processes in the MVStudium package / A.V. Poluektov, K. V. Zolnikov, V. I. Antsiferova // Modeling of systems and processes. – 2021.

– Vol. 14, No. 4. – pp. 139-148. – DOI 10.12737/2219-0767-2021-14-4-139-148. – EDN PPOUDI.

11. Poluektov A.V., Zarevich A. I., Makarenko F. V., Solodilov M. V. Investigation of the effectiveness of protection against gamma radiation using a multilayer hemispherical screen // Modeling of systems and processes. - 2025. – Vol. 18, No. 4. – pp. 71-83.

12. Analysis of the amount of SF₆ and cf₄ consumption for refueling high-voltage switching equipment / N. Y. Zalenskaya, F. V. Makarenko, A. I. Zarevich, A.V. Poluektov // Izvestiya vysshikh uchebnykh zavedeniy. Energy problems. – 2024. – Vol. 26, No. 4. – pp. 3-16. – DOI 10.30724/1998-9903-2024-26-4-3-16. – EDN HOOMCR.