Доклады ТУСУР. 2022 • Том 25, № 4

ISSN 1818-0442
DOI: 10.21293/1818-0442

ДОКЛАДЫ

Томского государственного университета систем управления и радиоэлектроники

2022 • Том 25, № 4

Министерство науки и высшего образования Российской Федерации

ДОКЛАДЫ ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

2022, том 25, № 4

Периодический научный журнал

Выходит 4 раза в год **ISSN 1818-0442**

Основан в 1997 г. **DOI: 10.21293/1818-0442**

Адрес редакции: 634050, г. Томск, пр. Ленина, 40, ТУСУР, тел. (382-2) 51-21-21

Свидетельство о регистрации МНС РФ № 1027000867068 от 13 октября 2004 г.

Учредитель: Томский государственный университет систем управления и радиоэлектроники

Подписной индекс 20648 в каталоге агентства «Урал-Пресс»: газеты и журналы.

Издательство Томского государственного университета систем управления и радиоэлектроники

634050, Томск, пр. Ленина, 40, тел. (382-2) 51-21-21.

Верстка, техническое редактирование, подготовка оригинал-макета В.М. Бочкаревой.

Корректор В.Г. Лихачева.

Подписано в печать 25.12.2022. Формат 60×84 1/8. Печ. л. 8,75. Тираж 500. Заказ 21. Цена 316 руб.

Editorial board

Содержание

ЭЛЕКТРОНИКА, РАДИОТЕХНИКА И СВЯЗЬ

УПРАВЛЕНИЕ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА

ЭЛЕКТРОТЕХНИКА

Contents

ELECTRONICS, RADIO ENGINEERING AND COMMUNICATIONS

CONTROL, COMPUTER SCIENCE AND INFORMATICS

ELECTRICAL ENGINEERING

ЭЛЕКТРОНИКА,
РАДИОТЕХНИКА И СВЯЗЬ

УДК 621.396.41

М. Исса, Д.Я. Суханов

Расширение зоны покрытия при связи вне прямой видимости MIMO с использованием пассивных ретрансляторов

Для системы связи с множеством излучателей и множеством приемников (MIMO) в городах слепые зоны в тени высоких зданий могут снизить качество связи. Эту проблему можно решить путем размещения пассивных ретрансляторов. Распределение этих ретрансляторов в MIMO-связи должно быть оптимизировано, чтобы максимально охватить целевую зону. Предлагается подход, основанный на алгоритме неотрицательных наименьших квадратов для оптимизации распределения минимального количества ретрансляторов в MIMO-связи вне прямой видимости. Рассматриваются пассивные ретрансляторы, состоящие из двух параболических антенн, соединенных через гибкий кабель. Путём численного моделирования представлен пример применения данного метода для типичной городской застройки. Получено оптимальное распределение ретрансляторов для покрытия заданной области минимальным количеством ретрансляторов.

Ключевые слова: MIMO, вне прямой видимости, NNLS, слепые зоны, пассивный ретранслятор.
DOI: 10.21293/1818-0442-2022-25-4-7-12

Технологии MIMO повышают пропускную способность радиоволнового канала связи [1]. Однако в условиях отсутствия прямой видимости слепые зоны, в которых блокируется радиоволна от базовых станций из-за высоких зданий или естественных препятствий, могут значительно снизить качество связи [2]. Ранее были разработаны различные подходы для расширения покрытия и доступа к слепым зонам в связи MIMO. В [3, 4] активные ретрансляторы используются для расширения покрытия и улучшения качества канала в системах мобильной связи 5G. Для расширения покрытия также предлагаются отражающие поверхности [5].

Авторы [6] предложили «MilliMirror» – полностью пассивную метаповерхность, изготовленную с помощью 3D-печати. «MilliMirror» может изменять форму и направлять лучи миллиметровых волн в аномальных направлениях для освещения слепых зон. В [7] предложены реконфигурируемые интеллектуальные поверхности для обеспечения контролируемого и сфокусированного отражения в направлении приемника, когда отсутствует связь в прямой видимости. Использование пассивных ретрансляторов для улучшения радиопокрытия внутри здания также исследуется во многих работах [8, 9].

Авторы [10] предложили размещать пассивные ретрансляторы на стенах, чтобы улучшить интернет-покрытие в домах в сельской Африке и снизить затухание в стене. Предлагаемый пассивный ретранслятор состоит из двух антенн, размещенных по обеим сторонам стены, две антенны соединены кабелем с пассивным фазовращателем. В [11] представлен и исследован массив пассивных ретрансляторов, который может отражать падающую мощность под определенным углом для устранения слепых зон для системы фиксированного беспроводного доступа 5G.

В [12, 13] система ретрансляторов на основе параболических рефлекторов (рис. 1) используется для манипулирования средой распространения как при прямой видимости, так и при MIMO-связи без прямой видимости. В [12] предложен алгоритм соответствующего распределения ретрансляторов для расширения покрытия в условиях отсутствия прямой видимости.

Рис. 1. Пассивный ретранслятор, состоящий из двух параболических антенн, соединённых гибким кабелем

В этой статье предлагается использовать пассивный ретранслятор, показанный на рис. 1, для расширения зоны покрытия в условиях связи вне прямой видимости. Ретрансляторы используются для непосредственной связи с абонентами или в качестве промежуточного звена для максимально возможного расширения зоны покрытия.

Расположение и направление ретрансляторов оптимизируются с использованием алгоритма неотрицательных наименьших квадратов (NNLS). Проверка предложенного подхода производится численным расчетом. Результаты показывают, что в условиях отсутствия прямой видимости предложенный алгоритм позволяет расширить зону покрытия, а также оптимизировать количество ретрансляторов, их местоположение и направление в соответствии с их вкладом в покрытие целевой области.

Конфигурация ретранслятора и диаграмма направленности

Предлагаемый пассивный ретранслятор состоит из двух частей. Оба представляют собой параболические отражатели с антеннами в фокусе. Первая часть направлена на базовую станцию в прямой видимости, а вторая часть направлена на абонентов. Первая часть антенны соединена со второй частью антенны гибкой микроволновой соединительной линией. Длина линии выбирается в соответствии с требованиями к размещению первой и второй частей.

Предлагаемый пассивный ретранслятор имеет следующие преимущества:

– не применяются активные радиоэлектронные компоненты или фазовращатели, ретранслятор полностью пассивный. Части ретранслятора направляются вручную в требуемую область;

– выбор размера параболического рефлектора позволяет задавать ширину луча;

– возможность использования разных поляризаций для двух частей ретранслятора обеспечивает предотвращение интерференции между прямой волной и волной от пассивного ретранслятора. При одинаковых поляризациях, если две волны не совпадают по фазе, может уменьшиться амплитуда поля. Кроме того, размещение рядом двух ретрансляторов с ортогональной поляризацией позволяет удвоить количество независимых каналов связи MIMO.

Диаграмма направленности параболического рефлектора определяется его размером и полем облучающей антенны, расположенной в фокусе параболы. Могут использоваться различные облучающие антенны, например, дипольный облучатель Герца, волноводный облучатель и рупорный облучатель [14]. Поле дальней зоны параболического отражателя можно аппроксимировать полем излучения круглой апертуры [12]

$$E(\phi) = G\frac{J_1(\pi D\sin\phi/\lambda)}{\pi D\sin\phi}\frac{2\lambda}{r}\exp(ikr), \qquad (1)$$

где J_1 – функция Бесселя первого порядка; D – диаметр апертуры параболической антенны ретранслятора на стороне абонента; r – расстояние между ретранслятором и местоположением абонента; k – волновое число; λ – длина волны; G – коэффициент усиления ретранслятора; ϕ – угол между положением абонента и ретранслятором относительно направления основного луча ретранслятора в сторону абонента.

Алгоритм оптимизации для расширения охвата в средах MIMO вне прямой видимости

Результатом алгоритма оптимизации должны быть координаты и направления минимального количества ретрансляторов, обеспечивающих интенсивность поля, пропорциональную вероятности нахождения абонентов в заданной области.

Явления отражения, преломления и дифракции вызывают непрямое распространение передаваемых сигналов, что можно использовать для расширения охвата слепых зон. Ранее авторы в [12] предложили алгоритм поиска размещения и направления для каждого ретранслятора на основе максимизации интенсивности поля в заданных областях.

В этой статье применение пассивных ретрансляторов для связи вне прямой видимости обобщается за счет использования промежуточных пассивных ретрансляторов с высоким усилением и направленностью для расширения покрытия на большие расстояния. Идея состоит в том, что эти промежуточные ретрансляторы имеют связь в пределах прямой видимости с базовой станцией, а также связь в пределах прямой видимости с другими ретрансляторами, которые отвечают за покрытие удаленных областей.

Ретрансляторы могут непосредственно облучать абонентов или работать в качестве промежуточного звена между базовой станцией и другими ретрансляторами для максимального расширения зоны покрытия.

Местоположения и направления ретрансляторов оптимизируются с использованием алгоритма, основанного на неотрицательном алгоритме наименьших квадратов. Рассматриваются неотрицательные весовые коэффициенты для каждого возможного ретранслятора, которые вычисляются в ходе оптимизации. Если весовой коэффициент ретранслятора окажется ниже определённого порога, то данный ретранслятор устраняется. Объяснение NNLS описано в [15].

Для предлагаемого алгоритма определения оптимального количества, координат и направления ретрансляторов требуется задать три входных параметра:

1. Пространственное статистическое распределение абонентов $D(x_m, y_m)$ со значениями от 0 до 1 для определения важности местоположения каждого m-го абонента, $m = 1...M$. Каждое значение пропорционально вероятности занятия соответствующего местоположения абонентами.

2. Множество всех возможных размещений и направлений ретрансляторов. Обозначим N – количество всех рассматриваемых вариантов ретрансляторов; $\mathbf{p}_n$ – координаты n-го ретранслятора и α_n – угол направления второй части ретранслятора, $n = 1...N$. Заранее определенные места размещения должны гарантировать, что первая часть каждого используемого ретранслятора может установить связь с базовой станцией или с промежуточным ретранслятором в прямой видимости.

3. Матрица $\mathbf{A}_{N\times M}$, описывающая интенсивность поля n-го ретранслятора для m-го абонента, где каждая строка A_n содержит интенсивность в местоположениях абонентов (x_m, y_m), создаваемую ретранслятором с заданным местоположением $\mathbf{p}_n$ и направлением α_n. Распределенная интенсивность рассчитывается с использованием метода конечных разностей во временной области (FDTD). Суммарная интенсивность поля в области размещения абонентов рассчитывается как взвешенная сумма интенсивностей всех ретрансляторов:

$$w_m = \sum_n A_{n,m}c_n,$$

где c_n – весовой коэффициент n-го ретранслятора. Рассматривается суммирование полей по интенсивности, поскольку заранее не известна форма сигналов, и их можно считать случайными.

Потребуем, чтобы ретрансляторы обеспечивали интенсивность поля, пропорциональную распределению абонентов $D_m = D(x_m, y_m)$. Введём обозна-

чение $W_m = \gamma \sum_n A_{n,m} c_n$, где коэффициент γ имеет размерность, обратную интенсивности. Коэффициент γ неизвестен. Включим его в весовой коэффициент, введя обозначение $C_n = \gamma c_n$, тогда

$$W_m = \sum_n A_{n,m} C_n . \quad (2)$$

Метод NNLS используется для нахождения неотрицательных размерных коэффициентов C_n из (2), обеспечивая минимизацию выражения:

$$||D - AC||^2 . \quad (3)$$

В результате будут определены коэффициенты $C_n \geq 0$, описывающие вклад каждого ретранслятора при оптимальном охвате всех абонентов.

NNLS основан на методе наименьших квадратов с ограничением области поиска решения только неотрицательными значениями. Ограничение поиска неотрицательных значений связано с суммированием полей по интенсивности, поскольку интенсивность не может быть отрицательной.

Если C_n окажется меньше заданного порога, то соответствующий ретранслятор устраняется. Может определяться из требований минимизации количества ретрансляторов. То есть выбирается достаточно высоким, чтобы оставить только требуемое количество ретрансляторов с наибольшей значимостью.

В итоге алгоритм оптимального размещения ретрансляторов состоит из следующих шагов:

1. Задать пространственное распределение вероятности присутствия абонентов $D(x_m, y_m)$.

2. Задать все возможные положения ретрансляторов и их направлений $\{\mathbf{p}_n, \alpha_n\}$.

3. Вычислить интенсивность поля от ретранслятора $\{\mathbf{p}_n, \alpha_n\}$ в области абонентов путём численного моделирования распространения волн.

4. Сформировать матрицу $\mathbf{A}_{N \times M}$, описывающую интенсивность поля *n*-го ретранслятора в точке размещения *m*-го абонента.

5. Методом NNLS вычислить весовые коэффициенты C_n для оптимального охвата всех абонентов пропорционально вероятности их наличия.

6. Отбросить ретрансляторы, весовой коэффициент C_n которых меньше заданного порога.

Моделирование и обсуждение

Рассмотрена часть г. Томска (Россия) для анализа сценария связи вне прямой видимости, как показано на рис. 2. Статистическое пространственное распределение абонентов *D* показано на рис. 3. Количество вероятных положений абонентов *M* = 36248. Координаты абонентов выбраны с шагом 1,6 м. Видно, что базовая станция не может установить связь прямой видимости с абонентами.

В качестве множества возможного размещения ретрансляторов ($\mathbf{p}_n$) рассматриваются точки на крышах первого ряда зданий, как показано на рис. 2, где базовая станция может установить связь прямой видимости с ретрансляторами, а также ретрансляторы не затеняют друг друга.

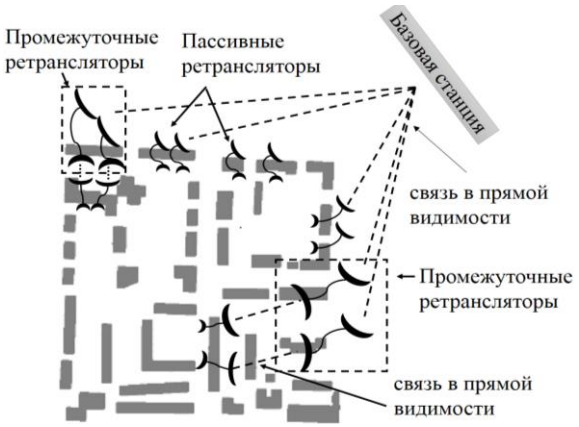


Рис. 2. Схема размещения ретрансляторов для связи MIMO вне прямой видимости

Две области *R*3 и *R*4 (рис. 3) находятся далеко от первого ряда зданий с множеством зданий посередине. Для передачи сигнала в эти области используются промежуточные ретрансляторы, как показано на рис. 2. Первая часть и вторая часть каждого промежуточного ретранслятора имеют связь в пределах прямой видимости с высоким усилением и направлением с базовой станцией и другим ретранслятором соответственно.

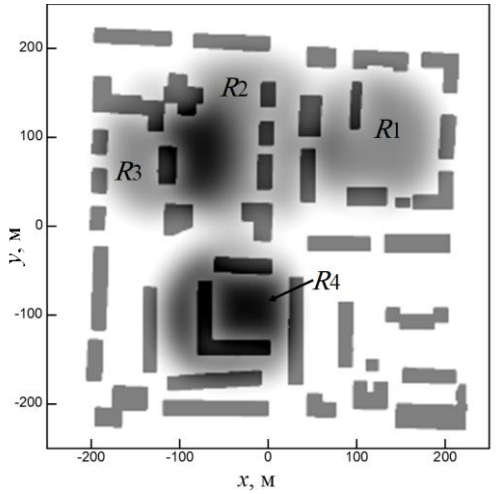


Рис. 3. Пространственное распределение вероятности наличия абонентов *D*(*x*, *y*)

Ретрансляторы распределяются по крышам, как показано на рис. 4. Для каждого местоположения ретранслятора тестируются разные варианты направления второй части ретранслятора. Общее количество вариантов (местоположения и направления ретрансляторов) составляет *N* = 125.

Для каждого местоположения и направления вычисляется поле ретранслятора методом FDTD. На рис. 5 показан результат расчёта интенсивности поля методом FDTD для ретранслятора в точке *x* = –60 м, *y* = 200 м. Для упрощения решения рассматривалась двумерная модель, что не принципиально для сути предлагаемого алгоритма. В качестве сигнала рассматривался короткий биполярный импульс с частотой до 100 МГц. Интенсивность поля в каждой точке вычислялась как интеграл по времени от квадрата

амплитуды поля. Согласно теореме Парсеваля, данная интенсивность равна суммарной интенсивности во всём диапазоне частот.

Рис. 4. Распределение ретрансляторов по крышам зданий

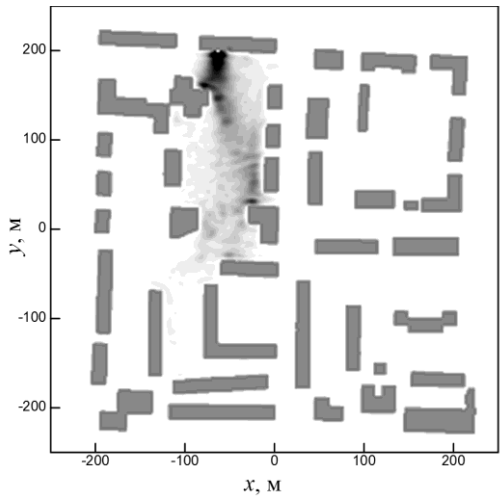


Рис. 5. Результат численного моделирования интенсивности поля методом FDTD для одного ретранслятора

На основе вычисления интенсивностей для всех вариантов ретрансляторов строится матрица **A.** После применения NNLS C_n описывает вес каждого ретранслятора и определяет, насколько он способствует охвату абонентов.

В данном примере вклад каждого варианта в охват абонентов считается приемлемым, если он составляет не менее 15% от максимального вклада из рассмотренных вариантов. После устранения ретрансляторов с малым весом из 125 вариантов осталось 15 вариантов. Зона покрытия, полученная от этих 15 ретрансляторов, показана на рис. 6. Видно, что целевые области охвачены.

При использовании промежуточных ретрансляторов зона покрытия распространяется на отдаленные регионы, как показано на рис. 6. Промежуточные ретрансляторы устанавливаются отдельно после алгоритма оптимизации, если в результате останутся ретрансляторы, недоступные напрямую для базовой станции.

Полученный результат размещения ретрансляторов представляется оптимальным, поскольку обеспечивает охват заданных областей минимальным количеством ретрансляторов.

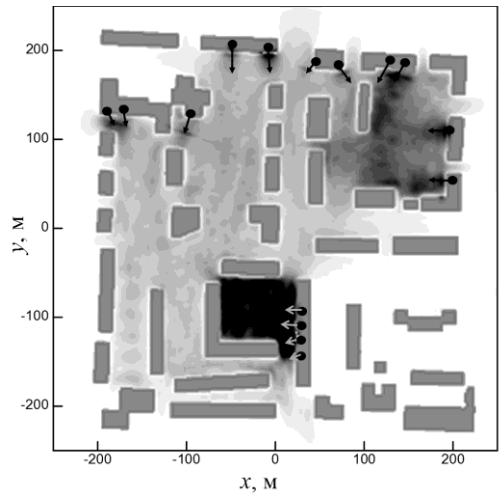


Рис. 6. Результат применения алгоритма NNLS: результирующая зона покрытия – суммарная интенсивность поля

Заключение

Предложено применение пассивных ретрансляторов для расширения покрытия и доступа к слепым зонам в MIMO-связи. Рассматриваемый ретранслятор состоит из двух частей, соединенных гибким кабелем. Каждая часть представляет собой параболический рефлектор с антенной в фокусе. Эти ретрансляторы используются либо для непосредственного охвата абонентов, либо в качестве промежуточного звена между базовой станцией и другими ретрансляторами.

Подход, основанный на неотрицательном алгоритме наименьших квадратов, используется для оптимизации распределения ретрансляторов в среде распространения. Оптимизация обеспечивает пропорциональное соответствие интенсивности поля и распределения абонентов в пространстве. Если вклад ретранслятора в освещение пользователей меньше заранее определенного порога, ретранслятор не используется.

Численное моделирование для определения полей ретрансляторов позволяет учесть существенные эффекты отражения и дифракции в конкретной обстановке. За счёт метода наименьших квадратов определяется минимальное множество ретрансляторов, обеспечивающих наибольший вклад в охват области вероятного расположения абонентов.

Применимость метода была проверена численно на примере части г. Томска, что показало возможность оптимального расширения зоны покрытия с минимальным количеством ретрансляторов.

Результаты были получены в рамках выполнения государственного задания Минобрнауки России, проект № FSWM-2020-0038.

Литература

1. Hampton J.R. Introduction to MIMO Communications. – NY: Cambridge University Press, 2014. – 288 p.

2. cDERSA: Cognitive D2D enabled relay selection algorithm to mitigate blind-spots in 5G cellular networks /

A. Iqbal, M. Rahim, R. Hussain, A. Noorwali, M.Z. Khan, A. Shakeel, I.L. Khan, M.A. Javed, Q.U. Hasan, S.A. Malik // IEEE Access. – 2021. – Vol. 9. – P. 89972–89988.

3. Relaying operation in 3GPP LTE: challenges and solutions / C. Hoymann, W. Chen, J. Montojo, A. Golitschek, C. Koutsimanis, X. Shen // IEEE Communications Magazine. – 2012. – Vol. 50. – P. 156–162.

4. Relay technologies for WiMAX and LTE-advanced mobile systems / Y. Yang, H. Hu, J. Xu, G. Mao // IEEE Communications Magazine. – 2009. – Vol. 47. – P. 100–105.

5. Beyond intelligent reflecting surfaces: Reflective-transmissive metasurface aided communications for full-dimensional coverage extension / S. Zhang, H. Zhang, B. Di, Y. Tan, Z. Han, L. Song // IEEE Trans. Veh. Technol. – 2020. – Vol. 69. – P. 13905–13909.

6. MilliMirror: 3D Printed Reflecting Surface for Millimeter-Wave Coverage Expansion / K. Qian, L. Yao, X. Zhang, T.N. Ng // MobiCom '22: Proceedings of the 28th Annual International Conference on Mobile Computing And Networking. – 2022. – P. 15–28.

7. Reflecting surfaces for beyond line-of-sight coverage in millimeter wave vehicular networks / K. Heimann, A. Marsch, B. Sliwa, C. Wietfeld // Proc. IEEE Veh. Netw. Conf. – 2020. – P. 1–4.

8. Huang Y. Investigation of using passive repeaters for indoor radio improvement / Y. Huang, N. Yi, X. Zhu // Proc. IEEE Int. Symp. Antennas Propag. – 2004. – Vol. 2. – P. 1623–1626.

9. Honma N. Manipulating MIMO propagation environment using tunable passive repeater / N. Honma, Y. Takahashi, Y. Tsunekawa // Proc. of IEEE Asia-Pacific Microwave Conference (APMC). – 2014. – P. 504–506.

10. Lynggaard P. Improving internet coverage in rural Africa by using passive repeaters in the home // Nordic and Baltic Journal of Information and Communications Technologies. – 2016. – Vol. 1. – P. 65–80.

11. Passive repeater for removal of blind spot in NLOS path for 5G fixed wireless access (FWA) system / D. Ha, D. Choi, H. Kim, J. Kum, J. Lee, Y. Lee // IEEE International Symposium on Antennas and Propagation USNC/URSI National Radio Science Meeting. – 2017. – P. 2049–2050.

12. Sukhanov D.Y. Manipulating LOS and NLOS MIMO Propagation Environments Using Passive Repeaters / D.Y. Sukhanov, M. Eissa // Progress In Electromagnetics Research M. – 2021. – Vol. 105. – P. 195–204.

13. Eissa M. Enhancing performance in a LOS MIMO communication using a passive repeater / M. Eissa, D. Sukhanov // Journal of Physics: Conference Series. – 2021. – Vol. 2140. – P. 012013.

14. Orfanidis S.J. Electromagnetic Waves and Antennas. – Rutgers University, 2016. – 1413 p.

15. Bro R. A fast non-negativity-constrained least squares algorithm / R. Bro, S.D. Jong // Journal of Chemometrics. – 1997. – Vol. 11. – P. 393–401.

Исса Махмуд
Аспирант каф. радиофизики радиофизического факультета (РФФ) Национального исследовательского Томского государственного университета (НИ ТГУ)
Ленина пр-т, 36, г. Томск, Россия, 634050
ORCID: 0000-0003-1647-9688
Тел.: +7-913-115-09-86
Эл. почта: mahmoud.eissa@stud.tsu.ru

Суханов Дмитрий Яковлевич
Д-р физ.-мат. наук, каф. радиофизики РФФ НИ ТГУ
Ленина пр-т, 36, г. Томск, Россия, 634050
ORCID: 0000-0002-0805-4543
Тел.: +7 (382-2) 41-25-83
Эл. почта: sdy@mail.tsu.ru

Eissa M., Sukhanov D.Y.

Extending coverage area in none line-of-sight MIMO communications using passive repeaters

In MIMO communications, high buildings in cities and other obstructions can prevent the propagation of radio waves, resulting in blind spots and poor communications. This problem can be solved using passive repeaters, which, by distributing them in the communication environment, the blind spots can be accessed and the coverage area can be extended. The distribution of these repeaters in the MIMO communication should be optimized in order to maximally cover the target area. In this article, an approach based on non-negative least square (NNLS) algorithm is proposed for optimizing the distribution of the minimum number of repeaters in none-line-of sight (NLOS) MIMO communications. The proposed approach is implemented using passive repeaters consisting of two parabolic antennas connected through a flexible cable. The numerical analysis is performed to verify the validity of the proposed approach, and it is found that the proposed method helps to optimally distribute passive repeaters and extend coverage area with minimum number of repeaters.

Keywords: MIMO, non-line-of-sight, NNLS, blind spots, passive repeater.
DOI: 10.21293/1818-0442-2022-25-4-7-12

References

1. Hampton J.R. *Introduction to MIMO communications.* New York, Cambridge University Press, 2014. 288 p.

2. Iqbal A., Rahim M., Hussain R. Noorwali A., Khan M.Z., Shakeel A., Khan I.L., Javed M.A., Hasan Q.U., Malik S.A. cDERSA: Cognitive D2D enabled relay selection algorithm to mitigate blind-spots in 5G cellular networks. *IEEE Access*, 2021, vol. 9, pp. 89972–89988.

3. Hoymann C., Chen W., Montojo J., Golitschek A., Koutsimanis C., Shen X. Relaying operation in 3GPP LTE: challenges and solutions. *IEEE Communications Magazine*, 2012, vol. 50, pp. 156–162.

4. Yang Y., Hu H., Xu J., Mao G. Relay technologies for WiMAX and LTE-advanced mobile systems. *IEEE Communications Magazine*, 2009, vol. 47, pp. 100–105.

5. Zhang S., Zhang H., Di B., Tan Y., Han Z., Song L. Beyond intelligent reflecting surfaces: Reflective-transmissive metasurface aided communications for full-dimensional coverage extension. *IEEE Transactions on Vehicular Technology*, 2020, vol. 69, pp. 13905–13909.

6. Qian K., Yao L., Zhang X., Ng T.N. MilliMirror: 3D Printed Reflecting Surface for Millimeter-Wave Coverage Expansion. *MobiCom '22: Proceedings of the 28th Annual International Conference on Mobile Computing and Networking*, 2022, pp. 15–28.

7. Heimann K., Marsch A., Sliwa B., Wietfeld C. Reflecting surfaces for beyond line-of-sight coverage in millimeter wave vehicular networks. *Proceedings of IEEE IEEE Vehicular Networking Conference*, 2020, pp. 1–4.

8. Huang Y., Yi N., Zhu X. Investigation of using passive repeaters for indoor radio improvement. *Proceedings of IEEE International Symposium on Antennas and Propagation Society*, 2004, vol. 2, pp. 1623–1626.

9. Honma N., Takahashi Y., Tsunekawa Y. Manipulating MIMO propagation environment using tunable passive repeater. *Proceedings of IEEE Asia-Pacific Microwave Conference (APMC)*, 2014, pp. 504–506.

10. Lynggaard P. Improving internet coverage in rural Africa by using passive repeaters in the home. *Nordic and Baltic Journal of Information and Communications Technologies*, 2016, vol. 1, pp. 65–80.

11. Ha D., Choi D., Kim H., Kum J., Lee J., Lee Y. Passive repeater for removal of blind spot in NLOS path for 5G fixed wireless access (FWA) system. *IEEE International Symposium on Antennas and Propagation USNC/URSI National Radio Science Meeting*, 2017, pp. 2049–2050.

12. Sukhanov D.Y., Eissa M. Manipulating LOS and NLOS MIMO Propagation Environments Using Passive Repeaters. *Progress In Electromagnetics Research M*, 2021, vol. 105, pp. 195–204.

13. Eissa M., Sukhanov D. Enhancing performance in a LOS MIMO communication using a passive repeater. *Journal of Physics: Conference Series*, 2021, vol. 2140, pp. 012013.

14. Orfanidis S.J. *Electromagnetic Waves and Antennas.* Rutgers University, 2016. 1413 p.

15. Bro R., Jong S.D. A fast non-negativity-constrained least squares algorithm. *Journal of Chemometrics*, 1997, vol. 11, pp. 393–401.

Mahmoud Eissa
Postgraduate student, Department of Radiophysics,
Faculty of Radiophysics, Tomsk State University (TSU)
36, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0003-1647-9688
Phone: +7-913-115-09-86
Email: mahmoud.eissa@stud.tsu.ru

Dmitry Y. Sukhanov
Doctor of Science in Physics and Mathematics,
Department of Radiophysics, Faculty of Radiophysics, TSU
36, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0002-0805-4543
Phone: +7 (382-2) 41-25-83
Email: sdy@mail.tsu.ru

УДК 621.396.41

А.П. Горбачев, Ю.Н. Паршин

Синтез широкополосных дифференциальных фазовращателей на электромагнитно связанных линиях для многолучевых антенных решёток*

Работа посвящена синтезу дифференциальных фазовращателей на электромагнитно связанных линиях с замкнутым кольцевым проводником. По сравнению с известными фазовращателями предлагаемая структура характеризуется дополнительными степенями свободы при печатном полосковом исполнении и обеспечивает возможность проектирования многолучевых эквидистантных фазированных антенных решёток с рабочими полосами частот до полутора октав при условии, что излучатели их антенных полотен характеризуются такой же широкополосностью, например, печатные логопериодические излучатели. При узкополосных излучателях открывается возможность реализации двухчастотного или многочастотного режима работы многолучевой антенной решётки.

Ключевые слова: дифференциальный фазовращатель, связанные полосковые линии, направленный ответвитель, антенные решетки.
DOI: 10.21293/1818-0442-2022-25-4-13-18

Многолучевые фазированные антенные решетки (ФАР) находят широкое применение в радиотехнических и инфокоммуникационных системах, обеспечивающих разнонаправленное излучение радиосигналов при неподвижной антенной системе [1]. Такие ФАР востребованы при организации радиосвязи с вахтовыми поселками геологов, нефтяников, газовиков, группами охотников и туристов с одной базовой радиопередающей станции. Они же используются также в радиолокации и наведении ракет на воздушную цель, когда зондирующий сигнал излучается на одной частоте, а ответный – на другой, причем возвращается он в точку излучения с направлений, положение которых в окружающем пространстве заранее неизвестно.

За истекшие десятилетия элементная база многолучевых ФАР непрерывно совершенствовалась, начиная с прямоугольных волноводов и дойдя до микроэлектронных узлов диапазона 60 ГГц. Однако существует и сейчас ключевое ограничение, которое следует учитывать при проектировании таких ФАР. Дело в том, что излучающие элементы антенной решетки находятся в окружающем свободном пространстве, где зачастую нельзя широко применять какие-либо диэлектрики из-за необходимости иметь высокую линейность поляризации радиоизлучения. Ибо наличие кросс-поляризационного излучения многолучевой антенны приводит к существенным ошибкам определения угловых координат и дальности воздушной цели. Поэтому распределительная система многолучевых ФАР и интегрированные с ней излучатели всё ещё продолжают реализовываться по технологии симметричных полосковых линий, что и нашло отражение в данной работе, поскольку поиск путей их модернизации и совершенствования остается актуальным и сегодня.

Синтез дифференциальных фазовращателей на связанных линиях с ТЕМ-волнами

Дифференциальные фазовращатели (ДФВ) являются базовыми элементами диаграммообразующих устройств многолучевых ФАР [1]. От эффективности их функционирования зависит точность установки луча (максимума диаграммы направленности) ФАР в окружающем пространстве. Поэтому не ослабевает внимание к интенсивному поиску новых структур таких фазовращателей и разработке методов их проектирования в печатном исполнении [2–14]. В настоящей работе предлагается новая структура широкополосных ДФВ на основе направленных ответвителей (НО) на электромагнитно связанных линиях при условии распространения в них ТЕМ-волн, а также описываются этапы разработанной методики их проектирования.

Идея построения ДФВ, структурно-компоновочная схема которого защищена патентом [15], основана на ряде результатов работ [16, 17]. На рис. 1 представлена эквивалентная схема ДФВ, где обозначено: 1^F, 2^F – вход и выход ДФВ; *1*, *2* – связанные линии первого восьмиполюсника; 1', 2', 3', 4' – плечи первого восьмиполюсника; *3*, *4* – связанные линии второго восьмиполюсника; 1", 2", 3", 4" – плечи второго восьмиполюсника.

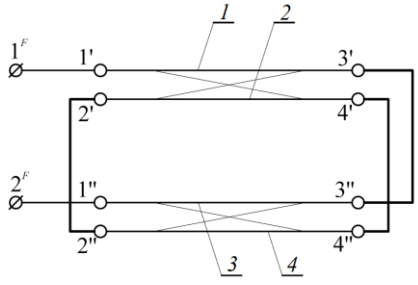


Рис. 1. Эквивалентная схема ДФВ

* Материал частично опубликован. См. Паршин Ю.Н. Печатные многолучевые антенные решётки с модифицированными фазовращателями и излучателями дипольного вида: дис. ... канд. техн. наук / Паршин Юрий Николаевич. – Новосибирск, 2022. – 198 с.

Таким образом, анализируемый ДФВ образован совокупностью двух четвертьволновых НО на связанных линиях *1*, *2* и *3*, *4*, у которых объединены по одной из связанных линий *2* и *4* в кольцевой проводник.

Пусть ко входу 1^F ДФВ подводится гармоническое СВЧ-напряжение $u_{1F}(t)$ с амплитудой U_m, неизменное в полосе частот порядка двух октав:

$$u_{1F}(t) = U_m \cos(\omega t + \varphi_{1F}) = U_m \cos(2\pi f t + \varphi_{1F}), \quad (1)$$

где U_m – амплитуда напряжения; ω – текущая круговая частота; f – текущая циклическая частота; φ_{1F} – начальная фаза сигнала.

Оно создаёт СВЧ-токи в связанных линиях *1*, *2* и *3*, *4*, которые за счёт связи с замкнутым кольцевым проводником из линий *2* и *4* формируют в нём циркулирующую бегущую волну. Последнее обусловливает в установившемся режиме поддержание неизменным по модулю выходного напряжения $u_{2F}(t)$ ДФВ, причём

$$u_{2F}(t) = u_{1F}(t) e^{j\psi}, \quad (2)$$

где ψ – вносимый фазовый сдвиг.

В результате ДФВ формирует задержку ψ между входным $u_{1F}(t)$ (1) и выходным $u_{2F}(t)$ (2) напряжениями. К тому же фазочастотная характеристика ψ(*f*) в широкой полосе частот, будучи подверженной влиянию циркулирующей в замкнутом кольцевом проводнике волны, принимает нелинейную форму.

Согласно общепринятой классификации, восьмиполюсники с нумерацией плеч 1', 2', 3', 4' и 1", 2", 3", 4" являются противонаправленными квадратурными четвертьволновыми ответвителями с матрицами рассеяния [**S**'] и [**S**"] и коэффициентами связи k_{12}, k_{34} соответственно (3).

Так как электрическая длина отрезков 2'–2", 4'–4" при реализации значительно короче длин линий 1'–3', 1"–3", то в дециметровом диапазоне волн их электрической длиной можно пренебречь. Кроме того, при надлежащем конструктивном исполнении электрические длины отрезков 1^F–1', 2^F–1" также являются достаточно малыми по сравнению с длинами отрезков 1'–3', 1"–3", так что и ими можно пренебречь. Поэтому целесообразно представить ДФВ в виде четырёхполюсника (4) с плечами 1^F и 2^F, который будет иметь матрицу рассеяния [$\mathbf{S}^F$] со структурой, определяемой согласно [18. С. 259] по уже известным матрицам рассеяния восьмиполюсников [**S**'] и [**S**"] (3).

Для нахождения элементов матрицы [$\mathbf{S}^F$] подставим в (4) соответствующие матрицы, получаем матрицу (5).

$$[\mathbf{S}'] = \begin{bmatrix} 0 & S'_{1F} & S'_{2F} & 0 \\ S'_{1F} & 0 & 0 & S'_{2F} \\ S'_{2F} & 0 & 0 & S'_{1F} \\ 0 & S'_{2F} & S'_{1F} & 0 \end{bmatrix}, \quad [\mathbf{S}''] = \begin{bmatrix} 0 & S''_{1F} & S''_{2F} & 0 \\ S''_{1F} & 0 & 0 & S''_{2F} \\ S''_{2F} & 0 & 0 & S''_{1F} \\ 0 & S''_{2F} & S''_{1F} & 0 \end{bmatrix}, \quad (3)$$

$$S'_{1F} = j\frac{k_{12}\sin\theta}{\sqrt{1-k_{12}^2}\cos\theta + j\sin\theta}, \quad S'_{2F} = \frac{\sqrt{1-k_{12}^2}}{\sqrt{1-k_{12}^2}\cos\theta + j\sin\theta},$$

$$S''_{1F} = j\frac{k_{34}\sin\theta}{\sqrt{1-k_{34}^2}\cos\theta + j\sin\theta}, \quad S''_{2F} = \frac{\sqrt{1-k_{34}^2}}{\sqrt{1-k_{34}^2}\cos\theta + j\sin\theta},$$

здесь $\theta = (\pi/2)(f/f_0)$ – электрическая длина полосковых линий *1*, *2*, *3*, *4* каждого НО (см. рис. 1); f_0 – центральная частота; f – текущая частота.

$$\left[\mathbf{S}^F\right] = \begin{bmatrix} S_{11}^F & S_{12}^F \\ S_{21}^F & S_{22}^F \end{bmatrix} = [\mathbf{S}_{PP}] + [\mathbf{S}_{PC}]\left([\mathbf{F}] - [\mathbf{S}_{CC}]\right)^{-1}[\mathbf{S}_{CP}],$$

$$[\mathbf{S}_{PP}] = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad [\mathbf{S}_{PC}] = \begin{bmatrix} S'_{2F} & 0 & 0 & 0 & S'_{1F} & 0 \\ 0 & S''_{2F} & 0 & 0 & 0 & S''_{1F} \end{bmatrix}, \quad (4)$$

$$[\mathbf{F}] = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, [\mathbf{S}_{CC}] = \begin{bmatrix} 0 & 0 & S'_{1F} & 0 & 0 & 0 \\ 0 & 0 & 0 & S''_{1F} & 0 & 0 \\ S'_{1F} & 0 & 0 & 0 & S'_{2F} & 0 \\ 0 & S''_{1F} & 0 & 0 & 0 & S''_{2F} \\ 0 & 0 & S'_{2F} & 0 & 0 & 0 \\ 0 & 0 & 0 & S''_{2F} & 0 & 0 \end{bmatrix}, [\mathbf{S}_{CP}] = \begin{bmatrix} S'_{2F} & 0 \\ 0 & S''_{2F} \\ 0 & 0 \\ 0 & 0 \\ S'_{1F} & 0 \\ 0 & S''_{1F} \end{bmatrix}.$$

$$[\mathbf{F}]-[\mathbf{S}_{CC}]=\begin{bmatrix} 0 & 1 & -S'_{1F} & 0 & 0 & 0 \\ 1 & 0 & 0 & -S''_{1F} & 0 & 0 \\ -S'_{1F} & 0 & 0 & 1 & -S'_{2F} & 0 \\ 0 & -S''_{1F} & 1 & 0 & 0 & -S''_{2F} \\ 0 & 0 & -S'_{2F} & 0 & 0 & 1 \\ 0 & 0 & 0 & -S''_{2F} & 1 & 0 \end{bmatrix}, \quad \left([\mathbf{F}]-[\mathbf{S}_{CC}]\right)^{-1}=\begin{bmatrix} [\mathbf{S}_{R11}] & [\mathbf{S}_{R12}] \\ [\mathbf{S}_{R21}] & [\mathbf{S}_{R22}] \end{bmatrix}, \quad (5)$$

$$[\mathbf{S}_{R11}]=\begin{bmatrix} 0 & \frac{S'_{2F}S''_{2F}-1}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & \frac{-S''_{1F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} \\ \frac{S'_{2F}S''_{2F}-1}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & 0 & 0 \\ \frac{-S''_{1F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & 0 & 0 \end{bmatrix},$$

$$[\mathbf{S}_{R12}]=\begin{bmatrix} 0 & 0 & \frac{-S''_{1F}S'_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} \\ \frac{-S'_{1F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & \frac{-S'_{1F}S''_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & 0 \\ \frac{-1}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & \frac{-S''_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & 0 \end{bmatrix},$$

$$[\mathbf{S}_{R21}]=\begin{bmatrix} 0 & \frac{-S'_{1F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & \frac{-1}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} \\ 0 & \frac{-S'_{1F}S''_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & \frac{-S''_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} \\ \frac{-S''_{1F}S'_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & 0 & 0 \end{bmatrix},$$

$$[\mathbf{S}_{R22}]=\begin{bmatrix} 0 & 0 & \frac{-S'_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} \\ 0 & 0 & \frac{S'_{1F}S''_{1F}-1}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} \\ \frac{-S'_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & \frac{S'_{1F}S''_{1F}-1}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & 0 \end{bmatrix},$$

$$\left([\mathbf{F}]-[\mathbf{S}_{CC}]\right)^{-1}[\mathbf{S}_{CP}]=\begin{bmatrix} 0 & \frac{-S''^{2}_{1F}S'_{2F}+S'_{2F}S''^{2}_{2F}-S''_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} \\ \frac{-S'^{2}_{1F}S''_{2F}+S'^{2}_{2F}S''_{2F}-S'_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & 0 \\ \frac{-S'_{1F}S''_{2F}-S''_{1F}S'_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & 0 \\ 0 & \frac{-S'_{1F}S''_{2F}-S''_{1F}S'_{2F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} \\ 0 & \frac{S'_{1F}S''^{2}_{1F}-S'_{1F}S''^{2}_{2F}-S''_{1F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} \\ \frac{S'^{2}_{1F}S''_{1F}-S''_{1F}S'^{2}_{2F}-S'_{1F}}{S'_{1F}S''_{1F}+S'_{2F}S''_{2F}-1} & 0 \end{bmatrix},$$

$$[\mathbf{S}_{PC}]([\mathbf{F}]-[\mathbf{S}_{CC}])^{-1}[\mathbf{S}_{CP}]=\begin{bmatrix} S_{11}^F & S_{12}^F \\ S_{21}^F & S_{22}^F \end{bmatrix},$$

при этом

$$S_{11}^F = S_{22}^F = 0, \tag{6}$$

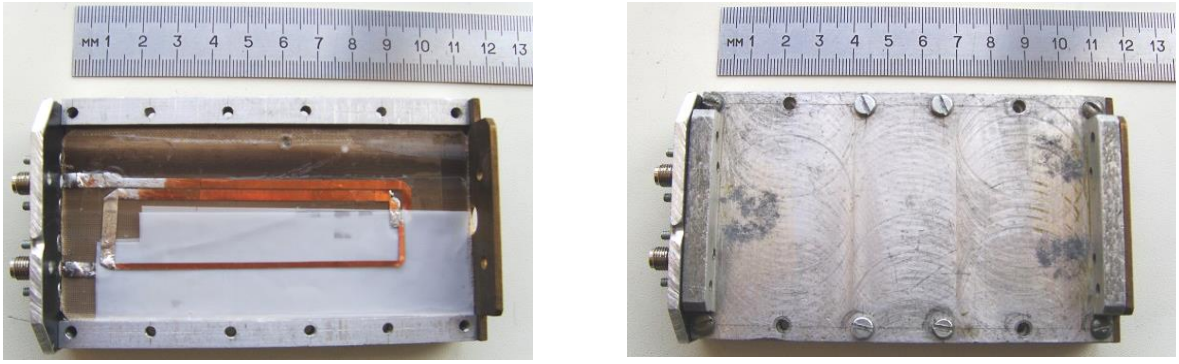
$$S_{12}^F = S_{21}^F = \frac{S'_{1F}{}^2 S''_{1F}{}^2 - S'_{1F} S''_{1F} - S'_{1F}{}^2 S''_{2F}{}^2 - S''_{1F}{}^2 S'_{2F}{}^2 - S'_{2F} S''_{2F} + S'_{2F}{}^2 S''_{2F}{}^2}{S'_{1F} S''_{1F} + S'_{2F} S''_{2F} - 1}. \tag{7}$$

Поскольку согласно (6) коэффициенты отражения ДФВ S_{11}^F и S_{22}^F равны нулю, то модули элементов S_{12}^F, S_{21}^F [коэффициентов передачи по напряжению (7)] должны быть равны единице ($\left|S_{12}^F\right| = \left|S_{21}^F\right| = 1$) при любых величинах коэффициентов связи линий *1*, *2* и *3*, *4*. Однако необходимо так подобрать эти коэффициенты связи, чтобы нелинейная фазочастотная характеристика ДФВ, проходя на соответствующем графике выше линейной фазочастотной характеристики регулярной согласованной линии передачи, обеспечивала бы дифференциальный/разностный сдвиг фаз, необходимый для построения диаграммообразующего устройства Батлера многолучевой ФАР [1]. Для достижения данных значений была решена задача нахождения оптимальных коэффициентов связи k_{12}, k_{34} через (6) и (7) посредством программы автоматизированного проектирования «MathCAD». При помощи параметрической оптимизации в пределах поиска $0 < k_{12} < 1$, $0 < k_{34} < 1$ были найдены коэффициенты k_{12} и k_{34} для ДФВ с фазовыми сдвигами 22,5; 45; 67,5; 90° при различных отклонениях от номинальных фазовых задержек, которые сведены в табл. 1, где также указаны относительные полосы рабочих частот Δf (в процентах), которые обеспечиваются при оптимальном выборе коэффициентов связи. Значения фазовых сдвигов для ДФВ выбраны не случайно, так как при дальнейшем проектировании диаграммообразующих устройств необходимо обеспечение именно таких дифференциальных фазовых сдвигов [1, 19].

Для экспериментального подтверждения результатов синтеза была разработана топология ДФВ для дифференциального фазового сдвига 45° на центральной частоте 550 МГц со следующими коэффициентами связи в ответвителях: $k_{12} = 0{,}728$ и $k_{34} = 0{,}608$, а затем проведён электродинамический анализ. Далее был изготовлен опытный образец (рис. 2) и измерены его характеристики. При изготовлении использовались материалы ФАФ-4Д и ФФ-4 с диэлектрической проницаемостью 2,5 и 2,0 соответственно. На рис. 3 совмещены результаты моделирования (чёрные непрерывные линии) и экспериментального исследования при помощи векторного анализатора цепей «Обзор-804» (штриховые линии): коэффициенты отражения (рис. 3, *а*) и дифференциальный фазовый сдвиг (рис. 3, *б*). Экспериментальные результаты свидетельствуют о вполне приемлемых показателях ДФВ в полосе частот 330…800 МГц: 45±1,5°. Аналогичным образом можно рассчитать фазовращатели на любую задержку в достаточно широкой полосе частот порядка полутора октав.

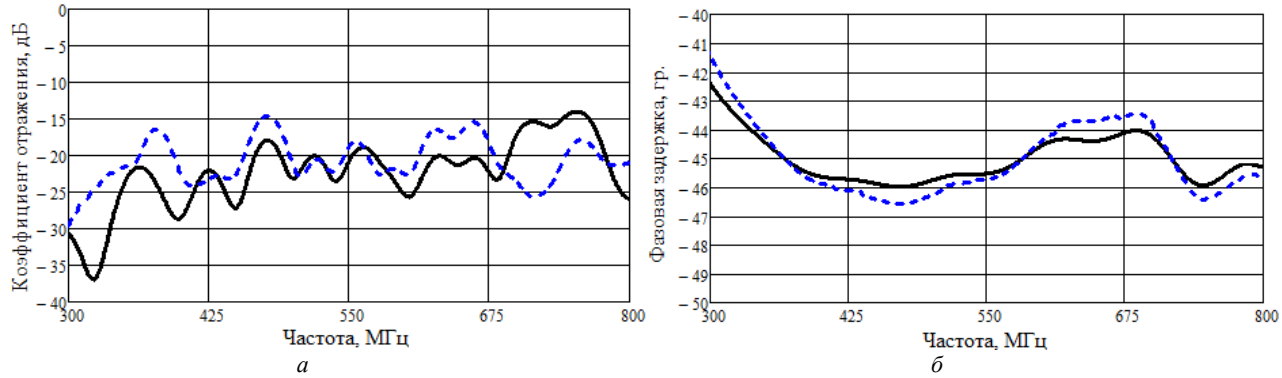
Значения коэффициентов связи для различных фазовых задержек и их отклонений от номиналов в соответствующих относительных полосах частот

Отклонения	Коэффициенты связи для фазовращателей и относительные полосы частот в процентах											
	22,5°			45°			67,5°			90°		
	k_{12}	k_{34}	Δf, %	k_{12}	k_{34}	Δf, %	k_{12}	k_{34}	Δf, %	k_{12}	k_{34}	Δf, %
±0°	0,555	0,435	–	0,691	0,571	–	0,785	0,665	–	0,865	0,665	–
±2°	0,608	0,488	59,1	0,728	0,608	42	0,801	0,681	37,5	0,873	0,673	29,5
±4°	0,652	0,532	68,2	0,757	0,637	50	0,825	0,705	45,5	0,889	0,689	36,4
±6°	0,688	0,568	77,2	0,782	0,662	56,8	0,844	0,724	47,7	0,905	0,705	40,9
±8°	0,721	0,601	84,1	0,805	0,685	61,4	0,86	0,74	51,1	0,916	0,716	43,2
±10°	0,749	0,629	88,6	0,825	0,705	65,9	0,874	0,754	54,5	0,927	0,727	45,5



а *б*

Рис. 2. Фотографии ДФВ: *а* – без крышки; *б* – собранного устройства



а *б*

Рис. 3. Параметры дифференциального фазовращателя (сплошная линия – моделирование, штриховая линия – эксперимент): *а* – коэффициент отражения; *б* – дифференциальный фазовый сдвиг

Заключение

Представленные результаты свидетельствуют о корректности методики проектирования ДФВ из отрезков электромагнитно связанных полосковых линий с кольцевым проводником, реализованных в печатном исполнении по новой конструктивно-компоновочной схеме, защищённой патентом Российской Федерации [15]. Описанные дифференциальные фазовращатели найдут применение при проектировании диаграммообразующих устройств полностью печатных (т.е. без каких-либо соединительных коаксиальных кабелей) многолучевых ФАР, конструктивно-компоновочная структура которых также защищена патентом Российской Федерации [19].

Публикация выполнена при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта № FEWM-2020-039 от 01.03.20.

Литература

1. Hansen R.C. Phased Array Antennas. – 2nd Edition. – New Jersey, Hoboken: John Wiley & Sons Inc., 2009. – 548 p.

2. Monteath G.D. Coupled transmission lines as symmetrical directional couplers // Proceedings of the IEE – Part B: Radio and Electronic Engineering. – 1955. – Vol. 102, No. 3. – P. 383–392.

3. Schiffman B.M. A New Class of Broad-Band Microwave 90-Degree Phase Shifters // IRE Transactions on Microwave Theory and Techniques. – 1958. – Vol. 6, No. 2. – P. 232–237.

4. Schiffman B.M. Multisection Microwave Phase-Shift Network // IEEE Transactions on Microwave Theory and Techniques. – 1966. – Vol. 14, No. 4. – P. 209–209.

5. Shelton J.P. Synthesis and Design of Wide-Band Equal-Ripple TEM Directional Couplers and Fixed Phase Shifters / J.P. Shelton, J.A. Mosko // IEEE Transactions on Microwave Theory and Techniques. – 1966. – Vol. 14, No. 10. – P. 462–473.

6. Горбачев А.П. Каскадные дифференциальные фазовращатели диапазона СВЧ / А.П. Горбачев, А.М. Куприянов, С.Г. Неверов // Изв. вузов МВ и ССО СССР. Радиоэлектроника. – 1984. – Т. 27, № 11. – С. 14–19.

7. Quirarte J.L.R. Synthesis of Schiffman phase shifters / J.L.R. Quirarte, J.P. Starski // IEEE Transactions on Microwave Theory and Techniques. – 1991. – Vol. 39, No. 11. – P. 1885–1889.

8. A New Structure of Microwave Ultrawide-Band Differential Phase Shifter / V.P. Meschanov, I.V. Metelnikova, V.D. Tupikin, G.G. Chumaevskaya // IEEE Transactions on Microwave Theory and Techniques. – 1994. – Vol. 42, No. 5. – P. 762–765.

9. Free C.E. Improved Analysis and Design of Coupled-Line Phase Shifters / C.E. Free, C.S. Aitchison // IEEE Transactions on Microwave Theory and Techniques. – 1995. – Vol. 43, No. 9. – P. 2126–2131.

10. Guo Y.-X. Improved Wide-Band Schiffman Phase Shifter / Y.-X. Guo, Z.-Yu Zhang, L.C. Ong // IEEE Transactions on Microwave Theory and Techniques. – 2006. – Vol. 54, No. 3. – P. 1196–1200.

11. Schiek B. Method for Broad-Band Matching of Microstrip Differential Phase Shifters / B. Schiek, J.A. Kohler // IEEE Transactions on Microwave Theory and Techniques. – 1977. – Vol. 25, No. 8. – P. 666–671.

12. Quirarte J.L.R. Novel Schiffman Phase Shifters / J.L.R. Quirarte, J.P. Starski // IEEE Transactions on Microwave Theory and Techniques. – 1993. – Vol. 41, No. 1. – P. 9–14.

13. Generalized Coupled-Line All-Pass Phasers / S. Gupta, Q. Zhang, L. Zou, L.J. Jiang, C. Caloz // IEEE Transactions on Microwave Theory and Techniques. – 2015. – Vol. 63, No. 3. – P. 1007–1018.

14. Lyu Y.-P. Design and Analysis of Schiffman Phase Shifter Under Operation of Its Second Phase Period / Y.-P. Lyu, L. Zhu, C.-H. Cheng // IEEE Transactions on Microwave Theory and Techniques. – 2018. – Vol. 66, No. 7. – P. 3263–3269.

15. Пат. 2 729 513 РФ, МПК H 01 P 1/18. Полосковый фазовращатель / А.П. Горбачев (РФ), Ю.Н. Паршин (РФ). – № 2 019 138 333; заявл. 26.11.19; опубл. 07.08.20, Бюл. № 22. – 16 с.

16. Горбачев А.П. Широкополосные диаграммообразующие устройства на несимметричных направленных ответвителях // Радиотехника и электроника. – 1980. – Т. 25, № 7. – С. 1384–1391.

17. Горбачев А.П. Анализ нетрадиционных всепропускающих четырехполюсников СВЧ на связанных линиях / А.П. Горбачев, А.М. Куприянов, С.Г. Неверов // Радиотехника и электроника. – 1986. – Т. 31, № 11. – С. 2277–2280.

18. Машковцев Б.М. Теория волноводов / Б.М. Машковцев, К.Н. Цибизов, Б.Ф. Емелин. – Л: Наука, 1966. – 351 с.

19. Пат. 2 757 538 РФ, МПК H 01 Q 21/00. Диаграммообразующее устройство / А.П. Горбачев (РФ), Ю.Н. Паршин (РФ). – № 2 020 143 539; заявл. 29.12.20; опубл. 18.10.21, Бюл. № 29. – 32 с.

Горбачев Анатолий Петрович
Д-р техн. наук, профессор каф. радиоприемных и радиопередающих устройств Новосибирского государственного технического университета (НГТУ)
Карла Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0002-2508-7566
Тел.: +7-913-761-91-08
Эл. почта: apgor@ngs.ru

Паршин Юрий Николаевич
Мл. науч. сотр. НИИ систем электросвязи
Томского государственного университета
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0002-8598-4154
Тел.: +7-965-829-12-41
Эл. почта: jurparnik@mail.ru

Gorbachev A.P., Parshin Yu.N.

Synthesis of broadband differential phase shifters on electromagnetically coupled lines for multibeam antenna arrays

The work is devoted to the synthesis of differential phase shifters on electromagnetically coupled lines with a closed ring conductor. In comparison with the known phase shifters, the proposed structure is characterized by additional degrees of freedom in printed strip design and provides the possibility of designing multipath equidistant phased antenna arrays with operating frequency bands up to one and a half octaves, provided that the emitters of their antenna canvases are characterized by the same broadband, for example, printed logoperiodic emitters. With narrow-band emitters, the possibility of implementing a dual-frequency or multi-frequency mode of operation of a multipath antenna array opens up.

Keywords: differential phase shifter, coupled strip lines, directional coupler, antenna arrays.
DOI: 10.21293/1818-0442-2022-25-4-13-18

References

1. Hansen R.C. *Phased Array Antennas*. 2nd Edition. New Jersey, Hoboken, John Wiley & Sons Inc., 2009. 548 p.

2. Monteath G.D. Coupled transmission lines as symmetrical directional couplers. *Proceedings of the IEE, Part B: Radio and Electronic Engineering*, 1955, vol. 102, no. 3, pp. 383–392.

3. Schiffman B.M. A New Class of Broad-Band Microwave 90-Degree Phase Shifters. *IRE Transactions on Microwave Theory and Techniques*, 1958, vol. 6, no. 2, pp. 232–237.

4. Schiffman B.M. Multisection Microwave Phase-Shift Network. *IEEE Transactions on Microwave Theory and Techniques*, 1966, vol. 14, no. 4, pp. 209–209.

5. Shelton J.P., Mosko J.A. Synthesis and Design of Wide-Band Equal-Ripple TEM Directional Couplers and Fixed Phase Shifters. *IEEE Transactions on Microwave Theory and Techniques*, 1966, vol. 14, no. 10, pp. 462–473.

6. Gorbachev A.P., Kupriyanov A.M., Neverov S.G. [Cascade differential phase shifters of the microwave range]. *Izvestia vuzov Ministerstva vyschego obrazovania USSR*, 1984, vol. 27, no. 11, pp. 14–19.

7. Quirarte J.L.R. Starski J.P. Synthesis of Schiffman phase shifters. *IEEE Transactions on Microwave Theory and Techniques*, 1991, vol. 39, no. 11, pp. 1885–1889.

8. Meschanov V.P., Metelnikova I.V., Tupikin V.D., Chumaevskaya G.G. A New Structure of Microwave Ultrawide-Band Differential Phase Shifter. *IEEE Transactions on Microwave Theory and Techniques*, 1994, vol. 42, no. 5, pp. 762–765.

9. Free C.E., Aitchison C.S. Improved Analysis and Design of Coupled-Line Phase Shifters. *IEEE Transactions on Microwave Theory and Techniques*, 1995, vol. 43, no. 9, pp. 2126–2131.

10. Guo Y.-X., Zhang Z.-Yu., Ong L.C. Improved Wide-Band Schiffman Phase Shifter. *IEEE Transactions on Microwave Theory and Techniques*, 2006, vol. 54, no. 3, pp. 1196–1200.

11. Schiek B., Kohler J. A Method for Broad-Band Matching of Microstrip Differential Phase Shifters. *IEEE Transactions on Microwave Theory and Techniques*, 1977, vol. 25, no. 8, pp. 666–671.

12. Quirarte J.L.R., Starski J.P. Novel Schiffman Phase Shifters. *IEEE Transactions on Microwave Theory and Techniques*, 1993, vol. 41, no. 1, pp. 9–14.

13. Gupta S., Zhang Q., Zou L., Jiang L.J., Caloz C. Generalized Coupled-Line All-Pass Phasers. *IEEE Transactions on Microwave Theory and Techniques*, 2015, vol. 63, no. 3, pp. 1007–1018.

14. Lyu Y.-P., Zhu L., Cheng C.-H. Design and Analysis of Schiffman Phase Shifter Under Operation of Its Second Phase Period. *IEEE Transactions on Microwave Theory and Techniques*, 2018, vol. 66, no. 7, pp. 3263–3269.

15. Gorbachev A.P., Parshin Yu.N. Poloskovyy fazovrashchatel' [Strip phase shifter]. Patent RF, no. 2729513, 2020.

16. Gorbachev A.P. Broadband diagram-forming devices on asymmetric directional couplers. *Radiotechnica i Electronica*, 1980, vol. 25, no. 7, pp. 1384-1391.

17. Gorbachev A.P., Kupriyanov A.M., Neverov S.G. Analysis of unconventional all-pass quadrupole microwave on coupled lines *Radiotechnica i Electronica*, 1986, vol. 31, no. 11, pp. 2277–2280.

18. Mashkovtsev B.M., Tsibizov K.N., Emelin B.F. *Theory of Waveguides*. L.: Nauka, 1966, 351 c.

19. Gorbachev A.P., Parshin Yu.N. Diagrammoobrazuyushcheye ustroystvo [Diagram-forming device]. Patent RF, no. 2757538, 2021.

Anatoly P. Gorbachev
Doctor of Science in Engineering, Professor,
Department of Radio Receiving and Transmitting Devices,
Novosibirsk State Technical University (NSTU)
20, Karl Marks pr., Novosibirsk, Russia, 630073
ORCID: 0000-0002-2508-7566
Phone: +7-913-761-91-08
Email: apgor@ngs.ru

Yury N. Parshin
Junior Research Fellow, Research Institute of Electrical Communications, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0002-8598-4154
Phone: +7-965-829-12-41
Email: jurparnik@mail.ru

УДК 621.372

А.Г. Лощилов, Т.Т. Чинь, Н.Д. Малютин, Г.А. Малютин

Расчетно-экспериментальный метод измерения частотной зависимости фазовых скоростей синфазных и противофазных волн в связанных линиях с неуравновешенной электромагнитной связью

Описан расчетно-экспериментальный метод измерения частотной зависимости фазовых скоростей синфазных и противофазных волн в связанных полосковых линиях передачи. Метод основан на экспериментальном определении резонансных частот секции, в которой первая полоска является токонесущей, включается между входом и выходом, а вторая полоска, связанная с токонесущей полоской, находится под плавающим потенциалом. При неоднородном диэлектрическом заполнении в секции наблюдаются периодически повторяющиеся резонансы. Параллельно с экспериментальными измерениями производится расчет частотных характеристик по приближенно определенным первичным параметрам. На каждой из резонансных частот значение расчетной резонансной частоты сводится к значению экспериментально определенной частоты путем вариации первичных параметров. Затем по найденным первичным параметрам определяются частотные зависимости фазовых скоростей синфазных и противофазных волн в комплексной форме. Метод был успешно применен для связанных полосковых линий в диапазоне частот до 8 ГГц.

Ключевые слова: связанные полосковые линии, полоска под плавающим потенциалом, резонансные частоты, вариация первичных параметров, эффективные диэлектрические проницаемости, фазовые скорости синфазных и противофазных волн.

DOI: 10.21293/1818-0442-2022-25-4-19-27

Полосковые линии находят широкое применение в современной радиоэлектронной аппаратуре радиолокации, связи, измерений, т.к. позволяют уменьшить массу и габариты узлов и улучшить их технологичность. Связанные полосковые линии (СПЛ) позволяют проектировать широкий спектр устройств СВЧ, поэтому их исследование актуально и в настоящее время [1–8]. Знание первичных и вторичных параметров связанных линий передачи необходимо для более точного моделирования устройств защиты от коротких импульсов (модальных фильтров) [9, 10], интегральных схем [11], высокоскоростных цифровых систем [12], а также для измерения диэлектрической проницаемости диэлектриков [13].

Одна из важных задач при характеризации связанных линий передачи заключается в определении расчетным и экспериментальным путем частотной зависимости фазовых скоростей синфазной v_c и противофазной v_π квази-Т-волн.

В [14] описан метод измерения, посредством которого можно точно определять параметры связанных микрополосковых линий путем раздельного возбуждения одного или другого режима возбуждения. Параметры, определенные на основе этих измерений, коррелируют с данными о характеристиках направленных ответвителей. Однако в них используется относительно сложная схема, требующая четырех подключений к микрополосковому образцу. Кроме этого, не учитывается изменение скорости распространения мод с частотой.

Известен способ измерения фазовых скоростей синфазных и противофазных волн в связанных полосковых линиях (СПЛ) путем измерения резонансных частот связанных отрезков [15]. Для определения частотной зависимости фазовых скоростей синфазных и противофазных волн необходимо измерять образцы разной длины, так как определяется «фундаментальный» полуволновый резонанс. Применение разных образцов вносит дополнительные погрешности в измерения. Недостатком данного способа является также необходимость определять резонансные частоты в двух разных режимах возбуждения, что связано с переключением коаксиально-полосковых переходов и соединительных коаксиальных кабелей.

Способ, основанный на измерении резонансных частот кольцевого резонатора из двух связанных линий, описан в статьях [16, 17]. Недостаток данного способа заключается в том, что в кольце связанные линии имеют разную физическую длину и, следовательно, разную электрическую длину. В результате могут наблюдаться два близко расположенных резонанса, что свидетельствует о невозможности обеспечения «чистых» режимов возбуждения синфазных и противофазных волн. Как следствие, приходится вводить поправочные коэффициенты при определении электрических длин, а в конечном итоге – фазовых скоростей синфазной и противофазной волн. Эти поправочные коэффициенты пропорциональны отношению близких резонансных частот.

Способ измерения в результате расчета и экспериментального измерения коэффициента отражения от образца, содержащего соединительные линии и С-секцию на основе связанных линий, описан в [18]. Недостатки данного способа связаны с особенностями частотных характеристик С-секции при неоднородном диэлектрическом заполнении в попереч-

ном сечении связанных линий. На частоте, соответствующей сдвигу фазы 90° в каждой из связанных линий, возникает резонанс вследствие интерференции волн, распространяющихся с разными фазовыми скоростями. Поэтому авторы способа ограничивают длину связанных линий так, чтобы не достигать частоты резонанса, на которой невозможно применить алгоритм расчета зависимости коэффициентов распространения от частоты. С целью получения коэффициентов распространения в более широком диапазоне частот в упомянутой выше работе применяется несколько образцов с разной длиной связанных линий, что фактически изменяет условия проведения эксперимента. Это является основным недостатком способа определения коэффициентов распространения синфазной (четной) и противофазной (нечетной) волн.

В настоящей работе представлены результаты разработки и реализации расчетно-экспериментального метода измерения частотной зависимости фазовых скоростей синфазных и противофазных волн в связанных полосковых линиях передачи. В основе метода лежит экспериментальное определение резонансных частот секции связанных полосковых линий с неоднородным диэлектрическим заполнением.

Эквивалентная схема секции и конструкция связанных линий

На рис. 1 показана эквивалентная схема секции связанных полосковых линий, моделируемая и экспериментально исследуемая в процессе реализации описываемого расчетно-экспериментального метода измерения фазовых скоростей синфазных и противофазных волн в СПЛ. Секция состоит из двух параллельных полосок I и II длиной $l = 0,048$ м и двух соединительных полосок длиной $l^* = 0,011$ м. В секции полоска I является токонесущей, она включается через соединительную полоску с входом (порт 1). Противоположный конец полоски I через другую соединительную полоску соединен с выходом секции (порт 3).

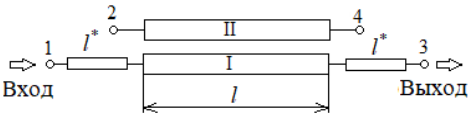


Рис. 1. Эквивалентная схема секции связанных полосковых линий

Полоска II, связанная с токонесущей полоской I, находится под плавающим потенциалом с граничными условиями холостого хода на обоих концах (порты 2 и 4).

Впервые наличие резонанса в секции представленных типов было показано в работах [19, 20]. В предложенном методе проводится определение резонансных частот в широком диапазоне частот, количество резонансов может достигать 5–10 в зависимости от конструктивного исполнения связанных линий и параметров используемых подложек. Возможность наблюдать ограниченное множество резонансов позволяет в одной позиции подключения испытуемого образца (секции связанных линий) получать необходимые данные для определения частотной зависимости фазовых скоростей волн синфазного и противофазного типов. В таких секциях возникают резонансы вследствие интерференции распространяющихся мод с разными фазовыми скоростями. Теоретические особенности интерференции синфазных и противофазных мод в подобных конструкциях связанных полосковых линий были рассмотрены в [21–25].

На рис. 2 показано поперечное сечение секции связанных полосковых линий, взятой для апробации метода. Параметры полосок структуры: ширина горизонтальных полосок $w_1 = 0,7$ мм; размер вертикальных полосок $w_2 = 2$ мм; толщина горизонтальной подложки $h_1 = 1,6$ мм; толщина вертикальной подложки $h_2 = 0,635$ мм; ширина горизонтальной подложки $a = 24$ мм; относительные диэлектрические проницаемости $\varepsilon_{r1} = 4,5$, $\varepsilon_{r2} = 6,15$; толщина проводников 0,035 мм.

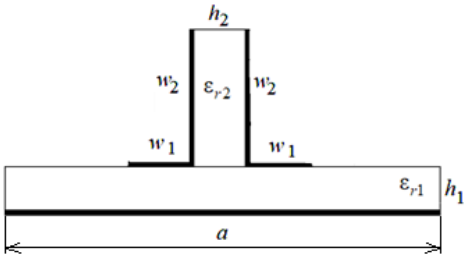


Рис. 2. Поперечное сечение связанных полосковых линий

На рис. 3 показан изготовленный макет СПЛ.

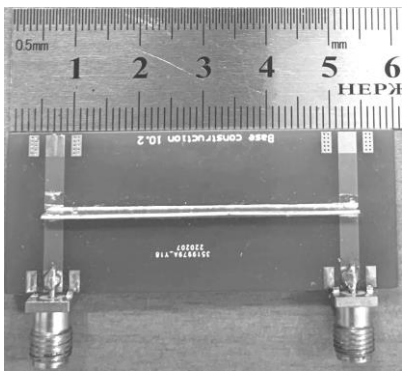


Рис. 3. Изготовленный макет СПЛ

В макете горизонтальная подложка сделана из фольгированного материала FR-4 размером 60×24 мм с диэлектрической проницаемостью $\varepsilon_{r1} = 4,5$, $\mathrm{tg}\delta_1 = 0,02$, а вертикальная – из материала RO-4360 G2 с диэлектрической проницаемостью $\varepsilon_{r1} = 6,15$, $\mathrm{tg}\delta_2 = 0,0038$.

На рис. 4 показаны экспериментальная и расчетная частотные зависимости коэффициента передачи секции в виде модуля коэффициента матрицы рассеяния $|S_{31}(f)|$. Пунктиром изображена измеренная частотная зависимость коэффициента пере-

дачи секции в виде модуля коэффициента матрицы рассеяния $|S_{31}(f)|_{\text{эксп}}$. Сплошной линией показана рассчитанная частотная зависимость $|S_{31}(f)|_{\text{расч}}$. На графиках размечены экспериментально полученные резонансные частоты $f_{i\ \text{эксп}}$ $(i=1,...,5)$ и расчетные резонансные частоты $f_{i\ \text{расч}}$ $(i=1,...,5)$.

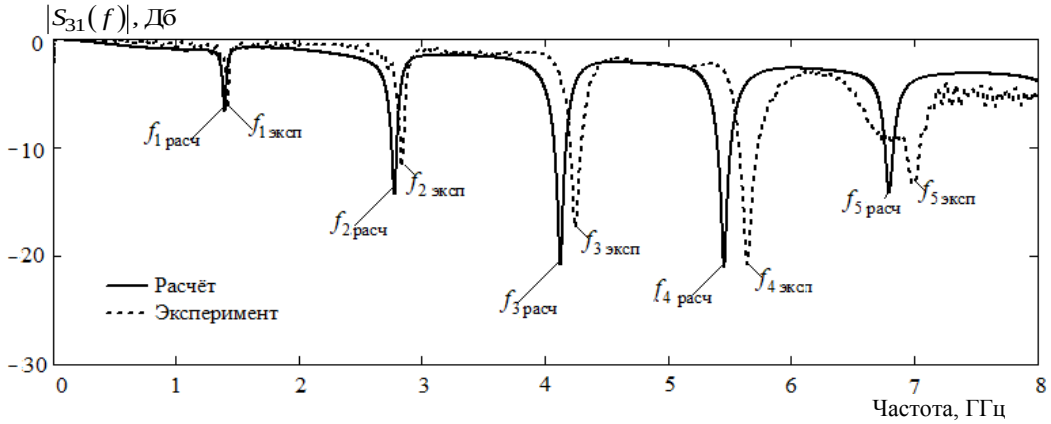


Рис. 4. Экспериментальные и расчетные частотные зависимости коэффициента передачи секции в виде модуля коэффициента матрицы рассеяния $|S_{31}(f)|$

Детализация метода.
Результат измерения фазовых скоростей

Метод измерения частотной зависимости фазовых скоростей синфазных и противофазных волн в связанных линиях с неуравновешенной электромагнитной связью состоит в следующей последовательности действий. Производят изготовление тестируемой секции связанных линий (см. рис. 1, рис. 2). На векторном анализаторе цепей измеряется коэффициент передачи в виде модуля коэффициента матрицы рассеяния $|S_{31}(f)|_{\text{эксп}}$ в широком диапазоне частот, определяются экспериментальные значения резонансных частот $f_{i\ \text{эксп}}$ из условия минимума $\min|S_{31}(f_i)|_{\text{эксп}}$. Пример измерений $|S_{31}(f)|_{\text{эксп}}$ показан на рис. 4 (пунктирная кривая). Индекс $i=1,2,...,5$ – номер резонанса, начиная с самого низкочастотного и заканчивая высокочастотным в частотном диапазоне измерений до 8 ГГц. Затем рассчитывается частотная зависимость коэффициента передачи $|S_{31}(f)|$ по приближенно определенным первичным параметрам в виде матриц коэффициентов электростатической индукции **C**, индуктивностей **L**, сопротивлений **R** и проводимостей **G** [26, 27]. На этом первом шаге расчет частотной зависимости $|S_{31}(f)|$ был проведен при следующих значениях матриц **C** и **L**:

$$\mathbf{C}=\begin{bmatrix} C_{11} & -C_{12} \\ -C_{21} & C_{22} \end{bmatrix}=\begin{bmatrix} 316,7 & -273,6 \\ -273,6 & 316,7 \end{bmatrix}\cdot 10^{-12},\ \text{Ф/м},$$

$$\mathbf{L}=\begin{bmatrix} L_{11} & L_{12} \\ L_{12} & L_{11} \end{bmatrix}.\begin{bmatrix} 0,4093 & 0,3096 \\ 0,3096 & 0,4093 \end{bmatrix}\cdot 10^{-6},\ \text{Гн/м}.$$

При этом на первом и последующих шагах учитывались потери в связанных линиях. Частотная зависимость матрицы **L** определялась так же, как в [28, 29]:

$$\mathbf{L}=\mathbf{L}+\frac{\mathbf{R}}{2\pi f},\ \text{Гн/м},$$

$$\mathbf{R}=\begin{bmatrix} \left(w_1\cdot\delta\cdot 10^{-3}\right)^{-1} & 0 \\ 0 & \left(w_1\cdot\delta\cdot 10^{-3}\right)^{-1} \end{bmatrix},\ \text{Ом/м}.$$

Матрица **G** рассчитывалась из условия того, что G_{12} зависит от потерь в диэлектрике вертикальной подложки, что обусловлено картиной электрического поля [24, 27]:

$$\mathbf{G}=\begin{bmatrix} \text{tg}\delta_1\cdot(C_{11}-C_{12})\cdot f & \text{tg}\delta_2\cdot C_{12}\cdot f \\ \text{tg}\delta_2\cdot C_{12}\cdot f & \text{tg}\delta_1\cdot(C_{11}-C_{12})\cdot f \end{bmatrix}\cdot 2\pi,\ \text{См/м},$$

где $\delta=\dfrac{2,074}{\sqrt{f\cdot 10^{-9}}}$, мкм – толщина скин-слоя [29], $\text{tg}\delta_1=0,02$ – для подложки FR-4, $\text{tg}\delta_2=0,0038$ – для подложки RO4360G2.

На следующих шагах решалась задача уточнения погонных параметров и приближения расчетных значений резонансных частот $f_{i\ \text{расч}}$ к $f_{i\ \text{эксп}}$ путем вариации элементов **C** и **L**.

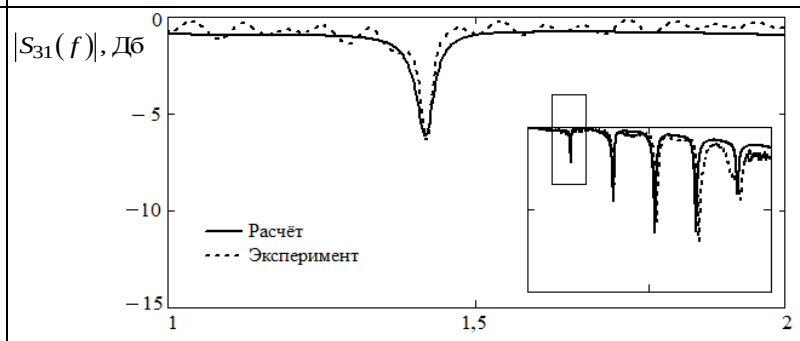
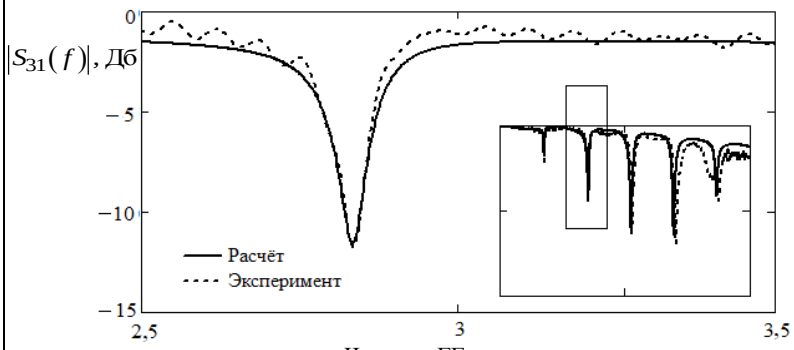
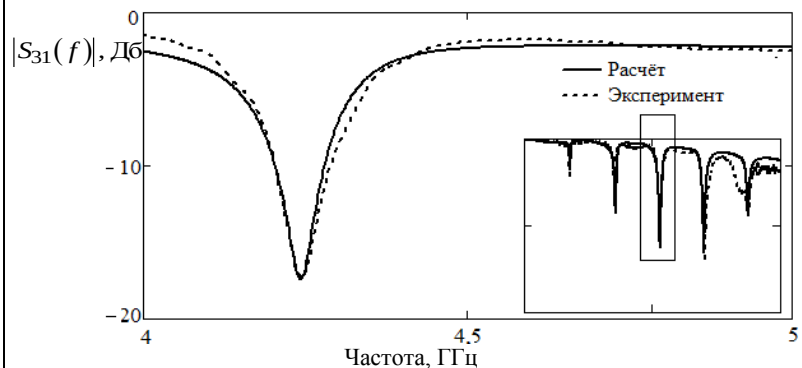
Расчетные значения резонансных частот $f_{i\ \text{расч}}$ определяются исходя из условия $\min|S_{31}(f_i)|_{\text{расч}}$. Далее производится сравнение экспериментальных частот резонанса $f_{i\ \text{эксп}}$ и вычисленных $f_{i\ \text{расч}}$, выполняется вариация первичных параметров в виде матриц коэффициентов электростатической индукции **C** и матриц погонных индуктивностей **L**, используемых при расчете частотных характеристик секции связанных линий с целью изменения $f_{i\ \text{расч}}$ до совпадения $f_{i\ \text{расч}}$ с $f_{i\ \text{эксп}}$ по критерию

$$\min\left(\left|f_{i\ \text{эксп}}-f_{i\ \text{расч}}\right|\cdot f_{ri\ \text{эксп}}^{-1}\right)\le\delta,\qquad(1)$$

где δ – погрешность несовпадения резонансных частот, полученных в результате вариации матриц **C** и **L**. Варьирование элементов матриц проводи-

лось случайным образом. При этом определялось условие (1) не только по совпадению частот $f_{i\ \text{эксп}}$ и $f_{i\ \text{расч}}$, но и по глубине резонанса. На каждой из частот $f_{i\ \text{эксп}}$ получены значения матрицы $\mathbf{C}_{i\ \text{корр}}$ и $\mathbf{L}_{i\ \text{корр}}$. На рис. 5 в таблице показаны результаты вариации матриц $\mathbf{C}_{1\ \text{корр}}$ и $\mathbf{L}_{1\ \text{корр}}$ до выполнения условия (1) на первой резонансной частоте. При указанных $\mathbf{C}_{1\ \text{корр}}$ и $\mathbf{L}_{1\ \text{корр}}$ получено $\delta = 0{,}12\%$. В выделенном квадрате на рис. 5 показаны частотные зависимости $|S_{31}(f)|_{\text{эксп}}$ и $|S_{31}(f)|_{\text{расч}}$ во всем частотном диапазоне для проверки условия устойчивости $\max\left(\left|f_{i\ \text{эксп}} - f_{i\ \text{расч}}\right|\right) \le \Delta$, где Δ – наибольшее отклонение расчетных значений от экспериментальных, фиксируемое на первом шаге. Графически это иллюстрируется отсутствием расхождения $f_{i+1\ \text{расч}}$ с $f_{i+1\ \text{эксп}}$ в результате изменения $C_{i\ \text{корр}}$, $L_{i\ \text{корр}}$ на предыдущем шаге i реализации процедуры случайного поиска. Вычисления делались нами при переходе от частоты $f_{1\ \text{эксп}}$ к каждой следующей частоте с проверкой условия (1) и условия устойчивости решения $\max\left(\left|f_{i\ \text{эксп}} - f_{i\ \text{расч}}\right|\right) \le \Delta$. С каждым последующим шагом происходило уменьшение Δ, что можно объяснить пошаговым приближением частотной зависимости расчетных параметров связанных линий к их измеряемым значениям. Полученные результаты иллюстрируется на рис. 5–9 из таблицы.

Результаты вариации корректирующих матриц для достижения совпадения резонансов секции СПЛ

	Графики	$\mathbf{C}_{i\ \text{корр}}$, пФ/м; $\mathbf{L}_{i\ \text{корр}}$, мкГн/м
1	 Рис. 5. Результат вариации для первого резонанса	$\mathbf{C}_{1\ \text{корр}} = \begin{bmatrix} 317{,}9 & -274{,}4 \\ -274{,}4 & 317{,}9 \end{bmatrix}$, $\mathbf{L}_{1\ \text{корр}} = \begin{bmatrix} 0{,}401 & 0{,}305 \\ 0{,}305 & 0{,}401 \end{bmatrix}$
2	 Рис. 6. Результат вариации для второго резонанса	$\mathbf{C}_{2\ \text{корр}} = \begin{bmatrix} 312{,}4 & -274{,}6 \\ -274{,}6 & 312{,}4 \end{bmatrix}$, $\mathbf{L}_{2\ \text{корр}} = \begin{bmatrix} 0{,}3995 & 0{,}3050 \\ 0{,}3050 & 0{,}4020 \end{bmatrix}$
3	 Рис. 7. Результат вариации для третьего резонанса	$\mathbf{C}_{3\ \text{корр}} = \begin{bmatrix} 318{,}3 & -271{,}4 \\ -271{,}4 & 318{,}3 \end{bmatrix}$, $\mathbf{L}_{3\ \text{корр}} = \begin{bmatrix} 0{,}3998 & 0{,}305 \\ 0{,}305 & 0{,}3998 \end{bmatrix}$

Продолжение таблицы

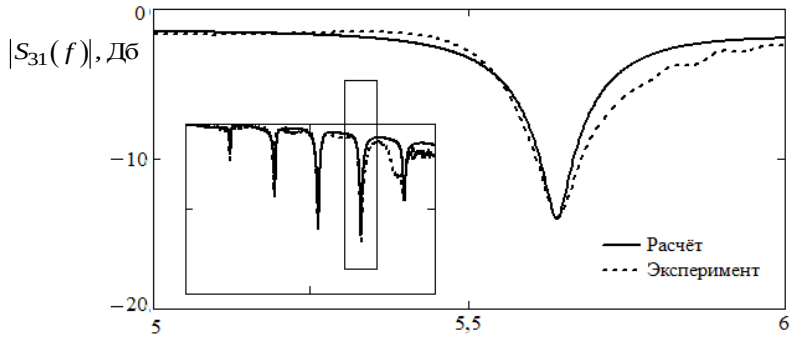
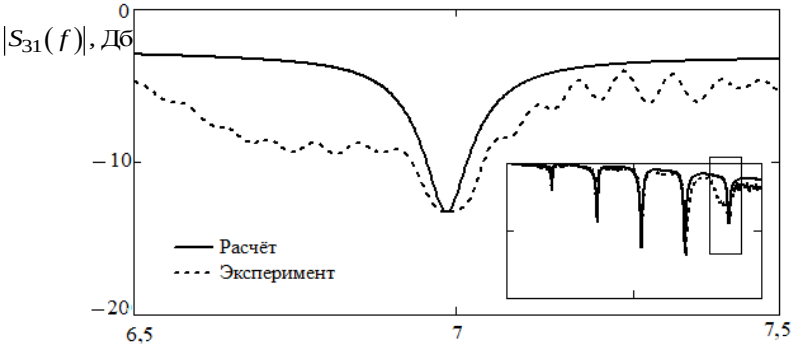
	Графики	$\mathbf{C}_{i\ \text{корр}}$, пФ/м; $\mathbf{L}_{i\ \text{корр}}$, мкГн/м
4	 Частота, ГГц	$\mathbf{C}_{4\ \text{корр}} = \begin{bmatrix} 319{,}8 & -271{,}4 \\ -271{,}4 & 319{,}8 \end{bmatrix}$, $\mathbf{L}_{4\ \text{корр}} = \begin{bmatrix} 0{,}3992 & 0{,}3050 \\ 0{,}3050 & 0{,}3992 \end{bmatrix}$
5	 Частота, ГГц	$\mathbf{C}_{5\ \text{корр}} = \begin{bmatrix} 317{,}3 & -276{,}0 \\ -276{,}0 & 317{,}3 \end{bmatrix}$, $\mathbf{L}_{5\ \text{корр}} = \begin{bmatrix} 0{,}3988 & 0{,}3050 \\ 0{,}3050 & 0{,}3988 \end{bmatrix}$

Рис. 8. Результат вариации для четвертого резонанса

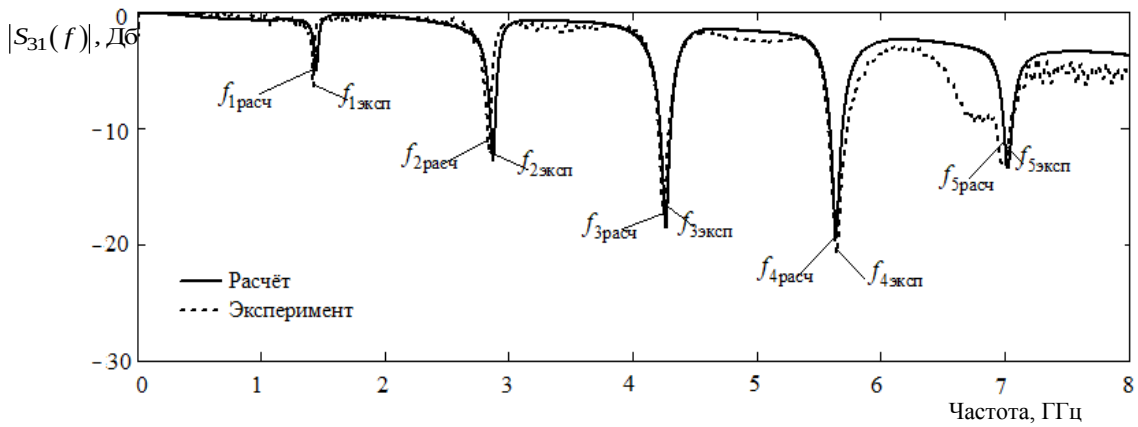
Рис. 9. Результат вариации для пятого резонанса

В результате получается множество откорректированных значений $\mathbf{C}_{i\ \text{корр}}$ и $\mathbf{L}_{i\ \text{корр}}$ и на каждой из частот $f_{i\ \text{эксп}}$ удовлетворяется условие $\min\left(\left|f_{i\ \text{эксп}} - f_{i\ \text{расч}}\right| \cdot f_{ri\ \text{эксп}}^{-1}\right) \le \delta$, а частотные зависимости $\left|S_{31}(f)\right|_{\text{расч}}$ и $\left|S_{31}(f)\right|_{\text{эксп}}$ удовлетворяют условию устойчивости $\max\left(\left|f_{i\ \text{эксп}} - f_{i\ \text{расч}}\right|\right) \le \Delta$ при любых из $\mathbf{C}_{i\ \text{корр}}$ и $\mathbf{L}_{i\ \text{корр}}$ (рис. 10). Далее рассчитываются эффективные диэлектрические проницаемости синфазных и противофазных волн [30] с учетом особенностей, изложенных в [31].

$\varepsilon_{i\ \text{эфф}\,c} = c^2 \cdot \left(L_{i11\text{корр}} + L_{i12\text{корр}}\right)\left(C_{i11\text{корр}} - C_{i12\text{корр}}\right)$,

$\varepsilon_{i\ \text{эфф}\,\pi} = c^2 \cdot \left(L_{i11\text{корр}} - L_{i12\text{корр}}\right)\left(C_{i11\text{корр}} + C_{i12\text{корр}}\right)$,

где $L_{i11\text{корр}}$, $L_{i12\text{корр}}$ – коэффициенты i-й корректированной матрицы индуктивностей $\mathbf{L}_{i\ \text{корр}}$; $C_{i11\text{корр}}$, $C_{i12\text{корр}}$ – коэффициенты корректированных матриц коэффициентов электростатической индукции $\mathbf{C}_{i\ \text{корр}}$; c – скорость света.



Частота, ГГц

Рис. 10. Экспериментальная и расчетная частотные зависимости коэффициента передачи секции в виде модуля коэффициента матрицы рассеяния $\left|S_{31}(f)\right|$

Затем рассчитываются фазовые скорости синфазных и противофазных волн на каждой из частот $f_{i\ \text{эксп}}$.

$$v_{ic} = \frac{c}{\sqrt{\varepsilon_{i\ \text{эфф}\,c}}}, \quad v_{i\pi} = \frac{c}{\sqrt{\varepsilon_{i\ \text{эфф}\,\pi}}}.$$

На рис. 11 показан результат определения частотной зависимости фазовых скоростей синфазной v_{ic} и противофазной $v_{i\pi}$ волн, отношения фазовых скоростей $v_{ic}/v_{i\pi}$ в связанных линиях с неуравновешенной электромагнитной связью.

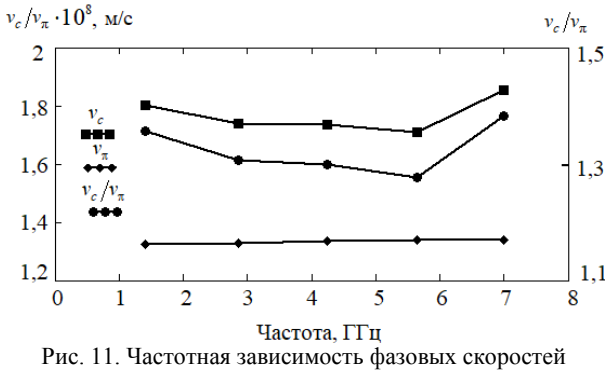


Рис. 11. Частотная зависимость фазовых скоростей синфазной v_{ic} и противофазной $v_{i\pi}$ волн и отношения фазовых скоростей $v_{ic}/v_{i\pi}$

Заключение

Итак, предложен и реализован относительно простой метод для измерения фазовых скоростей синфазных и противофазных волн в связанных линиях с неуравновешенной электромагнитной связью, основанный на экспериментальном определении резонансных частот секции связанных полосковых линий. Приведенный пример реализации метода показывает целесообразность такого пути получения недостающих данных для успешного проектирования устройств. Это справедливо, с одной стороны, по причине резкого сокращения времени для получения необходимой информации при наличии разработанных методик и измерительной аппаратуры; с другой стороны, получение экспериментальных данных так или иначе представляет более надежный способ проверки достижения заданных условий технического задания. Установлено частотное ограничение метода до 6 ГГц, это связано с качеством использованных коаксиально-полосковых переходов, их замена позволит увеличить верхнюю частоту.

Публикация выполнена при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта № FEWM-2023-0014 от 16.01.2023.

Литература

1. Особенности характеристик полосно-пропускающих фильтров второго порядка на полуволновых и четвертьволновых микрополосковых резонаторах / Б.А. Беляев, Я.Ф. Бальва, А.А. Лексиков, А.М. Сержантов, С.А. Ходенков, Т.Ю. Шумилов // Изв. вузов. Физика. – 2022. – Т. 65, № 2 (771). – С. 71–81.

2. A Microwave Bandpass Filter on Dielectric Layers with Metal Grids / B.A. Belyaev, V.V. Tyurnev, A.S. Voloshin, R.G. Galeev // Technical Physics Letters. – 2018. – P. 408–411.

3. Сычев А.Н. Параметры несимметричных связанных линий с неоднородным диэлектриком / А.Н. Сычев, Н.Ю. Рудый // Доклады ТУСУР. – 2018. – Т. 21, № 4–1. – С. 7–15.

4. A Novel trans-directional coupler based on vertically installed planar circuit / A.N. Sychev, S.M. Struchkov, V.N. Putilov, N.Y. Ruyi // Proc. of the 45-th Eur. Microw. Conf. – 2015. – P. 283–286.

5. Modeling of the vertically installed planar coupled lines by the numerical conformal transformation technique / A.N. Sychev, S.M. Struchkov, N.Y. Rudyi, A.S. Salnikov // IEEE MTT-S Int. Conf. on Numerical Electromagnetic and Multiphysics Modeling and Optimization (NEMO). – 2017. – P. 124–126.

6. Дроботун Н.Б. Модуль сверхширокополосного усилителя диапазона 10 МГц – 20 ГГц с диссипативной коррекцией АЧХ // Доклады ТУСУР. – 2016. – Т. 19, № 4. – С. 74–77.

7. Electrical characteristics of a modal filter with a passive conductor in the reference plane cutout / M.A. Samoylichenko, Y.S. Zhechev, V.P. Kosteletskii, T.R. Gazizov // IEEE Transactions on Electromagnetic Compatibility. – 2021. – Vol. 63, No. 2. – P. 435–442.

8. Экспериментальное подтверждение возможности защиты радиоэлектронной аппаратуры от сверхкороткого импульса за счет его разложения в С-секции с лицевой связью / А.В. Носов, Р.С. Суровцев, А.М. Заболоцкий, Т.Р. Газизов // Доклады ТУСУР. – 2016. – № 3. – С. 47–50.

9. Газизов А.Т. Измерение и моделирование временного отклика печатных модальных фильтров с лицевой связью / А.Т. Газизов, А.М. Заболоцкий, Т.Р. Газизов // Радиотехника и электроника. – 2018. – Т. 63, № 3. – С. 292–298.

10. Черникова Е.Б. Моделирование и разработка макета зеркально-симметричного модального фильтра / Е.Б. Черникова, А.О. Белоусов, А.М. Заболоцкий // Электронные средства и системы управления: матер. докл. междунар. науч.-практ. конф. – 2017. – № 1-2. – С. 5–7.

11. Analysis and modeling of GaAs-based coupled microstrip lines/ X. Lv, W. Yu, J. Wu, X. Luo, Y. Ge // Proc. IEEE Int. Conf. Microw. Technol. Comput. Electromagnet. – 2011. – P. 136–139.

12. Kim J.H. Accurate characterization of broadband multiconductor transmission lines for high-speed digital systems / J.-H. Kim, D. Oh, W. Kim // IEEE Trans. Adv. Packag. – Vol. 33, No. 4. – P. 857–867.

13. Microwave sensors for dielectric sample measurement based on coupled-line section / I. Piekarz, J. Sorocki, K. Wincza, S. Gruszczynski // IEEE Trans. Microw. Theory Techn. – 2017. – Vol. 65, No. 5. – P. 1615–1631.

14. Napoli L.S. Characteristics of coupled microstrip lines / L.S. Napoli, J.J. Hughes // RCA Rew. – 1970. – Vol. 31. – P. 479–498.

15. Richings J.G. Measured odd- and even-mode dispersion of coupled microstrip lines / J. G. Richings, B. Easter // IEEE Trans. Microw. Theory Techn. – 1975. – Vol. MTT-23, No. 10. – P. 826–828.

16. Gould J.W. Even and odd mode guide wavelengths of coupled lines in microstrip / J.W. Gould, E.C. Tolboys // Ezectron. Letts. – 1972. – Vol. 8, No. 5. – P. 121–122.

17. Wolff I. Microstrip ring resonator and dispersion measurement on microstrip lines / I. Wolff, N. Kpi // Electron. Lat. – 1971. – Vol. 7. – P. 779.

18. Broadband Determination of the Even- and Odd-Mode Propagation Constants of Coupled Lines Based on Two-

Port Measurements / A. Hernández-Escobar, E. Abdo-Sánchez, J. Esteban, T.M. Martín-Guerrero, C. Camacho-Peñalosa // IEEE Trans. Microw. Theory Techn. – 2020. – Vol. 68, Iss. 2. – P. 648–654.

19. Zysman G.I. Coupled Transmission Line Networks in an Inhomogeneous Dielectric Medium / G.I. Zysman, A.K. Johnson // IEEE Transactions on Microwave Theory and Techniques. – 1969. – Vol. 17, No. 10. – P. 753–759.

20. Vorobev P.A. Analysis of the Characteristics of Coupled Strip Lines Using a nonuniform Dielectric with Concentrated Controlled Discontinuities / P.A Vorob'ev, N.D Malyutin // Izvestiya Vysshikh Uchebnykh Zavedenij. Radioelektronika. – 1975. – Vol. 18, Iss. 2. – P. 97–99.

21. Special aspects in interference of in-phase and antiphase waves with unequal phase velocities in coupled lines under pulse impact / A.N. Sychev, N.D. Malyutin, E.I. Trenkal, G.A. Malyutin // Journal of Physics. – 2020. – P. 22023.

22. A Miniaturize. High Efficient Quadband Rectenna Design for RF Energy Harvesting / S. Ullah, C. Ruan, T.Ul. Haq, A.K. Fahad // Proceedings of the 2018 IEEE 7th Asia-Pacific Conference on Antennas and Propagation. – 2018. – No. 8538151. – P. 202–203.

23. Design of a compact wideband butler matrix using vertically installed planar structure / Q.P. Chen, Z. Qamar, S.Y. Zheng, Y. Long // IEEE Transactions on Components, Packaging and Manufacturing Technology. – 2018. – No. 8408811. – P. 1420–1430.

24. Modeling of the vertically installed planar coupled lines by the numerical conformal transformation technique / A.N. Sychev, S.M. Struchkov, N.Y. Rudyi, A.S. Salnikov // IEEE MTT-S International Conference on Numerical Electromagnetic and Multiphysics Modeling and Optimization for RF, Microwave, and Terahertz Applications. – 2017. – No. 7964202. – P. 106–108.

25. A Wideband Tunable Reflection-Type Phase Shifter with Wide Relative Phase Shift / W.J. Liu, S.Y. Zheng, Y.M. Pan, Y.X. Li, Y.L. Long // IEEE Transactions on Circuits and Systems II: Express Briefs. – 2017. – No. 7812672. – P. 1442–1446.

26. Fusco V. Microwave circuits. Analysis and computer-aided design // Radio and Communications. – 1990. – 286 p.

27. Малютин Г.А. Оптимизация алгоритма расчета полосковых структур методом сеток // Электронные средства и системы управления: матер. докл. Междунар. науч.-практ. конф. – 2021. – № 1–1. – С. 100–103.

28. Djordjevic A.R. Wideband Frequency-Domain Characterization of FR-4 and Time-Domain Causality / A.R. Djordjevic, M.B. Radivoje, D.L. Vladana, T.K. Sarkar // IEEE Trans. on Electromagn. Compatible. – 2001. – Vol. 43, No. 4. – P. 662–667.

29. Анпилогов В.Р. Диссипативные потери в микрополосковых линиях и микрополосковых антеннах / В.Р. Анпилогов, И.В. Зимин, Ю.Н. Чекушкин // Ракетно-космическое приборостроение и информационные системы. – 2018. – Т. 5, № 3. – С. 60–69.

30. Сычев А.Н. Системы параметров одинаковых связанных линий с неуравновешенной электромагнитной связью / А.Н. Сычев, С.М. Стручков // Доклады ТУСУР. – 2014. – № 1(31). – С. 39–50.

31. Чинь Т.Т. К определению матричных параметров связанных линий с неуравновешенной электромагнитной связью // Сборник избр. статей научной сессии ТУСУР. – 2021. – № 1-1. – С. 175–179.

Лощилов Антон Геннадьевич
Канд. техн. наук, доцент, зав. каф. конструирования узлов и деталей радиоэлектронной аппаратуры (КУДР) Томского университета систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0003-0669-5694
Тел.: +7 (382-2) 51-43-02
Эл. почта: lag@main.tusur.ru

Чинь То Тхань
Аспирант каф. КУДР ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-923-445-04-86
Эл. почта: thanhvodoi1995@gmail.com

Малютин Николай Дмитриевич
Д-р техн. наук, профессор каф. КУДР ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0003-0317-9096
Тел.: +7-391-312-34-56
Эл. почта: ndm@main.tusur.ru

Малютин Георгий Александрович
Студент каф. КУДР ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-953-911-86-10
Эл. почта: mr.mageorge@yandex.ru

Loschilov A.G., Trinh T.T., Malyutin N.D., Malyutin G.A.
Computational and experimental method for measuring the frequency dependence of phase velocities of in-phase and antiphase waves in coupled lines with unbalanced electromagnetic coupling

A computational and experimental method for measuring the frequency dependence of the phase velocities of in-phase and antiphase waves in coupled strip transmission lines is described. The method is based on the experimental determination of the resonant frequencies of a section in which the first strip is current-carrying, is switched on between the input and output, and the second strip connected to the current-carrying strip is under a floating potential. With non-homogeneous dielectric filling, periodically repeated resonances are observed in the section. In parallel with experimental measurements, the frequency characteristics are calculated according to approximately defined primary parameters. At each of the resonant frequencies, the value of the calculated resonant frequency is reduced to the value of an experimentally determined frequency by varying the primary parameters. Then, according to the found primary parameters, the frequency dependences of the phase velocities of in-phase and in-phase waves in a complex form are determined. The method has been successfully applied to connected strip lines in the frequency range up to 8 GHz
Keywords: coupled strip lines, horizontal and vertical position of the strips, phase velocities difference of synphase and antiphase waves, finding the permittivities of the substrates.
DOI: 10.21293/1818-0442-2022-25-4-19-27

References

1. Belyaev B.A., Balva Y.F., Leksikov A.A., Sergeants A.M., Khodenkov S.A., Shumilov T.Yu. [Characteristics of second-order band-pass filters on half-wave and quarter-wave

microstrip resonators] *Izvestiya Vuzov. Physics, 2022*, vol. 65, no. 2 (771), pp. 71–81 (in Russ.).

2. Belyaev B.A., Tyurnev V.V., Voloshin A.S., Galeev R.G. A Microwave Bandpass Filter on Dielectric Layers with Metal Grids. *Technical Physics Letters*, 2018, pp. 408–411.

3. Sychev A.N., Rudy N.Yu. [Parameters of asymmetric coupled lines with an inhomogeneous dielectric]. *Proceeding of TUSUR University*, 2018, vol. 21, no. 4–1, pp. 7–15 (in Russ.).

4. Sychev A.N., Struchkov S.M., Putilov V.N., Ruy N.Y. A Novel trans-directional coupler based on vertically installed planar circuit. *Proceedings of the 45-th European Microwave Conference*, 2015, pp. 283–286.

5. Sychev A.N., Struchkov S.M., Rudyi N.Y., Salnikov A.S. Modeling of the vertically installed planar coupled lines by the numerical conformal transformation technique. *IEEE MTT-S International Conference on Numerical Electromagnetic and Multiphysics Modeling and Optimization (NEMO)*, 2017, pp. 124–126.

6. Drobotun N.B. [Module of a 10 MHz – 20 GHz ultrawideband amplifier with dissipative frequency response correction]. *Proceeding of TUSUR University*, 2016, vol. 19, no. 4, pp. 74–77 (in Russ.).

7. Samoylichenko M.A., Zhechev Y.S., Kosteletskii V.P., Gazizov T.R. Electrical characteristics of a modal filter with a passive conductor in the reference plane cutout. *IEEE Transactions on Electromagnetic Compatibility*, 2021, vol. 63, no. 2, pp. 435–442.

8. Nosov A.V, Surovtsev R.S., Zabolotsky A.M., Gazizov T.P. [Experimental confirmation of the possibility of protecting radio-electronic equipment from an ultrashort pulse due to its decomposition in a C-section with a facial connection]. *Proceeding of TUSUR University*, 2016, no. 3, pp. 47–50 (in Russ.).

9. Gazizov A.T., Zabolotsky A.M., Gazizov T.R. [Measurement and modeling of the time response of printed modal filters with a face connection]. *Radio Engineering and Electronics*, 2018, vol. 63, no. 3, pp. 292–298 (in Russ.).

10. Chernikova E.B., Belousov A.O., Zabolotsky A.M. [Modeling and development of the layout of a mirror-symmetric modal filter]. *Electronic Devices and Control Systems. Materials of the International Scientific and Practical Conference*, 2017, no. 1-2, pp. 5–7 (in Russ.).

11. Lv X., Yu W., Wu J., Luo X., Ge Y. Analysis and modeling of GaAs-based coupled microstrip lines. *Proceeding IEEE International Conference Microwave Technologies and Computational Electromagnetics*, 2011, pp. 136–139.

12. Kim J.H., Oh D., Kim W. Accurate characterization of broadband multiconductor transmission lines for high-speed digital systems. *IEEE Transactions on Advanced Packaging*, Vol. 33, no. 4, pp. 857–867.

13. Piekarz I., Sorocki J., Wincza K., Gruszczynski S. Microwave sensors for dielectric sample measurement based on coupled-line section. *IEEE Transactions on Microwave Theory and Techniques*, 2017, vol. 65, no. 5, pp. 1615–1631.

14. Napoli L.S., Hughes J.J. Characteristics of coupled microstrip lines. *RCA Review*, 1970, vol. 31, pp. 479–498.

15. Richings J.G., Easter B. Measured odd- and even-mode dispersion of coupled microstrip lines. *IEEE Transactions on Microwave Theory and Techniques*, 1975, vol. MTT-23, no. 10, pp. 826–828.

16. Gould J.W., Tolboys E.C. Even and odd mode guide wavelengths of coupled lines in microstrip. *Electronics Letters*, 1972, vol. 8, no. 5, pp. 121–122.

17. Wolff I., Kpi N. Microstrip ring resonator and dispersion measurement on microstrip lines. *Electronics Letters*, 1971, vol. 7, pp. 779–781.

18. Hernández-Escobar A., Abdo-Sánchez E., Esteban J., Martín-Guerrero T.M., Camacho-Peñalosa C. Broadband Determination of the Even- and Odd-Mode Propagation Constants of Coupled Lines Based on Two-Port Measurements. *IEEE Transactions on Microwave Theory and Techniques*, 2020, vol. 68, iss. 2, pp. 648–654.

19. Zysman G.I., Johnson A.K. Coupled Transmission Line Networks in an Inhomogeneous Dielectric Medium. *IEEE Transactions on Microwave Theory and Techniques*, 1969, vol. 17, no. 10, pp. 753–759.

20. Vorob'ev P.A., Malyutin N.D. Analysis of the Characteristics of Coupled Strip Lines Using a nonuniform Dielectric with Concentrated Controlled Discontinuities. *Izvestiya Vysshikh Uchebnykh Zavedenij. Radioelektronika*, 1975, vol. 18, iss. 2, pp. 97–99.

21. Sychev A.N., Malyutin N.D., Trenkal E.I., Malyutin G.A. Special aspects in interference of in-phase and antiphase waves with unequal phase velocities in coupled lines under pulse impact. *Journal of Physics*, 2020, pp. 22023.

22. Ullah S., Ruan C., Haq T.Ul., Fahad A.K. A Miniaturize and High Efficient Quadband Rectenna Design for RF Energy Harvesting. *Proceedings of the 2018 IEEE 7th Asia-Pacific Conference on Antennas and Propagation*, 2018, no. 8538151, pp. 202–203.

23. Chen Q.P., Qamar Z., Zheng S.Y., Long Y. Design of a compact wideband butler matrix using vertically installed planar structure. *IEEE Transactions on Components, Packaging and Manufacturing Technology*, 2018, no. 8408811, pp. 1420–1430.

24. Sychev A.N., Struchkov S.M., Rudyi N.Y., Salnikov A.S. Modeling of the vertically installed planar coupled lines by the numerical conformal transformation technique. *IEEE MTT-S International Conference on Numerical Electromagnetic and Multiphysics Modeling and Optimization for RF, Microwave, and Terahertz Applications*, 2017, no. 7964202, pp. 106–108.

25. Liu W.J., Zheng S.Y., Pan Y.M., Li Y.X., Long Y.L. A Wideband Tunable Reflection-Type Phase Shifter with Wide Relative Phase Shift. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2017, no. 7812672, pp. 1442–1446.

26. Fusco V. Microwave circuits. Analysis and computer-aided design. *Radio and Communications*, 1990, 286 pp.

27. Malyutin G.A. [Optimization of the algorithm for calculating strip structures by the grid method]. *Electronic Devices and Control Systems. Materials of the International Scientific and Practical Conference*, 2021, no. 1-1, pp. 100–103 (in Russ.).

28. Radivoje M.B., Vladana D.L., Sarkar T.K., Djordjevic A.R. Wideband Frequency-Domain Characterization of FR-4 and Time-Domain Causality. *IEEE Transactions on Electromagnetic Compatibility*, 2001, vol. 43, no 4, pp. 662–667.

29. Anpilogov V.R., Zimin I.V., Chekushkin Yu.N. [Dissipative losses in microstrip lines and microstrip antennas]. *Rocket and Space Instrumentation and Information Systems*, 2018, vol. 5, no. 3, pp. 60–69 (in Russ.).

30. Sychev A.N., Struchkov S.M. [Systems of parameters of identical connected lines with unbalanced electromagnetic communication]. *Proceeding of TUSUR University*, 2014, no 1(31), pp. 39–50 (in Russ.).

31. Trinh T.T. [To the definition of matrix parameters of connected lines with unbalanced electromagnetic coupling]. *Collection of Selected Articles of TUSUR Scientific Session*, 2021, no 1–1, pp. 175–179 (in Russ.).

Anton G. Loschilov
Candidate of Science in Engineering, Associate Professor,
Department of Design of Units and Components for
Radioelectronic Systems (KUDR), Tomsk University
of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0003-0669-5694
Phone: +7 (382-2) 51-43-02
Email: lag@main.tusur.ru

Thanh T. Trinh
Postgraduate student, KUDR, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-923-445-04-86
Email: thanhvodoi1995@gmail.com

Nickolay D. Malyutin
Doctor of Science in Engineering, Professor, KUDR), TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0003-0317-9096
Phone: +7-391-312-34-56
Email: ndm@main.tusur.ru

George A. Malyutin
Student KUDR, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-953-911-86-10
Email: mr.mageorge@yandex.ru

УДК 621.396.41

А.А. Дроздова, М.Е. Комнатнов

Оценка уровня наведённого тока на испытуемый объект в ТЕМ-камере при воздействии на её вход электростатического разряда

Выполнена оценка наведённых токов и напряжений на монополь и микрополосковую линию в малогабаритной ТЕМ (transverse electromagnetic)-камере при воздействии на её вход электростатического разряда. Представлены аналитическая, квазистатическая и электродинамическая модели для расчёта форм и амплитуд токов и напряжений, наведённых на монополь и микрополосковую линию, расположенные внутри малогабаритной ТЕМ-камеры, при воздействии электростатического разряда на её вход. Представлены формы наведённых токов и напряжений на монополь и микрополосковую линию при аналитическом, квазистатическом и электродинамическом расчётах и измерениях. Максимальные отклонения результатов аналитического и электродинамического вычислений для монополя и микрополосковой линии составляют 25 и 9%. Представлен подход по использованию половины коаксиальной камеры в качестве устройства согласования между источником электростатического разряда и ТЕМ-камерой. Результаты расчётов согласуются с результатами измерений, что делает возможным применение малогабаритной ТЕМ-камеры и половины коаксиальной камеры для исследования влияния наведённых токов и напряжений, возбуждаемых электростатическим разрядом, на интегральные схемы, электронную компонентную базу и небольшие устройства в целом.

Ключевые слова: электромагнитная совместимость, восприимчивость, ТЕМ-камера, электростатический разряд.
DOI: 10.21293/1818-0442-2022-25-4-28-36

Одной из задач обеспечения электромагнитной совместимости (ЭМС) является защита радиоэлектронных средств (РЭС) от электромагнитных помех. Создаваемое электростатическим разрядом (ЭСР) электромагнитное излучение характеризуется высокой амплитудой напряжённости электрического поля с широким спектром. Восприимчивость современных РЭС к подобным видам воздействия с каждым годом возрастает [1], что требует поиска новых средств и методов защиты РЭС. Непосредственное воздействие ЭСР на электронный компонент может привести к различным изменениям в его внутренней структуре (выгорание проводника, плавление металлизации, пробой диэлектрика и пр.), которые могут вызвать различные виды обратимых и необратимых отказов [2]. Так, исходя из статистических данных [1] отказов электронных компонентов, примерно половина (47%) из них вызвана воздействием ЭСР. Другая половина связана с качеством компонентов (30%), особенностями их применения (13%), влажностью и температурой воздуха при их эксплуатации (10%).

Существуют различные устройства и методы защиты от ЭСР на уровне компонента, устройства или системы в целом. Например, известен метод расчёта паразитной ёмкости цепей входа/выхода, который может быть успешно использован при защите от ЭСР [3]. Предложен встроенный в интегральную схему (ИС) фиксатор напряжения, ослабляющий амплитуду напряжения ЭСР [4]. Кроме того, для повышения помехоустойчивости ИС предложена встроенная схема защиты от ЭСР положительной или отрицательной полярности, содержащая цепь из транзисторов и паразитных резисторов [5], а для снижения напряжения и равномерного распределения тока ЭСР предложен метод, использующий связанные ёмкости [6]. Отказы ИС при воздействии ЭСР могут возникать независимо от наличия устройств помехозащиты [7–9]. Например, экспериментально доказано, что при воздействии ЭСР на ИС происходит искажение выходного сигнала [7], а также пробой диэлектрика [8]. Путём проведения экспериментальных и теоретических исследований [9] показано, что ЭСР может приводить к сбоям в работе микроконтроллеров (МК) и ИС в целом, основной причиной которых являются наведённые импульсные сигналы на проводники печатной платы (ПП).

Известны методы для измерения помехоэмиссии [10] и восприимчивости [11] ИС. Используя ТЕМ (transverse electromagnetic)-камеру [12], возможно выполнить оценку уровня излучаемой помехоэмиссии [13] и восприимчивости [14] для ИС различного назначения. Кроме того, при помощи ТЕМ-камеры возможно определить локальные места сбоев в ИС [15].

Малогабаритная ТЕМ-камера [16, 17] с более высокой граничной частотой (5,2 ГГц) позволяет провести оценки излучаемых помехоэмиссий и восприимчивости, удовлетворяющие большинству требований, предъявляемых к современным мобильным, навигационным и связным устройствам. Кроме того, при помощи малогабаритной ТЕМ-камеры возможно оценить амплитуду и форму наведённых тока и напряжения на испытуемый объект (ИО), расположенный в её внутреннем пространстве, при воздействии на её вход импульса от имитатора ЭСР. Анализ амплитуды и формы наведённых тока и напряжения на ИО позволит сымитировать подобное воздействие и использовать его при создании новых средств и методов защиты от ЭСР. Для первоначального приближения к ИО необходимы простые геометрические объекты, в качестве которых

выбраны монополь и микрополосковая линия (МПЛ) передачи.

Цель работы – оценить амплитуды и формы токов и напряжений на монополе и МПЛ, расположенных в малогабаритной ТЕМ-камере, при воздействии ЭСР на её вход.

Аналитическая модель формы тока ЭСР

Модель, описывающая форму тока ЭСР, известна как модель человеческого тела, позволяет имитировать разряд от кончика пальца человека на ИО. Упрощённая схема имитатора ЭСР [18], реализующая модель человеческого тела, представлена на рис. 1. Схема содержит источник высоковольтного напряжения (U), зарядные ключ и резистор R_c (50–100 МОм), разрядные ключ и резистор R_d (330 Ом±10%), конденсатор C_s (150 пФ±10%) и ИО. Значение C_s имитирует ёмкость человеческого тела, а сопротивление R_d имитирует электрический контакт между человеческим телом и металлическим объектом. Номиналы элементов схемы могут отличаться, так как ёмкость (C_s) человеческого тела может варьироваться от 100 до 500 пФ, а сопротивление (R_d) – от нескольких десятков Ом до сотен килоом.

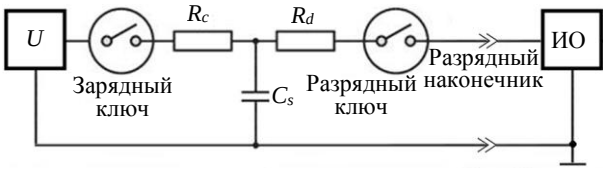


Рис. 1. Упрощённая схема имитатора ЭСР [18]

Для моделирования выбрана минимально возможная амплитуда воздействия имитатором ЭСР, составляющая 1 кВ. Расчёт значений токов первого (I_1) и второго (I_2) максимумов для ЭСР с напряжением 1 кВ выполнен, используя аналитическую запись, предложенную Хайдлером [19]:

$$I_{\text{ЭСР}}(t)=\frac{I_1 e^{-t/\tau_2}\left(t/\tau_1\right)^n}{\left(1+\left(\frac{t}{\tau_1}\right)^n\right)e^{\frac{-\tau_1}{\tau_2}\cdot\left(\frac{n\cdot\tau_2}{\tau_1}\right)^{\frac{1}{n}}}}+\frac{I_2 e^{-t/\tau_4}\left(t/\tau_3\right)^n}{\left(1+\left(\frac{t}{\tau_3}\right)^n\right)e^{\frac{-\tau_3}{\tau_4}\cdot\left(\frac{n\cdot\tau_4}{\tau_3}\right)^{\frac{1}{n}}}}. \quad (1)$$

Результаты расчёта составили 4,2 и 1,9 А для I_1 и I_2 соответственно, а временные характеристики соответствуют [18] и составляют: τ_1 = 1,1 нс, τ_2 = 2 нс, τ_3 = 12 нс, τ_4 = 37 нс, n = 1,8. По вычисленным значениям построена форма напряжения ЭСР на входе ТЕМ-камеры с входным волновым сопротивлением 50 Ом (рис. 2).

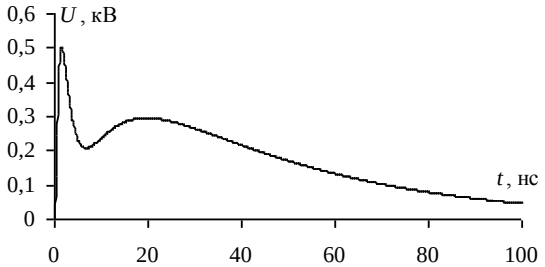


Рис. 2. Форма напряжения ЭСР на входе ТЕМ-камеры

Аналитическая модель форм тока и напряжения ЭСР, наводимых внутри ТЕМ-камеры

Ток (I_K), протекающий в центральном проводнике ТЕМ-камеры, зависит от её КСВН и тока $I_{\text{ЭСР}}(t)$, подводимого к её входу, а также от последовательно включённого R_d, сопротивления (Z_K) ТЕМ-камеры и согласованной нагрузки (Z_C = 50 Ом). Ток I_K может быть получен при известном значении коэффициента отражения S_{11} ТЕМ-камеры как

$$I_K(t)=\frac{I(t)R_d Z_K}{Z_C^2}=\frac{I_{\text{ЭСР}}(t)R_d\left(1-|S_{11}|\right)}{Z_C\left(1+|S_{11}|\right)}. \quad (2)$$

Из (2) видно, что сопротивления R_d, Z_C (5), Z_K окажут существенное влияние на амплитуду тока, протекающего по центральному проводнику ТЕМ-камеры. Предполагая, что ИО располагается на ПП (*1*), на которой имеются печатные проводники в виде МПЛ *2* (рис. 3), связь между центральным проводником *3* ТЕМ-камеры *4* и МПЛ, при их продольном расположении, может быть представлена на основе теоремы Гаусса для магнитной индукции.

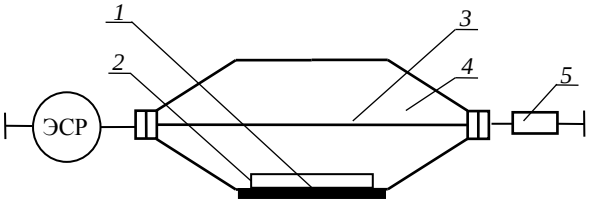


Рис. 3. МПЛ, расположенная внутри ТЕМ-камеры

Поток вектора магнитной индукции ($\mathbf{\Phi}_B$), создаваемый током (I_K), протекающим по центральному проводнику ТЕМ-камеры на расстоянии длины $2(a+b)$ контура [20] в поперечном сечении внешнего проводника ТЕМ-камеры, связан с линией передачи длиной l, расположенной под центральным проводником ($\cos(0°)$ = 1) на расстоянии h от внешнего проводника ТЕМ-камеры, как

$$\mathbf{\Phi}_{31}=\mathbf{\Phi}_B=\int_S \mathbf{B}d\mathbf{S}\approx\omega BS\cos(\theta)\approx\omega Blh=\frac{\omega\mu_0 I_K lh}{2(a+b)}. \quad (3)$$

где ω – круговая частота; B – проекция вектора $\mathbf{B}$ на нормаль к поверхности; S – площадь поверхности; θ – угол между вектором $\mathbf{B}$ и единичным вектором нормали к участку поверхности; μ_0 – магнитная постоянная.

Принимая отсутствие рассеяния ЭМВ на малом объекте, расположенным внутри ТЕМ-камеры [21], и связь частотной зависимости $|S_{31}|$ [20] ТЕМ-камеры с максимальным значением магнитного потока, проходящего через ИО, получим

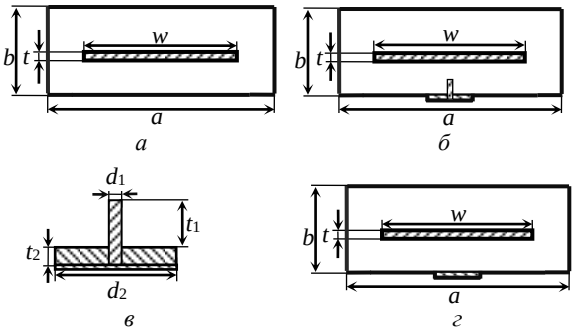
$$|S_{31}|=\left|\frac{U_{вых}}{U_{вх}}\right|=\left|\frac{\mathbf{\Phi}_{31}}{U_{вх}}\right|=\left|\frac{\omega\mu_0 I_K lh}{2(a+b)I_{\text{ЭСР}}(t)R_d}\right|. \quad (4)$$

После вычисления $|S_{31}|$, можно найти наведённый ток на ИО как

$$I_{\text{ИО}}=\frac{U_{\text{вых}}(1-|S_{11}|)}{|S_{31}|Z_C(1+|S_{11}|)}. \quad (5)$$

Геометрические математические модели монополя и микрополосковой линии в ТЕМ-камере

Созданы геометрические математические модели для квазистатического и электродинамического анализа монополя в ТЕМ-камере. Для этого изначально создана группа моделей поперечных сечений малогабаритной ТЕМ-камеры и монополя (рис. 4). Поперечное сечение ТЕМ-камеры с геометрическими параметрами для внешнего (a = 104; b = 31 мм) и внутреннего (w = 40; t = 1 мм) проводников с длиной регулярной части l = 104 мм представлено на рис. 4, *а*. Показаны модель поперечного сечения ТЕМ-камеры с расположенным внутри неё монополем (см. рис. 4, *б*) с заданными значениями геометрических параметров (d_1 = 1,28; d_2 = 4,1; t_1=5; t_2 = 2 мм) (см. рис. 4, *в*), а также модель поперечного сечения с диэлектрической подложкой с относительной диэлектрической проницаемостью ε_r = 2,1, соответствующей тефлону (рис. 4, *г*).



а *б* *в* *г*

Рис. 4. Поперечные сечения ТЕМ-камеры (*а*) с расположенным в центре монополем (*б*) с геометрическими параметрами (*в*) и диэлектрической подложкой (*г*)

Используя созданные модели поперечных сечений (см. рис. 4), собрана принципиальная схема (рис. 5), позволяющая вычислить *S*-параметры, а также токи и напряжения, наводимые на монополь внутри ТЕМ-камеры. Принципиальная схема состоит из пяти (Trl_1–Trl_5) отрезков линий передачи с сопротивлениями $R1 = R2 = 50$ Ом для согласования камеры на концах. Так, Trl_1 и Trl_5 – поперечные сечения ТЕМ-камеры без монополя (см. рис. 4, *а*) имеют длину l = 49,95 мм; Trl_2 и Trl_4 – поперечные сечения ТЕМ-камеры с диэлектрической подложкой длиной l = 1,41 мм (см. рис. 4, *г*). Trl_3 – поперечное сечение ТЕМ-камеры с монополем длиной l = 1,28 мм (см. рис. 4, *б*).

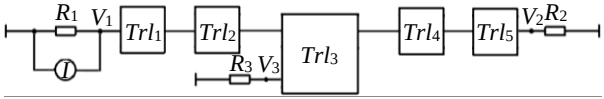
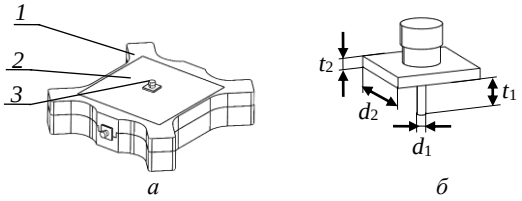


Рис. 5. Схема воздействия ЭСР на вход ТЕМ-камеры с монополем

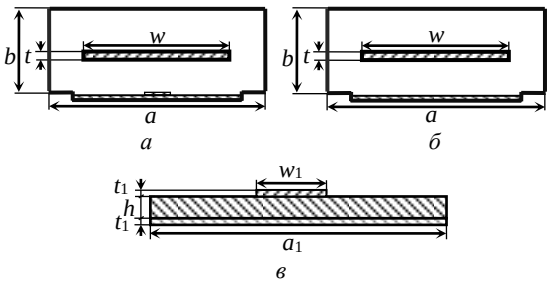
Аналогично по указанным геометрическим размерам создана электродинамическая модель (рис. 6, *а*) ТЕМ-камеры *1* с установленной ПП *2* и с размещённым в центре монополем *3* (см. рис. 6, *б*).

Создана группа моделей поперечных сечений малогабаритной ТЕМ-камеры и МПЛ (рис. 7). В качестве диэлектрика ПП использован фольгированный (t_1 = 105 мкм) стеклотекстолит с ε_r = 4,3, толщиной h = 0,4 мм (см. рис. 7, *б*), ширина активного проводника МПЛ составляла w_1 = 0,5 мм, длина l = 70 мм, а ширина ПП a_1 = 100 мм (см. рис. 7, *в*).



а *б*

Рис. 6. Электродинамическая модель ТЕМ-камеры (*а*) с размещённой в её апертуре ПП с монополем (*б*)



а *б* *в*

Рис. 7. Поперечное сечение ТЕМ-камеры с МПЛ (*а*), диэлектрической подложкой (*б*), с заданными для МПЛ геометрическими параметрами (*в*)

Используя созданные модели поперечных сечений (см. рис. 7, *а*, *б*), собрана схема для квазистатического моделирования амплитуды наведённого напряжения на МПЛ в ТЕМ-камере (рис. 8).

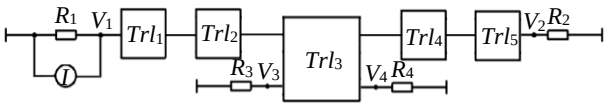
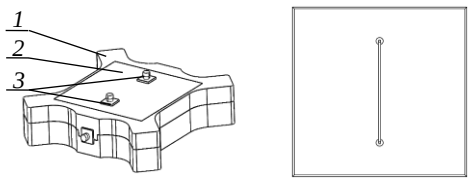


Рис. 8. Схема воздействия ЭСР на вход ТЕМ-камеры с МПЛ для квазистатического моделирования

Создана электродинамическая модель (рис. 9, *а*) ТЕМ-камеры *1* с установленной в апертуру ПП с МПЛ *2* (см. рис. 9, *б*) и размещёнными на её концах СВЧ-соединителями (SMA типа) *3*.



а *б*

Рис. 9. Электродинамическая модель ТЕМ-камеры (*а*) с размещённой в её апертуре ПП с МПЛ (*б*)

Экспериментальная установка

Для подтверждения полученных результатов моделирования собрана экспериментальная установка для измерения напряжения, наведённого на монополь и МПЛ. Так как при моделировании воздействие ЭСР выполнялось на центральный провод-

ник ТЕМ-камеры, то при натурном эксперименте возникла необходимость в устройстве, согласующем генератор ЭСР и центральный проводник ТЕМ-камеры, обеспечивающем прохождение сигнала от наконечника имитатора ЭСР внутрь ТЕМ-камеры. В ГОСТ Р 51317.4.2–2010 [18] представлен адаптер, соединяющий коаксиальный кабель с датчиком тока (рис. 10, *а*). Геометрическая форма адаптера соответствует плавному переходу от диаметра коаксиального кабеля к заданному диаметру датчика. Адаптер должен поддерживать волновое сопротивление 50±1 Ом в полосе частот до 4 ГГц. При этом если для конкретного датчика тока сопротивление, вычисляемое из отношения внешнего диаметра электрода *d* и внутреннего диаметра заземления *D* (см. рис. 10, *б*) не соответствует 50 Ом, тогда конструкция адаптера должна быть такой, чтобы *d* был равен диаметру внутреннего электрода датчика тока.

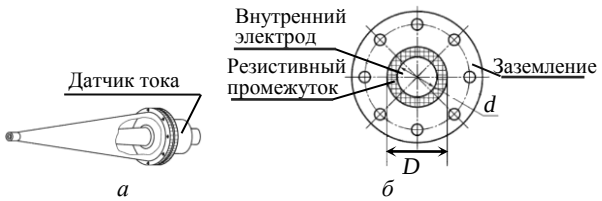
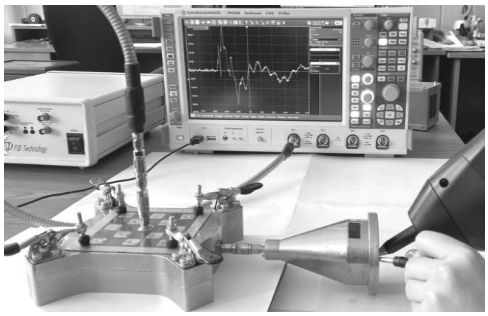


Рис. 10. Конусообразный адаптер для соединения имитатора ЭСР с датчиком тока (*а*); его поперечное сечение (*б*)

Коаксиальная ТЕМ-камера [22] с волновым сопротивлением 50 Ом в диапазоне частот до 12 ГГц соответствует параметрам адаптера, представленного в [18]. Таким образом, использована половина коаксиальной ТЕМ-камеры в качестве адаптера между ТЕМ -камерой и имитатором ЭСР.

Собрана экспериментальная установка (рис. 11, *а*) для измерения наведённых напряжений на монополь, расположенный внутри ТЕМ-камеры, при воздействии ЭСР на её вход.



а

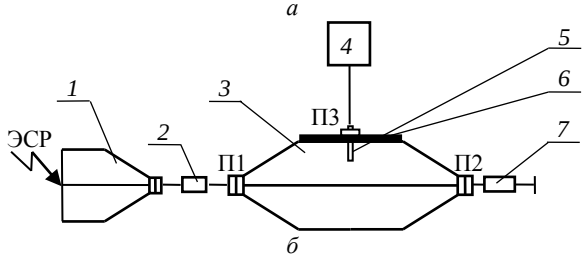


Рис. 11. Экспериментальная установка (*а*); схема (*б*) для измерения формы наведённого напряжения на монополь при воздействии имитатором ЭСР

Схема измерения (см. рис. 11, *б*) состоит из источника ЭСР, адаптера в виде половины коаксиальной камеры *1*, коаксиального перехода РК2-20-03Р-13 *2*, ТЕМ-камеры *3*, к которой подключена согласованная нагрузка сопротивлением 50 Ом *7*, а также монополя *5*, расположенного на ПП *6*, помещённой во внутреннее пространство ТЕМ-камеры.

Напряжение на монополе фиксировалось при помощи программно реализованной маски в осциллографе *4* Rohde&Schwarz RTO2044. В качестве источника ЭСР использовался имитатор ЭСР ONYX 30, который соответствует требованиям стандарта [18].

Схема измерения напряжения на ближнем и дальнем концах МПЛ представлена на рис. 12. Схема состоит из источника ЭСР, адаптера в виде половины коаксиальной ТЕМ-камеры *3*, ТЕМ-камеры *5*, коаксиального перехода РК2-20-03Р-13 *4*, резисторов *1* с сопротивлением 50 Ом, ИО в виде МПЛ *7*, расположенного на ПП *6*, помещённой во внутреннее пространство ТЕМ-камеры. Ключами *К*1 и *К*2 условно показана коммутация для измерения напряжения на ближнем и дальнем концах МПЛ. Напряжение на МПЛ фиксировалось при помощи осциллографа *2* Rohde&Schwarz RTO2044.

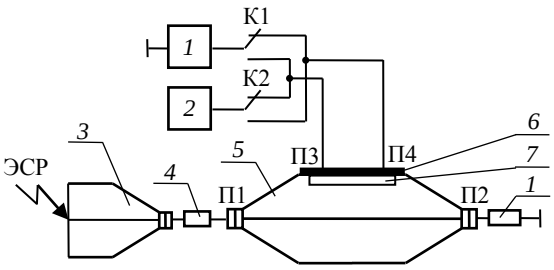


Рис. 12. Схема измерения напряжения на ближнем и дальнем концах МПЛ при воздействии ЭСР

Результаты вычислений и измерений токов и напряжений, наведённых на монополь

Вычисленные аналитическим и квазистатическим методами формы тока в центральном проводнике ТЕМ-камеры представлены на рис. 13.

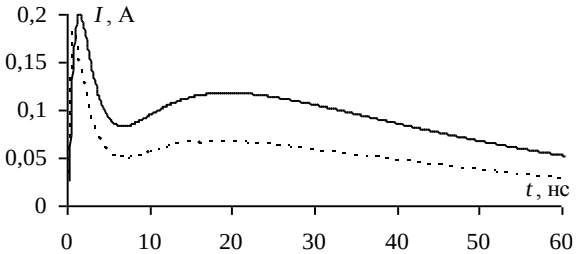


Рис. 13. Вычисленные аналитическим (- -) и квазистатическим (—) методами формы тока ЭСР в центральном проводнике ТЕМ-камеры

Из рис. 13 видно, что максимальный ток в центральном проводнике ТЕМ-камеры при аналитическом и квазистатическом расчётах не превышает 0,18 и 0,2 А соответственно. При этом форма тока, вычисленная аналитическим методом, существенно отличается от исходной формы тока ЭСР. Максимальная разница доходит до 50%. Такое различие

связано с тем, что при расчёте волнового сопротивления ТЕМ-камеры использованы измеренные значения коэффициентов отражения $|S_{11}|$ ТЕМ-камеры.

Собрана (рис. 14) экспериментальная установка для измерения коэффициента передачи $|S_{31}|$.

Измеренные и вычисленные частотные зависимости коэффициента передачи $|S_{31}|$, используя аналитическую (4), квазистатическую (см. рис. 4, *б*) и электродинамическую (см. рис. 6, *а*) модели, представлены на рис. 15.

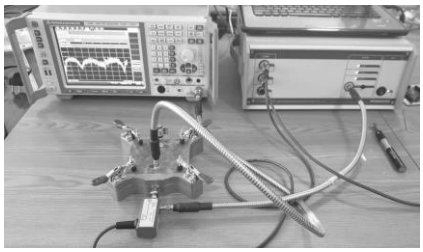


Рис. 14. Экспериментальная установка для измерения частотной зависимости $|S_{31}|$

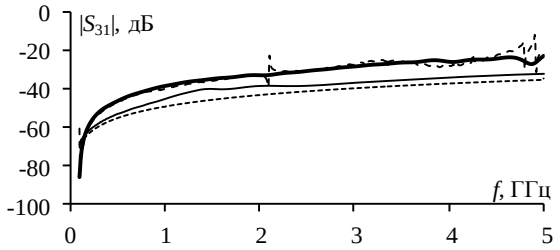


Рис. 15. Измеренные (– –) и вычисленные аналитическим (—), квазистатическим (---) и электродинамическим (—) методами зависимости $|S_{31}|$

Из рис. 15 видно, что с увеличением частоты электромагнитная связь между монополем и центральным проводником ТЕМ-камеры увеличивается. Аналитически вычисленные значения коэффициентов передачи $|S_{31}|$ составляют –45,2 дБ на 1 ГГц и –32 дБ на 5 ГГц. Квазистатическое моделирование на тех же частотах приближалось к –49,1 и –34,5 дБ соответственно. При электродинамическом моделировании получено –38,4 и –22,7 дБ, а при измерениях – –38,9 и –20,5 дБ. Максимальные отклонения результатов аналитического от результатов квазистатического, электродинамического моделирований и измерения составляют 2,5, 9,7 и 11,5 дБ соответственно. Таким образом, аналитическая модель (4) может быть использована при дальнейших вычислениях наведённого тока $I_{ОИ}$ на ИО.

Используя созданные аналитическую (5), квазистатическую (см. рис. 5) и электродинамическую (см. рис. 6) модели, выполнен расчёт наведённого тока на монополь, размещённый внутри ТЕМ-камеры, при воздействии на её вход ЭСР. Вычислены формы наведённого тока на монополь (рис. 16).

Из рис. 16 видно, что максимальные токи, наведённые на монополь при аналитическом расчёте (20 мА) и электродинамическом моделировании (25 мА), отличаются на 5 мА. При квазистатическом моделировании максимальный ток не превышает 10 мА. Это объясняется тем, что расчёт был выполнен при длине отрезка с монополем, равной диаметру самого монополя. Максимальные отклонения результатов аналитического расчёта от результатов электродинамического и квазистатического моделирования составляют 25 и 50% соответственно. При этом длительность ($t_д$) наведённого сигнала при аналитическом, квазистатическом и электродинамическом расчётах составила 0,75; 1,08 и 1,25 нс, время нарастания $t_н$ – 0,33; 0,21 и 0,27 нс и время спада $t_с$ – 0,31; 0,59 и 0,78 нс соответственно.

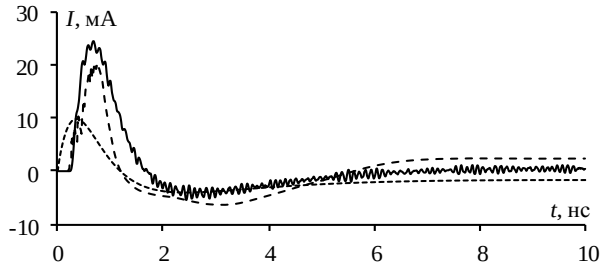


Рис. 16. Вычисленные аналитическим (– –), квазистатическим (---) и электродинамическим (—) методами формы тока, наведённого на монополь

Измерены и вычислены с использованием аналитической, квазистатической и электродинамической моделей формы напряжения, наведённого на монополь (рис. 17).

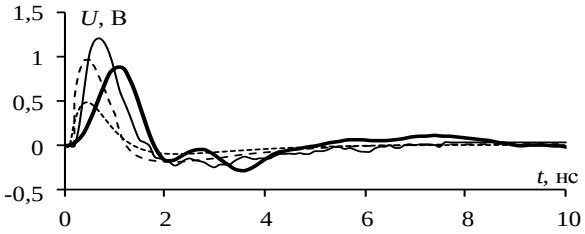


Рис. 17. Измеренные (—) и вычисленные аналитическим (– –), квазистатическим (---) и электродинамическим (—) методами формы напряжения, наведённого на монополь

Из рис. 17 видно, что формы сигналов из результатов вычисления и измерения схожи, но имеются отличия по амплитуде и времени. Так, $t_д$ при аналитическом расчёте составляет 1,05 нс, при квазистатическом – 1,2 нс, при электродинамическом – 1,4 нс, а при измерении – 1,3 нс. При квазистатическом и электродинамическом моделированиях время нарастания ($t_н$) и время спада ($t_с$) сигнала соответствуют $t_н$ = 0,2 нс и $t_с$ = 0,6 нс, при измерении $t_н$ = 0,6 нс и $t_с$ = 0,5 нс, а при аналитическом расчёте $t_н$ = 0,22 нс и $t_с$ = 0,53 нс соответственно. Однако при квазистатическом вычислении максимальная амплитуда наводки составляет 0,5 В, при аналитическом – 0,97 В, при электродинамическом – 1,2 В, а при измерении – 0,9 В. Такое различие результатов с квазистатическим моделированием объясняется тем, что при электродинамическом анализе используется полноценная трёхмерная модель, а также полноволновое моделирование, которое является более кор-

ректным для данной модели по сравнению с квазистатическим моделированием. Кроме того, квазистатическое вычисление выполнено при длине отрезка ТЕМ-камеры, соизмеримой с диаметром монополя. Стоит отметить, что максимальные значения, вычисленные, используя аналитическую модель (0,97 В), близки к измеренным (0,9 В) и вычисленным с помощью электродинамического моделирования (1,2 В). Максимальные отклонения результатов аналитического расчёта от результатов электродинамического моделирования и измерения составляют 23,7 и 7% соответственно. Таким образом, используя размеры ТЕМ-камеры, ИО и входное напряжение ЭСР, возможно вычислить наведённые токи и напряжения на ИО при воздействии ЭСР.

Результаты вычислений и измерений токов и напряжений, наведённых на МПЛ

Вычислены, используя аналитическую, квазистатическую и электродинамическую модели, формы тока, наведённого на МПЛ (рис. 18).

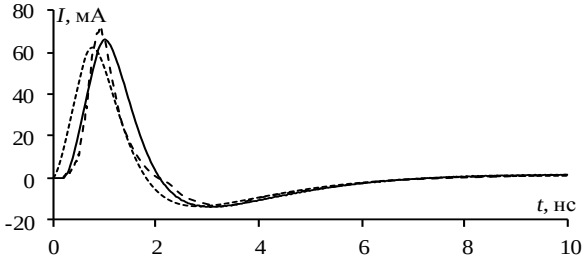


Рис. 18. Вычисленные аналитическим (– –), квазистатическим (---) и электродинамическим (—) методами формы тока, наведённого на МПЛ

Из рис. 18 видно, что значения наведённых токов на МПЛ при аналитическом, квазистатическом и электродинамическом расчётах согласуются. Однако имеются различия по амплитуде и времени. Так, $t_д$ при аналитическом расчёте составляет 1,28 нс, при квазистатическом – 1,53 нс, при электродинамическом – 1,58 нс. Времена нарастания и спада сигнала при аналитическом расчёте соответствуют $t_н$ = 0,4 нс, $t_с$ = 0,6 нс, квазистатическом – $t_н$ = 0,48 нс, $t_с$ = 0,7 нс, а электродинамическом – $t_н$ = 0,52 нс, $t_с$ = 0,73 нс. При этом максимальный ток, наведённый на МПЛ, не превышает 72 мА при аналитическом, 62,2 мА при квазистатическом и 66 мА при электродинамическом расчётах. Максимальные отклонения результатов аналитического расчёта от результатов электродинамического и квазистатического моделирования составляют 8,6 и 13,8% соответственно.

Формы напряжений на ближнем и дальнем концах МПЛ, полученные с использованием квазистатического и электродинамического моделирования, а также из результатов измерения, представлены на рис. 19. Также приведены результаты вычисления формы напряжения на ближнем конце, используя аналитическую модель.

Из рис. 19 видно, что значения напряжений на ближнем и дальнем концах МПЛ при моделировании и измерении близки между собой. Значения $t_д$, $t_н$ и $t_с$ на ближнем конце при квазистатическом и электродинамическом моделированиях совпадают и составляют $t_д$ = 1,7 нс, $t_н$ = 0,5 нс, $t_с$ = 0,7 нс, при измерениях – $t_д$ = 1,9 нс, $t_н$ = 0,7 нс, $t_с$ = 0,6 нс, а при аналитическом расчёте – $t_д$ = 1,4 нс, $t_н$ = 0,5 нс, $t_с$ = 0,65 нс. При этом амплитуда при аналитическом расчёте составляет 3,3 В, при квазистатическом – 2,8 В, при электродинамическом – 3 В, а при измерении – 2,35 В. Максимальные отклонения результатов аналитического расчёта от результатов квазистатического и электродинамического моделирований, а также измерения составляют 15,2; 9 и 28,7% соответственно.

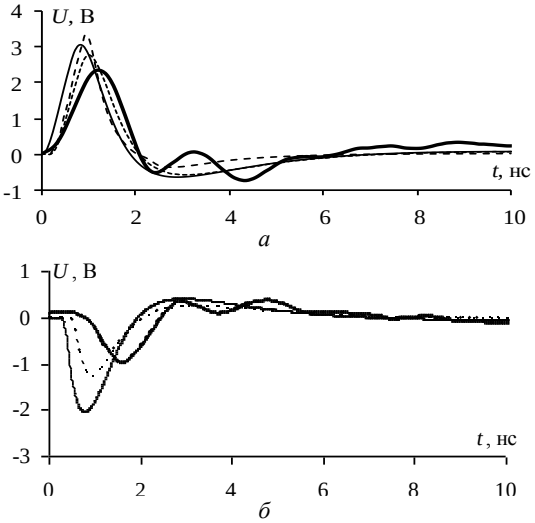


Рис. 19. Измеренные (—) и вычисленные аналитическим (– –), квазистатическим (---) и электродинамическим (—) методами формы напряжения на ближнем (*а*) и дальнем (*б*) концах МПЛ

На дальнем конце МПЛ при квазистатическом и электродинамическом моделированиях $t_д$, $t_н$ и $t_с$ совпадают и составляют $t_д$ = 1,5 нс, $t_н$ = 0,3 нс, $t_с$ = 0,8 нс. Результаты измерений также незначительно отличаются: $t_д$ = 1,5 нс, $t_н$ = 0,5 нс, $t_с$ = 0,6 нс. При этом амплитуда при квазистатическом моделировании составляет –1,3 В, электродинамическом – –2 В, а измерении – –1 В. Различия амплитуд связаны с потерями в проводнике и диэлектрике МПЛ, а также неучётом припоя на СВЧ-соединителях, расположенных с внутренней стороны ПП.

Заключение

Выполнена оценка наведённых токов и напряжений, создаваемых имитатором ЭСР, в малогабаритной ТЕМ-камере на монополь и МПЛ. Представлена аналитическая модель, позволяющая вычислить формы тока и напряжения, наводимых на ИО в виде монополя и МПЛ при воздействии ЭСР на вход ТЕМ-камеры. Созданы модели и выполнено квазистатическое и электродинамическое моделирования, а также натурный эксперимент. При воздействии ЭСР на ТЕМ-камеру с расположенным внутри монополем максимальная амплитуда напряжения на монополе не превышает 0,97 В при аналитическом расчёте, 1,2 В при электродинамическом моделировании и 0,9 В при измерении. Максимальные отклонения результатов аналитического расчёта от ре-

зультатов электродинамического моделирования и измерения составляют 23,7 и 7% соответственно. При воздействии ЭСР на ТЕМ-камеру с расположенной внутри МПЛ максимальная амплитуда напряжения не превышает 3,3 В при аналитическом расчёте, 3 В при электродинамическом моделировании и 2,35 В при измерении. Максимальные отклонения результатов аналитического расчёта от результатов электродинамического моделирования и измерения составляют 9 и 28,7% соответственно. Результаты моделирования схожи с результатами измерений, что делает возможным использование ТЕМ-камеры и половины коаксиальной камеры для исследования влияния подобных воздействий на ИС-электронную компонентную базу и небольшие устройства в целом.

Работа выполнена при финансовой поддержке Российского научного фонда, проект №19-79-10162, https://rscf.ru/project/19-79-10162/.

Литература

1. Lin N. Evolution of ESD process capability in future electronic industry / N. Lin, Y. Liang, Dr. P. Wang // 15th International conference on electronic packaging technology. – 2014. – P. 1556–1560 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/6922951, свободный (дата обращения: 2.02.2022).

2. Кечиев Л.Н. Защита электронных средств от воздействия статического электричества / Л.Н. Кечиев, Е.Д. Пожидаев. – М.: ИД «Технологии», 2005. – 352 с.

3. Amerasekera A. The impact of technology scaling on ESD robustness and protection circuit design / A. Amerasekera, C. Duvvury // IEEE Transactions on components, packaging, and manufacturing technology: Part A. – 1995. – Vol. 18, No. 2. – P. 314–320.

4. Narita K. Low clamping voltage protection for improvements of powered ESD robustness / K. Narita, M. Okushima // 40th Electrical overstress/electrostatic discharge symposium (EOS/ESD). – 2018. – P. 1–8 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/8509793, свободный (дата обращения: 5.02.2022).

5. Wang A. On a dual-polarity on-chip electrostatic discharge protection structure / A. Wang, C. Tsay // IEEE Transactions on electron devices. – 2001. – Vol. 48, No. 5. – P. 978–984.

6. Capacitor-couple ESD protection circuit for deep-submicron low-voltage CMOS ASIC / M. Ker, C. Wu, T. Cheng, H.H. Chang // IEEE Transactions on very large scale integration (VLSI) systems. – 1996. – Vol. 4, No. 3. – P. 307–321.

7. Ostermann T. Soft Failures in Integrated Circuits as a Matter of ESD Events // International conference on IC design and technology (ICICDT). – 2018. – P. 169–172 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/8399783, свободный (дата обращения: 7.02.2022).

8. Investigation on ESD failures of RF IC / D. Yang, N. Mei, T. Sun, L. Yuan, S. Chao // International conference on electronic packaging technology (ICEPT). – 2020 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/9202494, свободный (дата обращения: 25.02.2022).

9. Xijun Z. Study on effect experiment of ESD EMP to – single chip microcontroller // IEEE International symposium on microwave, antenna, propagation and EMC technologies. – 2005. – P. 631–634 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/1617990, свободный (дата обращения: 25.02.2022).

10. IEC 61967-3. Integrated circuits – Measurement of electromagnetic emissions. – Part 3: Measurement of radiated emissions. – Surface scan method, 2014-08 [Электронный ресурс]. – Режим доступа: https://webstore.iec.ch/publication/6186, свободный (дата обращения: 27.02.2022).

11. IEC 61000-4-21, Electromagnetic compatibility (EMC). – Part 4-21: Testing and measurement techniques – reverberation chamber test methods, 2003-08 [Электронный ресурс]. – Режим доступа: https://webstore.iec.ch/publication/4191, свободный (дата обращения: 01.03.2022).

12. Crawford M.L. Generation of standard EM fields using TEM transmission cell // IEEE Transaction on electromagnetic compatibility. – 1974. – Vol. EMC-16, No. 4. – P. 40–46.

13. Integrated Circuits. Measurement of Electromagnetic Emissions. – Part 2: Measurement of Radiated Emissions, TEM Cell and Wideband TEM Cell Method, IEC 61967-2, First Edit, 2005 [Электронный ресурс]. – Режим доступа: https://webstore.iec.ch/publication/6185, свободный (дата обращения: 05.03.2022).

14. Integrated Circuits. Measurement of Electromagnetic Immunity. Part 2: Measurement of Radiated Immunity, TEM Cell and Wideband TEM Cell Method, IEC 62132-2, First Edit., 2010 [Электронный ресурс]. – Режим доступа: https://webstore.iec.ch/publication/6508, свободный (дата обращения: 10.03.2022).

15. Measurement of microcontroller radiated emissions at different operation modes / A.V. Demakov, A.V. Osintsev, V.A. Semenjuk, M.E. Komnatnov // 2021 IEEE 22nd International conference of young professionals in electron devices and materials (EDM). – Russia: Souzga, the Altai Republic, 2021. – P. 193–197 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/9507688, свободный (дата обращения: 6.02.2022).

16. Демаков А.В. Разработка ТЕМ-камеры для испытаний интегральных схем на электромагнитную совместимость / А.В. Демаков, М.Е. Комнатнов // Доклады ТУСУР. – 2018. – Т. 21, № 1. – С. 52–56.

17. Demakov A.V. TEM cell for testing lowprofile integrated circuits for EMC / A.V. Demakov, M.E. Komnatnov. – International conference of young specialists on micro/nanotechnologies and electron devices (EDM) // Russia: Chemal, 2020. – P. 154–158 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/9153508, свободный (дата обращения: 6.02.2022).

18. IEC 61000-4-2. Electromagnetic compatibility (EMC). – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test. – 2008. – 26 p.

19. Numerical modeling of electrostatic discharge generators / D. Pommerenke, R. Chundry, T.V. Doren, J.L. Drewniak, A. Shashindranarh, K. Wang // IEEE Transactions on electromagnetic compatibility. – 2003. – No. 42 (2). – P. 258–270.

20. Quantifying electric and magnetic field coupling from integrated circuits with TEM cell measurements / V. Kasturi, S. Deng, T. Hubing, D. Beetner // IEEE Int. symp. on electromagn. compat. – 2006. – P. 422–425 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/1706339, свободный (дата обращения: 8.02.2022).

21. Wilson P.F. Small aperture analysis of the dual TEM cell and an investigation of test object scattering in a single TEM cell / P.F. Wilson, M.T Ma. – National bureau of standards. – 1984. – 57 p.

22. Пат. 2 759 079 РФ. Коаксиальная камера для измерения эффективности электромагнитного экранирования радиопоглощающих материалов / А.В. Демаков, М.Е. Комнатнов, А.А. Иванов И.И. Николаев, Т.Р. Газизов. – № 2020131978; заявл. 29.09.2020; опубл.: 09.11.2021, Бюл. №31. – 10 с.

Дроздова Анастасия Александровна
Аспирант каф. телевидения и управления (ТУ)
Томского государственного университета
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-999-619-37-70
Эл. почта: anastasiya.drozdova.00@list.ru

Комнатнов Максим Евгеньевич
Канд. техн. наук, доцент, доцент каф. ТУ ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-952-888-38-96
Эл. почта: maxmek@mail.ru

Drozdova A.A., Komnatnov M.E.

Evaluating the level of electromagnetic interference generated by the ESD source in the TEM-cell

We evaluated the induced electromagnetic interference on a monopole and a microstrip line generated by an electrostatic discharge source in a small-sized TEM-cell. Analytical, quasi-static, and electrodynamic models are presented for calculating the waveforms and amplitudes of currents and voltages induced on the monopole and the microstrip line. These waveforms are presented for analytical, quasi-static, electrodynamic calculations, and measurements. The maximum deviations of analytical and electrodynamic calculations results for the monopole and the microstrip line are 25 and 9%. An approach is presented for using half of the coaxial cell as a matching device between the electrostatic discharge source and the TEM-cell. The results of calculations and measurements agree well, which indicates the possibility of using a small-sized TEM-cell and half of the coaxial cell. These devices could be helpful to study the effect of electrostatic discharge -generated electromagnetic interference on integrated circuits, electronic component base, and small devices in general.

Keywords: electromagnetic compatibility, susceptibility, small-sized TEM-cell, electrostatic discharge
DOI: 10.21293/1818-0442-2022-25-4-28-36

References

1. Lin N., Liang Y., Wang Dr. P. Evolution of ESD process capability in future electronic industry. *15th International Conference on Electronic Packaging Technology*, 2014, pp. 1556–1560. Available at: https://ieeexplore.ieee.org/document/6922951, free (Accessed: February 02, 2022).

2. Kechiev L.N, Pozhidaev E.D. *Zashchita elektronnykh sredstv ot vozdeystviya staticheskogo elektrichestva* [Protection of electronic means from the effects of static electricity]. Moscow, Publ. house "Technologies". 2005. 352 p. (in Russ.).

3. Amerasekera A., Duvvury C. The impact of technology scaling on ESD robustness and protection circuit design / A. Amerasekera. *IEEE Transactions on Components, Packaging, and Manufacturing Technology: part A*, 1995, vol. 18, no. 2, pp. 314–320.

4. Narita K., Okushima M. Low clamping voltage protection for improvements of powered ESD robustness. *40th Electrical overstress/electrostatic discharge symposium (EOS/ESD)*, 2018, pp. 1–8. Available at: https://ieeexplore. ieee.org/document/8509793, free (Accessed: February 05, 2022).

5. Wang A., Tsay C. On a dual-polarity on-chip electrostatic discharge protection structure. *IEEE Transactions on Electron Devices*, 2001, vol. 48, no. 5, pp. 978–984.

6. Ker M., Wu C., Cheng T., Chang H.H. Capacitor-couple ESD protection circuit for deep-submicron low-voltage CMOS ASIC. *IEEE Transactions on Very Large-scale Integration (VLSI) Systems*, 1996, vol. 4, no. 3, pp. 307–321.

7. Ostermann T. Soft Failures in Integrated Circuits as a Matter of ESD Events. *International Conference on IC Design and Technology (ICICDT)*, 2018, pp. 169–172. Available at: https://ieeexplore.ieee.org/document/8399783, free (Accessed: February 07, 2022).

8. Yang D., Mei N., Sun T., Yuan L., Chao S. Investigation on ESD failures of RF IC. *International Conference on Electronic Packaging Technology (ICEPT)*, 2020. Available at: https://ieeexplore.ieee.org/document/9202494, free (Accessed: February 25, 2022).

9. Xijun Z. Study on effect experiment of ESD EMP to - single chip microcontroller. *IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies*, 2005, pp. 631–634. Available at: https://ieeexplore.ieee.org/document/1617990, free (Accessed: February 25, 2022).

10. *IEC 61967-3. Integrated circuits – Measurement of Electromagnetic Emissions. – Part 3: Measurement of Radiated Emissions – Surface Scan Method, 2014-08*. Available at: https://webstore.iec.ch/publication/6186, free (Accessed: February 27, 2022).

11. *IEC 61000-4-21, Electromagnetic Compatibility (EMC). Part 4-21: Testing and Measurement Techniques – Reverberation Chamber Test Methods, 2003-08*. Available at: https://webstore.iec.ch/publication/4191, free (Accessed: March 01, 2022).

12. Crawford M.L. Generation of standard EM fields using TEM transmission cell. *IEEE Transaction on Electromagnetic Compatibility*, 1974, vol. EMC-16, no. 4, pp. 40–46.

13. *Integrated Circuits. Measurement of Electromagnetic Emissions. Part 2: Measurement of Radiated Emissions, TEM Cell and Wideband TEM Cell Method, IEC 61967-2*. First Edit, 2005. Available at: https://webstore.iec.ch/publication/6185, free (Accessed: March 05, 2022).

14. *Integrated Circuits. Measurement of Electromagnetic Immunity. Part 2: Measurement of Radiated Immunity, TEM Cell and Wideband TEM Cell Method, IEC 62132-2*, First Edit., 2010. Available at: https://webstore.iec.ch/publication/6508, free (Accessed: March 10, 2022).

15. Demakov A.V., Osintsev A.V., Semenjuk V.A., Komnatnov M.E. Measurement of microcontroller radiated emissions at different operation modes. *2021 IEEE 22nd International Conference of Young Professionals in Electron Devices and Materials (EDM)*, Russia: Souzga, the Altai Republic, 2021, pp. 193–197. Available at: https://ieeexplore.ieee.org/document/9507688, free (Accessed: February 06, 2022).

16. Demakov A.V., Komnatnov M.E. Development of a TEM-cell for electromagnetic compatibility testing of integrated circuits. *Proceedings of TUSUR University*, 2018, vol. 21, no. 1, pp. 52–56 (in Russ.).

17. Demakov A.V., Komnatnov M.E. TEM cell for testing lowprofile integrated circuits for EMC. *International Conference of Young Specialists on Micro/nanotechnologies and Electron Devices (EDM)*, Russia: Chemal, 2020, pp. 154–158. Available at: https://ieeexplore.ieee.org/document/9153508, free (Accessed: February 06, 2022).

18. *IEC 61000-4-2. Electromagnetic Compatibility (EMC). Part 4-2: Testing and Measurement Techniques – Electrostatic Discharge Immunity Test*, 2008, 26 p.

19. Pommerenke D., Chundry R., Doren T.V., Drewniak J.L., Shashindranarh A., Wang K. Numerical modeling of electrostatic discharge generators. *IEEE Transactions on Electromagnetic Compatibility*, 2003, no. 42 (2), pp. 258–270.

20. Kasturi V., Deng S., Hubing T., Beetner D. Quantifying electric and magnetic field coupling from integrated circuits with TEM cell measurements. *IEEE International Sym-*

posium on Electromagnetic Compatibility, 2006, pp. 422–425. Available at: https://ieeexplore.ieee.org/document/1706339, free (Accessed: February 8, 2022).

21. Wilson P.F., Ma M.T. Small aperture analysis of the dual TEM cell and an investigation of test object scattering in a single TEM cell. *National Bureau of Standards*, 1984, 57 p.

22. Demakov A.V., Komnatnov M.E., Ivanov A.A., Nikolaev I.I., Gazizov T.R. *Koaksialnaya kamera dlya izmereniya effektivnosti elektromagnitnogo ekranirovaniya radiopogloshchayushchikh materialov* [Coaxial chamber for measuring the effectiveness of electromagnetic shielding of radio absorbing materials]. Patent RF, no. 2020131978, 2021 (in Russ.).

Anastasiya A. Drozdova
Postgraduate student, Department of Television and Control, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-999-619-37-70
Email: anastasiya.drozdova.00@list.ru

Maxim E. Komnatnov
Candidate of Science in Engineering, Assistant Professor, Department of Television and Control, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-952-888-38-96
Email: maxmek@mail.ru

УДК 621.382

И.М. Добуш, К.В. Дудинов, Д.Д. Зыков, А.С. Сальников, А.А. Попов, А.М. Емельянов, Д.С. Брагин, Д.Р. Хайров

Разработка масштабируемой малосигнальной модели 0,1 мкм GaAs-pHEMT-транзистора для усилительных применений

Описана разработка масштабируемой малосигнальной модели pHEMT-транзистора на основе GaAs с проектной нормой 0,1 мкм для применения в САПР электронных устройств. При её построении в качестве базового был выбран транзистор с общей шириной затвора 6×35 мкм, для которого достигнута хорошая точность в различных режимах работы по постоянному току и в широком диапазоне частот. Разработанная модель может использоваться для ускорения и удешевления разработки усилительных СВЧ-монолитных интегральных схем, в которых базовым активным элементом является pHEMT-транзистор. В дальнейших исследованиях полученная модель станет основной для создания более сложных типов моделей, таких как шумовые и нелинейные.
Ключевые слова: СВЧ-транзистор, модель СВЧ-транзистора, СВЧ-интегральная схема, экстракция параметров модели, эквивалентная схема, малосигнальная модель, линейные параметры, pHEMT, GaAs.
DOI: 10.21293/1818-0442-2022-25-4-37-47

Сверхвысокочастотные (СВЧ) интегральные схемы (ИС) являются неотъемлемыми компонентами при разработке современных и перспективных радиоэлектронных устройств и систем [1–5]. Они могут производиться в больших объемах, имеют низкую стоимость изготовления в массовом производстве, малые вес и размеры, хорошую воспроизводимость параметров, высокую надёжность [6–8]. Вместе с тем требования к качеству и скорости проектирования СВЧ ИС всё более ужесточаются.

Общей научно-технической задачей при создании любых интегральных СВЧ-устройств на всех этапах цикла разработки является создание библиотек стандартных элементов [9]. Проектирование современных СВЧ ИС невозможно без использования специализированных систем автоматизированного проектирования (САПР) электронных устройств. При этом важную роль в процессе проектирования играют библиотеки элементов, которые интегрируются в САПР и позволяют осуществить моделирование и разработку топологии ИС для конкретной технологии изготовления. Библиотека элементов позволяет наиболее просто передать сведения о технологии проектировщикам схем как внутри предприятия, так и сторонним организациям. Это позволит повысить эффективность разработки СВЧ-устройств. Этим определяется актуальность исследования.

Важнейшей составной частью библиотеки являются электрические модели отдельных элементов ИС, позволяющие предсказать создаваемые на их основе характеристики разрабатываемой схемы. Электрические модели различаются по сложности, зависящей от различных факторов (активные или пассивные компоненты, количество изменяемых параметров, моделируемые эффекты, особенности технологии и др.) [10–15].

Данная работа посвящена разработке масштабируемой малосигнальной модели pHEMT-транзисторов, изготовленных на основе GaAs с проектной нормой 0,1 мкм. pHEMT-транзистор является базовым активным элементом для разработки усилительных СВЧ ИС, а его линейная модель является основной для создания более сложных типов моделей, таких как шумовые и нелинейные.

Описание масштабируемой малосигнальной модели транзистора

Для восстановления линейных параметров из измеренных данных матрицы транзисторов использовалась малосигнальная эквивалентная схема (ЭС), состоящая из 18 элементов (рис. 1). ЭС, а также методики экстракции её параметров и выбора репрезентативных транзисторов подробно описаны в работах [16, 17].

К внешним элементам малосигнальной ЭС относятся ёмкости, ассоциируемые с электродами транзистора C_{pg}, C_{pd}, C_{pgd}, сопротивления металлизации и контактных областей R_g, R_s, R_d и индуктивности металлизации L_g, L_s, L_d.

Внутренние параметры ЭС восстановлены во всех рабочих точках базового транзистора. Для возможности выбора рабочей точки в малосигнальной модели реализован блок считывания файла, в котором записаны значения внутренних элементов ЭС, а также значения токов стока и затвора для базового транзистора в каждой рабочей точке.

Среди внутренних элементов ЭС присутствуют дифференциальные проводимости диодов затвора R_{gdf}, R_{gsf}, благодаря которым ЭС может воспроизводить *S*-параметры транзистора в режимах, где ток затвора оказывает существенное влияние на характеристики прибора.

Для возможности масштабирования малосигнальной модели относительно единичной ширины затвора *UGW* и количества затворов *NFG* в подсхеме реализованы следующие выражения:

$$SFN = \frac{NFG}{NFG_{ref}}, \quad (1)$$

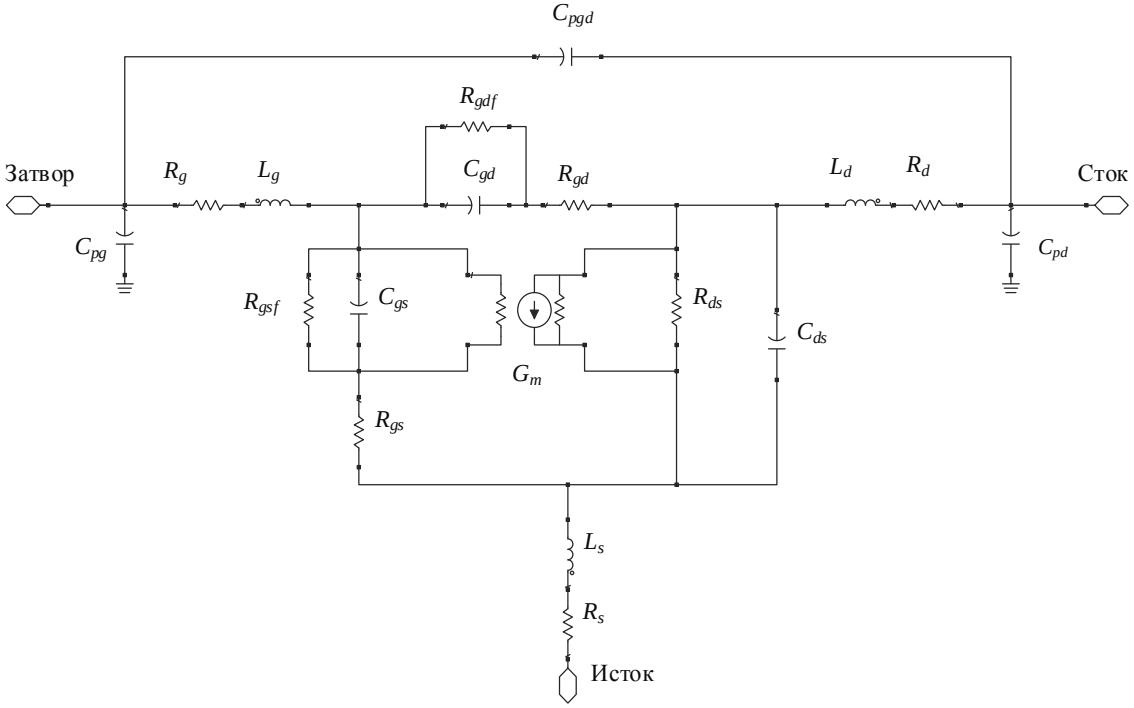


Рис. 1. Малосигнальная эквивалентная схема транзистора

$$SFGW = \frac{UGW}{UGW_{ref}}, \quad (2)$$

$$SF = SFN \cdot SFGW, \quad (3)$$

$$SFG = \frac{SFN}{SFGW}, \quad (4)$$

где UGW – единичная ширина затвора текущей малосигнальной модели; NFG – число затворов текущей малосигнальной модели; UGW_{ref} – единичная ширина затвора базового транзистора; NFG_{ref} – число затворов базового транзистора.

Выражения (1)–(4) используются в виде коэффициентов пропорциональности для значений элементов ЭС базового транзистора при изменении параметров UGW и NFG масштабируемой малосигнальной модели.

Сопротивление затвора R_g масштабируется по правилу

$$R_g = \frac{R_{g\_ref}}{SFG}, \quad (5)$$

где R_g – сопротивление затвора в текущей малосигнальной модели с единичной шириной затвора UGW и числом затворов NFG; R_{g_ref} – сопротивление затвора в малосигнальной модели базового транзистора.

Сопротивления R_s, R_d, R_{gs}, R_{gd}, R_{gsf}, R_{gdf} масштабируются по правилу

$$R = \frac{R_{ref}}{SF}, \quad (6)$$

где R – значение сопротивления в текущей малосигнальной модели с единичной шириной затвора UGW и числом затворов NFG; R_{ref} – значение сопротивления в малосигнальной модели базового транзистора.

Внешние ёмкости C_{pg}, C_{pd}, C_{pgd} масштабируются по правилу

$$C = C_{ref} \cdot SFN, \quad (7)$$

где C – значение ёмкости в текущей малосигнальной модели с единичной шириной затвора UGW и числом затворов NFG; C_{ref} – значение ёмкости в малосигнальной модели базового транзистора.

Индуктивности L_g и L_d масштабируются по правилу

$$L = L_{ref} \cdot SFGW, \quad (8)$$

где L – значение индуктивности в текущей малосигнальной модели с единичной шириной затвора UGW и числом затворов NFG; L_{ref} – значение индуктивности в малосигнальной модели базового транзистора.

Индуктивность L_s, внутренние ёмкости C_{gs}, C_{gd}, C_{ds} и крутизна транзистора G_m масштабируются по правилу

$$X = X_{ref} \cdot SF, \quad (9)$$

где X – значение элемента в текущей малосигнальной модели с единичной шириной затвора UGW и числом затворов NFG; X_{ref} – значение элемента в малосигнальной модели базового транзистора.

Экстракция параметров малосигнальной модели базового транзистора и её верификация

При построении масштабируемой малосигнальной модели в качестве базового был выбран транзистор с общей шириной затвора 6×35 мкм. Результаты восстановления некоторых внутренних параметров малосигнальной ЭС базового транзистора во множестве рабочих точек представлены на рис. 2.

На рис. 3 представлены результаты измерений семейства выходных вольт-амперных характеристик (ВАХ) базового транзистора с отмеченными точками, в которых проводилась верификация малосигнальной модели.

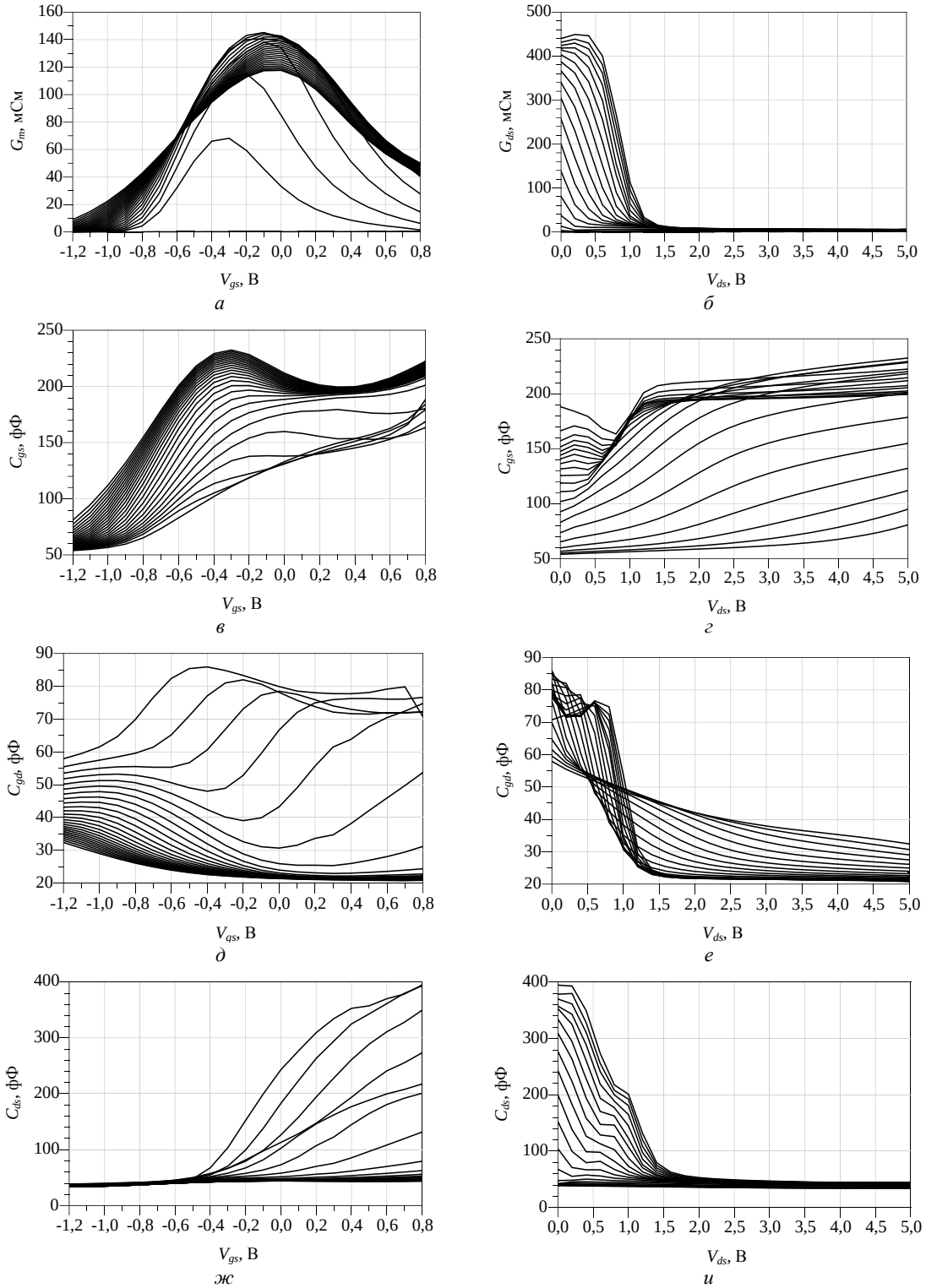


Рис. 2. Внутренние параметры ЭС транзистора с общей шириной затвора 6×35 мкм во множестве рабочих точек: крутизна (*а*); выходная проводимость (*б*); ёмкость затвор-исток (*в*, *г*); ёмкость затвор-сток (*д*, *е*); ёмкость сток-исток (*ж*, *и*)

Сравнение измеренных и рассчитанных *S*-параметров в данных точках в диапазоне частот от 0,1 до 67 ГГц приведено на рис. 4.

Верификация малосигнальной модели транзистора по критерию масштабирования относительно периферии затвора

Для верификации малосигнальной модели транзистора по критерию масштабирования относительно единичной ширины затвора были выбраны результаты измерений *S*-параметров транзисторов с периферией затвора 6×25 и 6×50 мкм. Сравнение измеренных и рассчитанных *S*-параметров для данных транзисторов представлено на рис. 5–6.

Для верификации малосигнальной модели по критерию масштабирования относительно числа затворов были выбраны результаты измерений

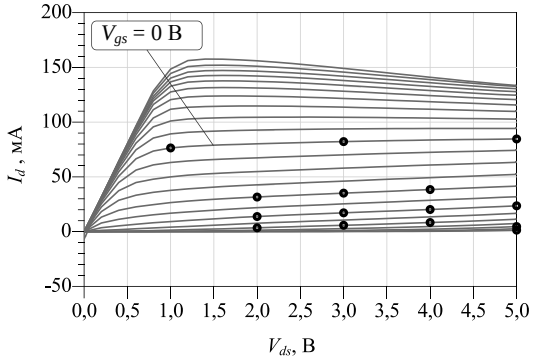


Рис. 3. Результаты измерений семейства выходных ВАХ базового транзистора с отмеченными точками для проведения верификации малосигнальной модели

S-параметров транзисторов с периферией затвора 2×35, 4×35 и 8×35 мкм. Сравнение измеренных и рассчитанных *S*-параметров для данных транзисторов представлено на рис. 7–9.

Заключение

Разработана масштабируемая малосигнальная модель pHEMT-транзисторов, изготовленных на основе GaAs с проектной нормой 0,1 мкм для применения в САПР электронных устройств. При её построении в качестве базового был выбран транзистор с общей шириной затвора 6×35 мкм, для которого достигнута хорошая точность в различных режимах работы по постоянному току и в широком диапазоне частот.

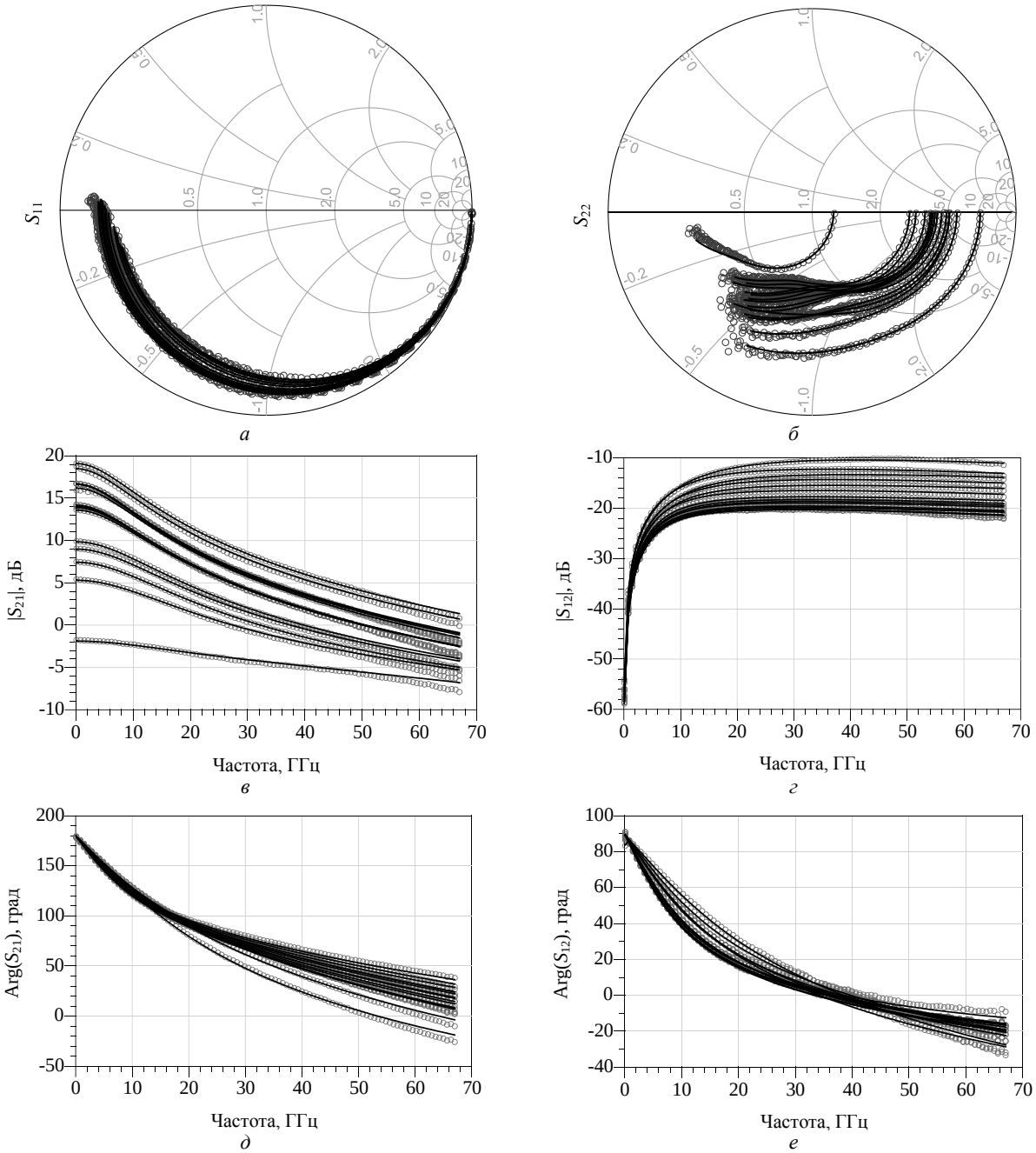


Рис. 4. Сравнение измеренных (точечные линии) и рассчитанных (сплошные линии) *S*-параметров базового транзистора в диапазоне частот от 0,1 до 67 ГГц

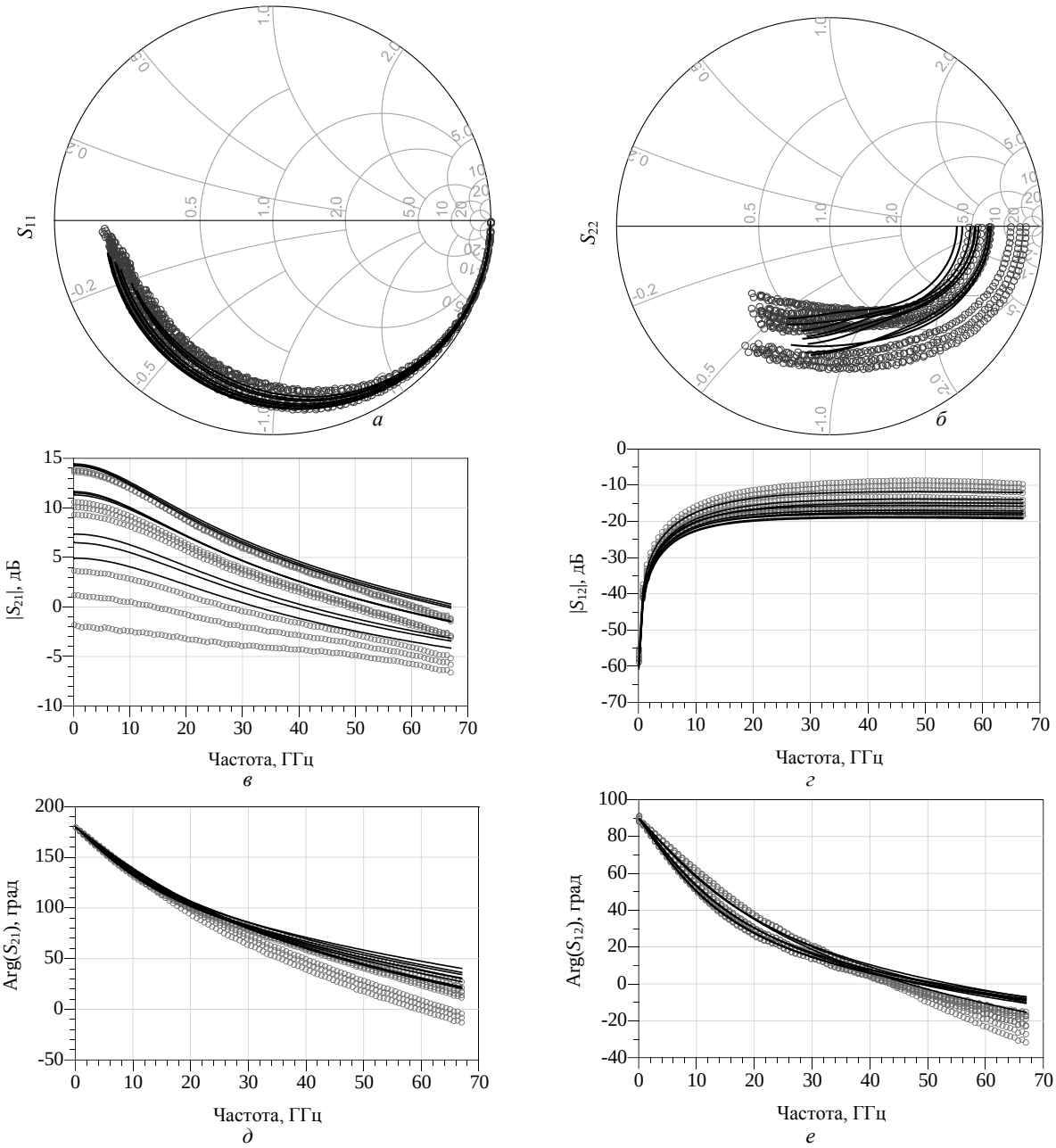


Рис. 5. Сравнение измеренных (точечные линии) и рассчитанных (сплошные линии) *S*-параметров транзистора с периферией затвора 6×25 мкм в диапазоне частот от 0,1 до 67 ГГц при напряжениях V_{ds} = (2; 3; 4) В и V_{gs} = (–0,8; –0,6; – 0,4) В

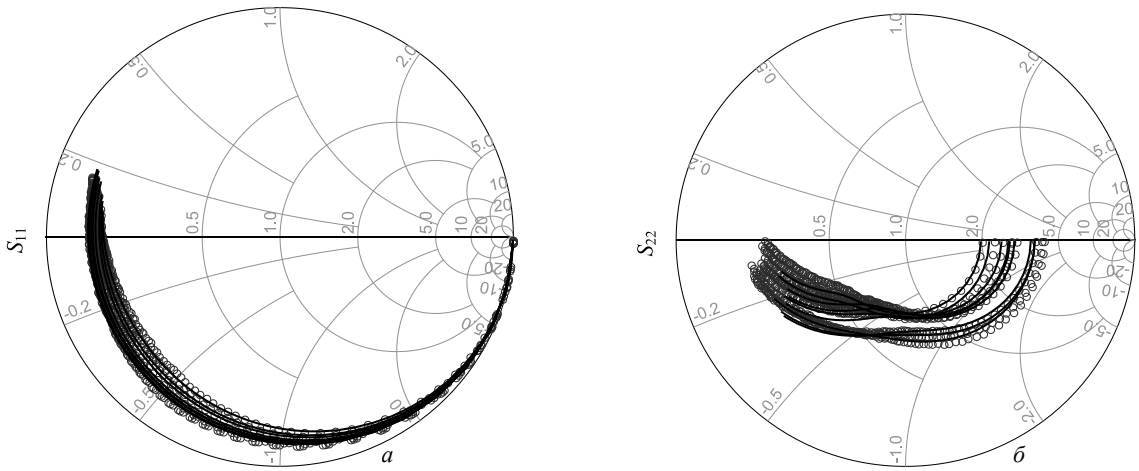


Рис. 6 (начало)

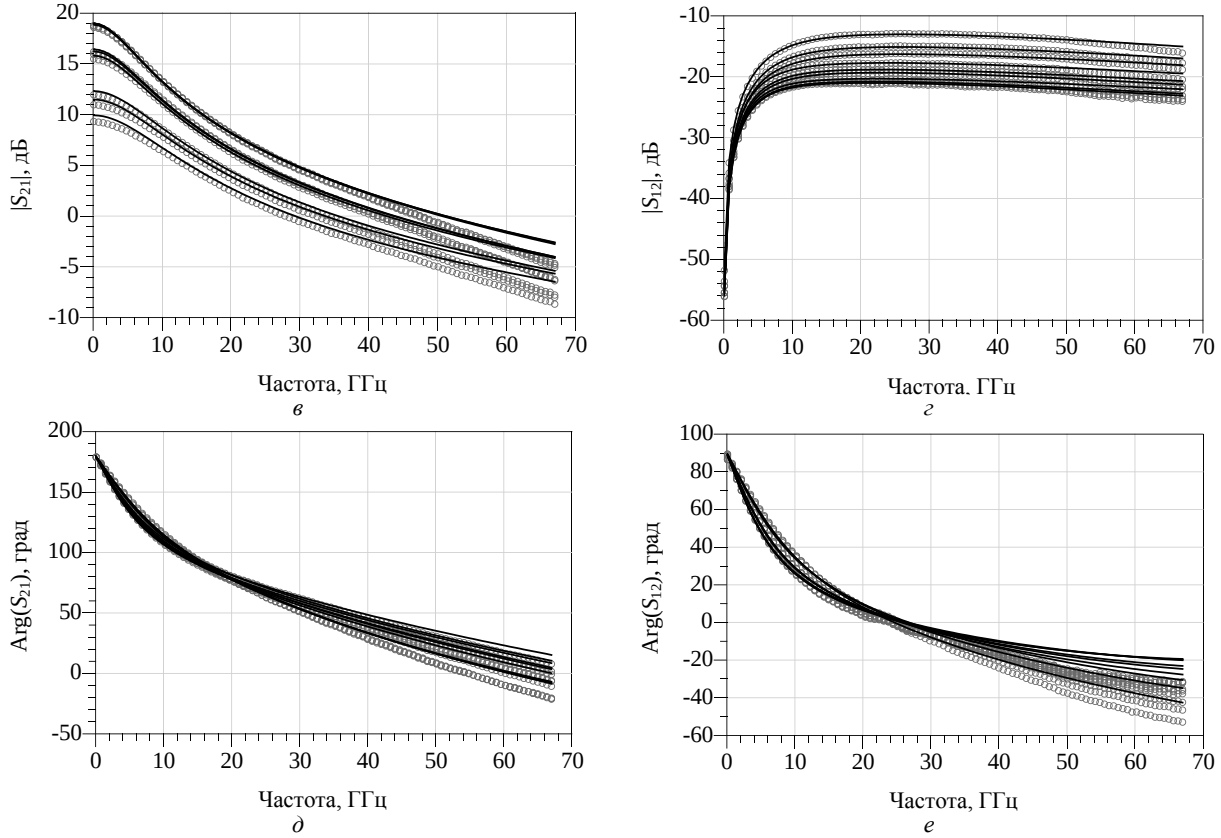


Рис. 6 (окончание). Сравнение измеренных (точечные линии) и рассчитанных (сплошные линии) *S*-параметров транзистора с периферией затвора 6×50 мкм в диапазоне частот от 0,1 до 67 ГГц при напряжениях V_{ds} = (2; 3; 4) В и V_{gs} = (–0,8; –0,6; – 0,4) В

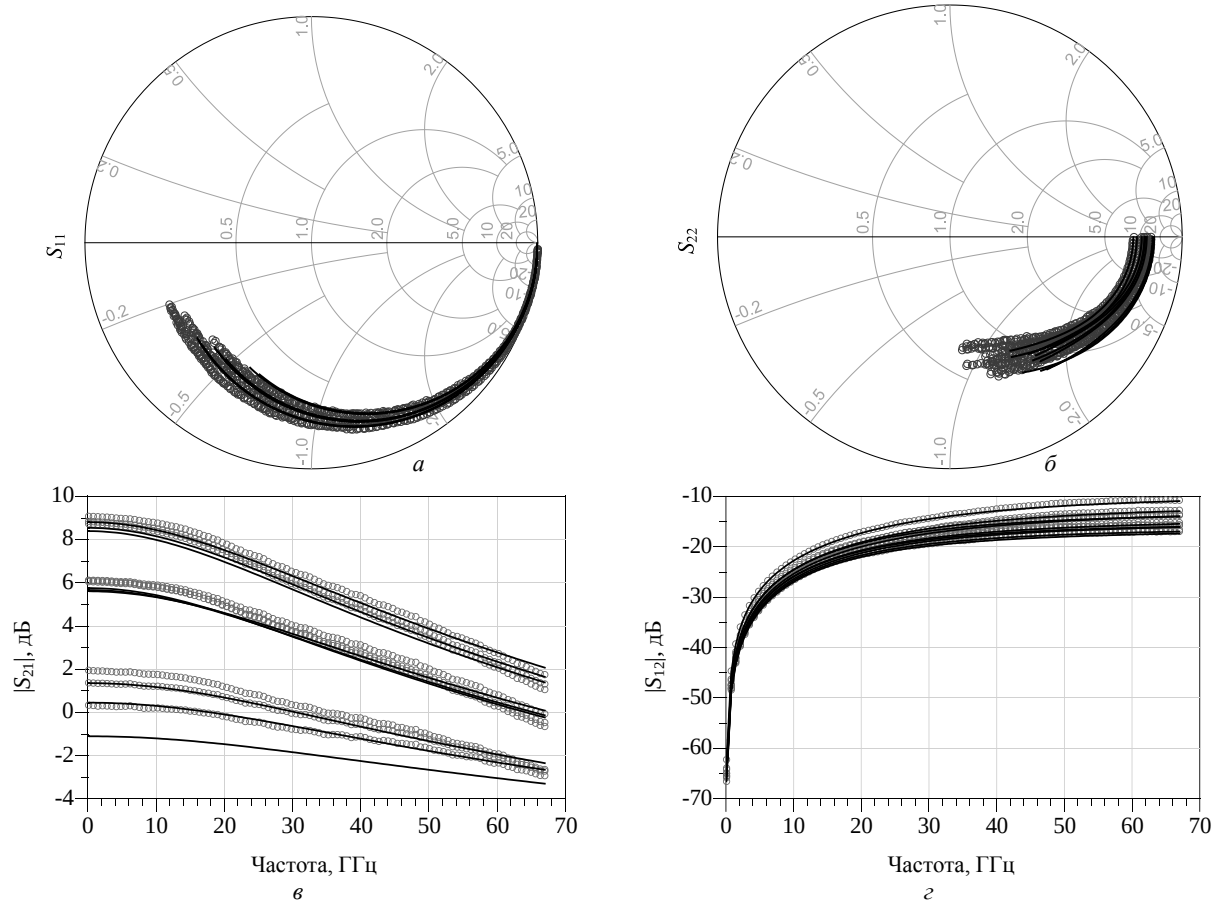
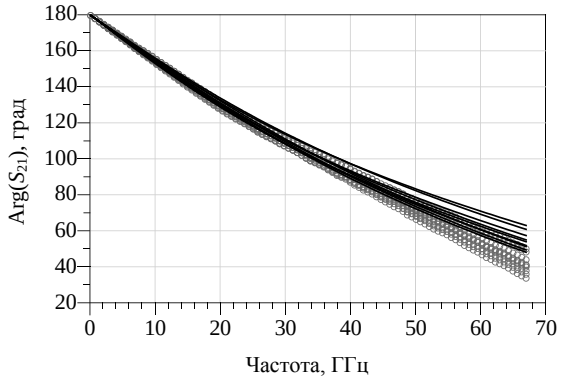
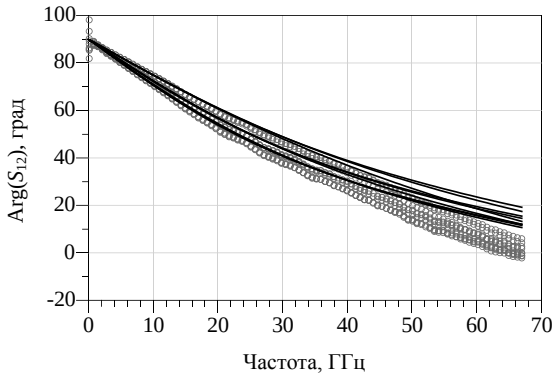


Рис. 7 (начало)

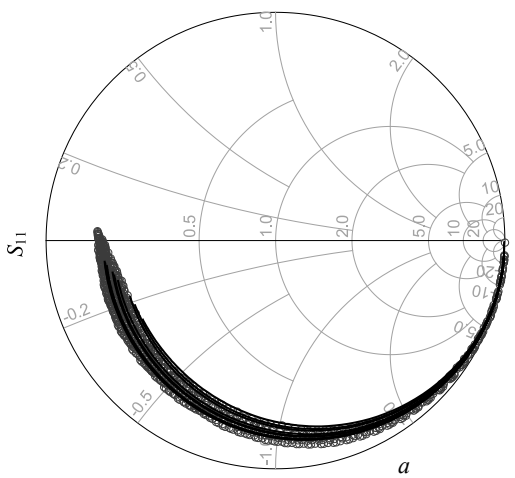


д

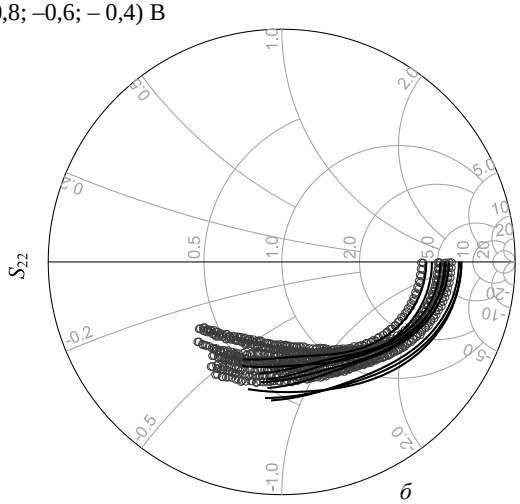


е

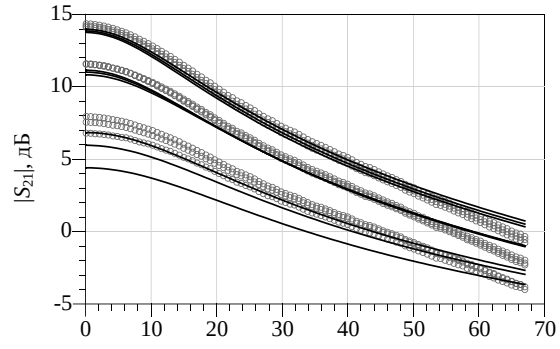
Рис. 7 (окончание). Сравнение измеренных (точечные линии) и рассчитанных (сплошные линии) *S*-параметров транзистора с периферией затвора 2×35 мкм в диапазоне частот от 0,1 до 67 ГГц при напряжениях V_{ds} = (2; 3; 4) В и V_{gs} = (–0,8; –0,6; – 0,4) В



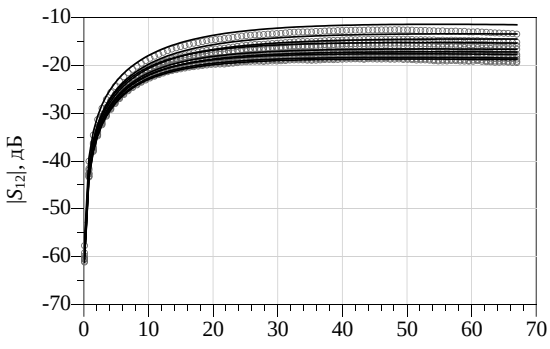
а



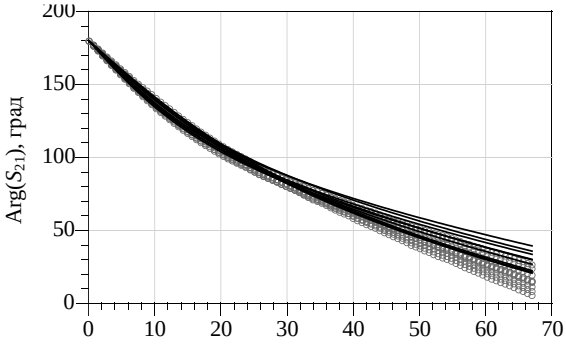
б



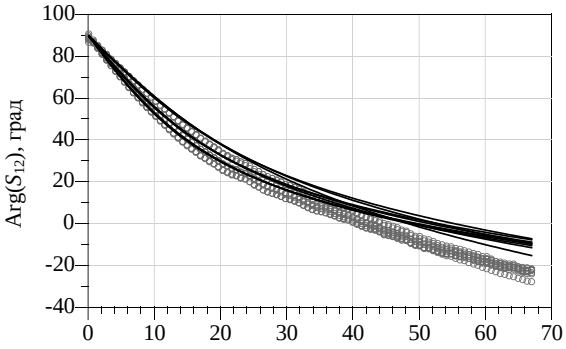
в



г



д



е

Рис. 8. Сравнение измеренных (точечные линии) и рассчитанных (сплошные линии) *S*-параметров транзистора с периферией затвора 4×35 мкм в диапазоне частот от 0,1 до 67 ГГц при напряжениях V_{ds} = (2; 3; 4) В и V_{gs} = (–0,8; –0,6; – 0,4) В

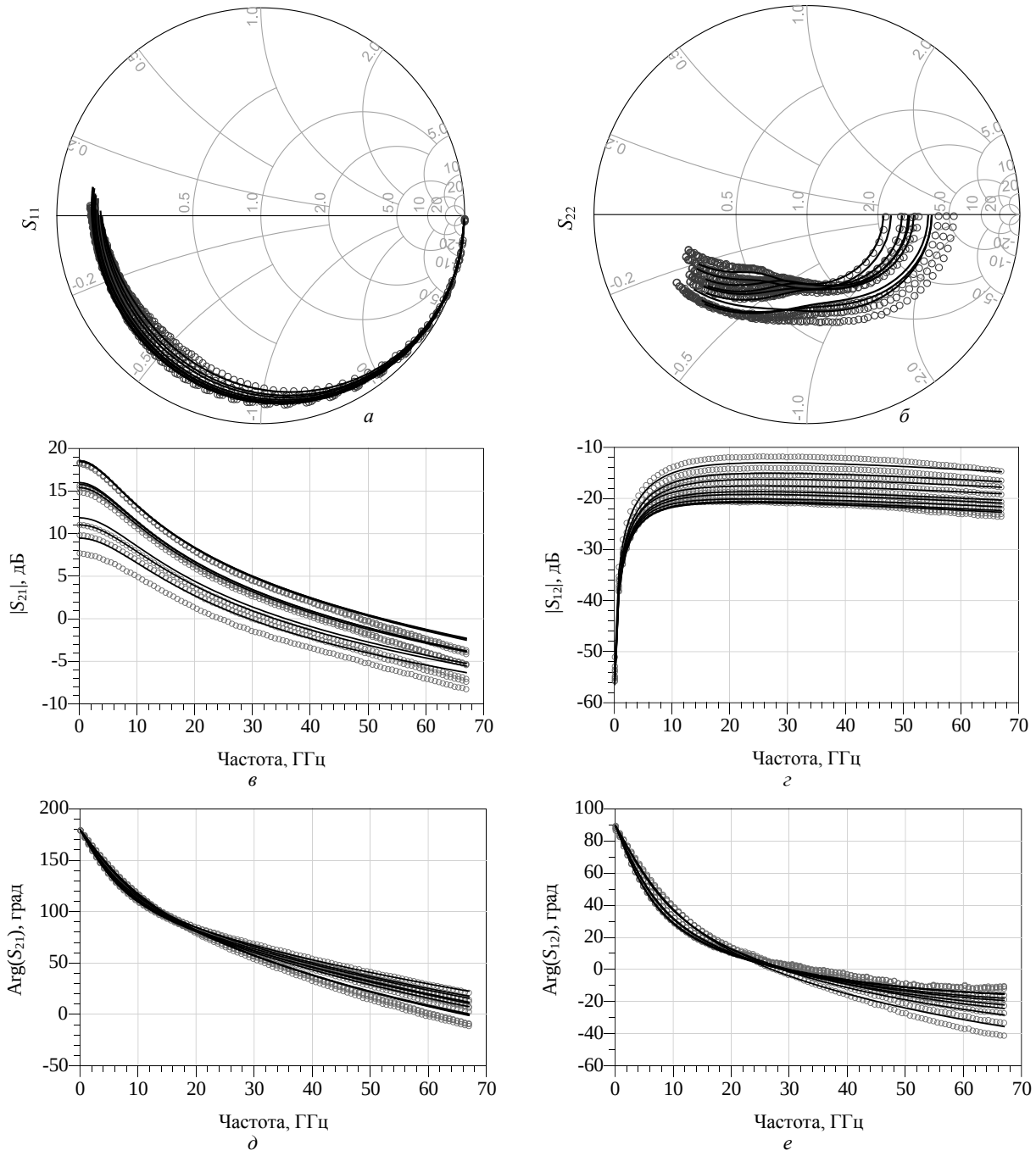


Рис. 9. Сравнение измеренных (точечные линии) и рассчитанных (сплошные линии) *S*-параметров транзистора с периферией затвора 8×35 мкм в диапазоне частот от 0,1 до 67 ГГц при напряжениях V_{ds} = (2; 3; 4) В и V_{gs} = (–0,8; –0,6; – 0,4) В

Снижение точности масштабируемой линейной модели наблюдается при переходе к меньшим периферия затвора, это может быть вызвано несколькими факторами: технологический разброс измеренных образцов транзисторов, неопределенности при проведении процедуры деэмбеддинга, использование традиционных аппроксимирующих функций.

Дальнейшие исследования в рамках настоящей тематики целесообразно вести в следующих направлениях: повышение точности масштабирования на меньших периферия затвора; валидация модели в усилительных устройствах; использование результатов для построения более сложных типов моделей, таких как шумовые и нелинейные.

Работа подготовлена в рамках реализации программы ЛИЦ «Доверенные сенсорные системы» (Договор № 009/20 от 10.04.2020) при финансовой поддержке Минкомсвязи России и АО «РВК». Идентификатор соглашения о предоставлении субсидии – 0000000007119P190002.

Литература

1. Sensing and Communication Integrated System for Autonomous Driving Vehicles / Q. Zhang, H. Sun, Zh. Wei, Zh. Feng // IEEE INFOCOM 2020 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, 6–9 July 2020. – IEEE, 2020. – P. 1278–1279.

2. Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research / C. De Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang, M. Liyanage // IEEE Open Journal of the Communications Society. – 2021. – Vol. 2. – P. 836–886.

3. Terahertz band communication systems: Challenges, novelties and standardization efforts / K. Tekbıyık, A.R. Ekti, G.K. Kurt, A. Görçin // Physical Communication. – 2019. – Vol. 35. – P. 100700.

4. Abdel Hakeem S.A. Security Requirements and Challenges of 6G Technologies and Applications / S.A. Abdel Hakeem, H.H. Hussein, H. Kim // Sensors. – 2022. – Vol. 22, No. 5. – P. 1969.

5. Implementation Challenges and Opportunities in Beyond-5G and 6G Communication / U. Gustavsson, P. Frenger, C. Fager, T. Eriksson, H. Zirath, F. Dielacher, … N. Carvalho // IEEE Journal of Microwaves. – 2021. – Vol. 1, No. 1. – P. 86–100.

6. Marsh S. Practical MMIC Design. – Artech House, 2006. – P. 376.

7. Golio M. RF and Microwave Passive and Active Technologies / M. Golio, J. Golio. – Boca Raton: CRC Press, 2007. – P. 736.

8. Robertson I.D. RFIC and MMIC Design and Technology / I.D. Robertson, S. Lucyszyn. – London, UK: The Institution of Electrical Engineers, 2001. – 555 p. – P. 125–181. DOI: 10.1049/PBCS013E

9. Development of a 0.15 μm GaAs pHEMT Process Design Kit for Low-Noise Applications / I.M. Dobush, I.S. Vasil'evskii, D.D. Zykov, D.S. Bragin, A.S. Salnikov, A.A. Popov, A.A. Gorelov, N.I. Kargin // Electronics (Basel). – 2021. – Vol. 10, No. 22. – P. 2775.

10. A new extrinsic equivalent circuit of HEMT's including noise for millimeter-wave circuit design / G. Dambrine, J.-M. Belquin, F. Danneville, A. Cappy // IEEE Transactions on Microwave Theory and Techniques. – 1998. – Vol. 46, No. 9 – P. 1231–1236.

11. Berroth M. Broad-band determination of the FET small-signal equivalent circuit / M. Berroth, R. Bosch // IEEE Transactions on Microwave Theory and Techniques. – IEEE, 1990. – Vol. 38, No. 7 – P. 891–895.

12. Luo L. Small-signal modeling and parameter extraction method for a multigate GaAs pHEMT switch / L. Luo, J. Liu, G. Wang, Y. Wu // Journal of Semiconductors. – 2020. – Vol. 41, No. 3. – P. 032102.

13. Caddemi A. Equivalent-circuit-based modeling of the scattering and noise parameters for multi-finger GaAs pHEMTs / A. Caddemi, E. Cardillo, G. Crupi // International Journal of Numerical Modelling: Electronic Networks, Devices and Fields. – 2019. – January. – P. e2587.

14. Angelov I. Extensions of the Chalmers nonlinear HEMT and MESFET model / I. Angelov, L. Bengtsson, M. Garcia // IEEE Transactions on Microwave Theory and Techniques. – 1996. – Vol. 44, No. 10. – P. 1664–1674.

15. ASM-HEMT: Compact model for GaN HEMTs / A. Dasgupta, S. Ghosh, Y.S. Chauhan, S. Khandelwal // 2015 IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC). – IEEE. – 2015. – No. 4. – P. 495–498.

16. A combined technique for amplifier oriented small- signal noise model extraction / A.A. Popov, D.V. Bilevich, A.S. Salnikov, I.M. Dobush, A.E. Goryainov, A.A. Kalentyev, A.A. Metel // International Journal of RF and Microwave Computer- Aided Engineering. – 2020. – Vol. 30, No. 9. – P. e22273.

17. Automatic golden device selection and measurement smoothing algorithms for microwave transistor small-signal noise modeling / A.S. Salnikov, I.M. Dobush, A.A. Popov, D.V. Bilevich, A.E. Goryainov, A.A. Kalentyev, A.A. Metel // International Journal of Microwave and Wireless Technologies. – 2022. – P. 1–12.

Добуш Игорь Мирославович
Канд. техн. наук, инженер ООО «50ом Тех.»,
с.н.с. лаб. «50ohm Lab», каф. КСУП ТУСУРа
Красноармейская ул., 147, г. Томск, Россия, 634045
Тел.: +7-923-402-92-86
Эл. почта: igor.dobush@50ohm.tech

Дудинов Константин Владимирович
Зам. нач. научно-производственного комплекса
АО «НПП Исток им. Шокина»
Вокзальная ул., 2а, г. Фрязино, Московская обл.,
Россия, 141190
Тел.: +7 (495-4) 65-86-93
Эл. почта: kvdudinov@istokmw.ru

Зыков Дмитрий Дмитриевич
Канд. техн. наук, доцент, технический директор
ООО «Центр проектирования и технологий полупроводниковых изделий», зав. базовой каф. микроэлектроники, информационных технологий и управляющих систем (МИТУС) ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 70-15-29
Эл. почта: Dmitry.Zykov@tusur.ru

Сальников Андрей Сергеевич
Канд. техн. наук, вед. н.с. ООО «50ом Тех.»,
зав. лаб. «50ohm Lab», каф. КСУП ТУСУРа
Красноармейская ул., 147, г. Томск, Россия, 634045
Тел.: +7-913-886-44-65
Эл. почта: andrei.salnikov@50ohm.tech

Попов Артем Александрович
Науч. сотр. ООО «50ом Тех.», каф. КСУП ТУСУРа,
м.н.с. лаб. «50ohm Lab»
Красноармейская ул., 147, г. Томск, Россия, 634045
Тел.: +7-913-880-78-12
Эл. почта: artem.popov@50ohm.tech

Емельянов Артем Михайлович
Вед. инженер-технолог АО «НПП Исток им. Шокина»
Вокзальная ул., 2а, г. Фрязино, Московская обл.,
Россия, 141190
Тел.: +7 (495-4) 65-86-93
Эл. почта: amemeljanov@istokmw.ru

Брагин Дмитрий Сергеевич
Директор Проектного офиса ЦК НТИ «Технологии доверенного взаимодействия» ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-952-151-65-48
Эл. почта: bds@csp.tusur.ru

Хайров Дамир Рашидович
Директор по развитию ООО «Центр проектирования и технологий полупроводниковых изделий»
Кулакова ул., 20/1, г. Москва, Россия, 123592
Тел.: +7-960-372-76-73
Эл. почта: d.hairov@i-pdk.ru

Dobush I.M., Dudinov K.V., Zykov D.D., Sal'nikov A.S., Popov A.A., Emelyanov A.M., Bragin D.S., Khayrov D.R.

Development of a scalable small-signal 0.1 μm GaAs-pHEMT-model for amplifier applications

This work deals with the development of a 0.1-μm GaAs-pHEMT-model for use in EDA applications. The model is constructed using a reference transistor with a total gate width of 6×35 μm, which showed good accuracy under different DC operation modes in a wide frequency range. The developed model can be used to speed up and reduce the cost of the monolithic microwave integrated circuit amplifiers design in which the pHEMT transistor is the basic active element. In further studies the obtained model will be extended to develop more complex types of models, such as noise and nonlinear ones.

Keywords: microwave transistor, microwave transistor model, monolithic microwave integrated circuit, extraction of model parameters, equivalent circuit, small-signal model, linear parameters, pHEMT, GaAs.

DOI: 10.21293/1818-0442-2022-25-4-37-47

References

1. Zhang Q., Sun H., Wei Zh., Feng Zh. Sensing and communication integrated system for autonomous driving vehicles. *Proceedings of IEEE INFOCOM 2020 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Toronto, ON, Canada, 6–9 July 2020, pp. 1278–1279.

2. De Alwis C., Kalla A., Pham Q.-V., Kumar P., Dev K., Hwang W.-J., Liyanage M. Survey on 6G frontiers: trends, applications, requirements, technologies and future research. *IEEE Open Journal of the Communications Society*, 2021, 2, pp. 836–886.

3. Tekbıyık K., Ekti A.R., Kurt G.K., Görçin A. Terahertz band communication systems: challenges, novelties and standardization efforts. *Physics Communications.*, 2019, 35, p. 100700.

4. Abdel Hakeem S.A., Hussein H.H., Kim H. Security requirements and challenges of 6G technologies and applications. *Sensors*, 2022, 22, p. 1969.

5. Gustavsson U., Frenger P., Fager C., Eriksson T., Zirath H., Dielacher F., ... Carvalho N. Implementation challenges and opportunities in beyond-5G and 6G communication. *IEEE Journal of Microwaves*, 2021, 1, pp. 86–100.

6. Marsh S. *Practical MMIC Design*; Artech House, Inc.: Norwood, MA, 2006. 376 p.

7. Golio M., Golio J. *RF and Microwave Passive and Active Technologies*. Boca Raton, CRC Press, 2007. 736 p.

8. Robertson I.D., Lucyszyn S. *RFIC and MMIC Design and Technology*. London, UK, The Institution of Electrical Engineers, 2001, 555 p. pp. 125–181. DOI: 10.1049/PBCS013E.

9. Dobush, I.M.; Vasil'evskii, I.S.; Zykov, D.D.; Bragin, D.S.; Salnikov, A.S.; Popov, A.A.; ... Kargin, N.I. Development of a 0.15 μm GaAs-pHEMT-process design kit for low-noise applications. *Electronics* (Basel) 2021, 10, p. 2775.

10. Dambrine G.. Belquin J.-M., Danneville F.. Cappy A. A new extrinsic equivalent circuit of HEMT's including noise for millimeter-wave circuit design. *IEEE Transactions on Microwave Theory and Technique*, 1998, 46, pp. 1231–1236.

11. Berroth M., Bosch R. Broad-band determination of the FET small-signal equivalent circuit. *IEEE Transactions on Microwave Theory and Technique*, 1990, 38, pp. 891–895.

12. Luo L., Liu J., Wang G., Wu Y. Small-signal modeling and parameter extraction method for a multigate GaAs-pHEMT switch. *Journal of Semiconductors*, 2020, 41, p. 032102.

13. Caddemi A., Cardillo E., Crupi G. Equivalent-circuit-based modeling of the scattering and noise parameters for mul-ti-finger GaAs-pHEMTs. *International Journal of Numerical Modelling: Electronic Networks, Devices and Field*, 2020, 33, e2587.

14. Angelov I., Bengtsson L., Garcia M. Extensions of the Chalmers nonlinear HEMT and MESFET model. *IEEE Transactions on Microwave Theory and Techniques*, 1996, 44, pp. 1664–1674.

15. Dasgupta A., Ghosh S., Chauhan Y.S., Khandelwal S. ASM-HEMT: Compact model for GaN HEMTs, *Proceedings of 2015 IEEE International Conference on Electron Devices and Solid-State Circuits* (EDSSC), Singapore, 1–4 June 2015, pp. 495–498.

16. Popov A.A., Bilevich D.V., Salnikov A.S., Dobush I.M., Goryainov A.E.; Kalentyev A.A.; Metel A.A. A combined technique for amplifier oriented small- signal noise model extraction. *International Journal of RF and Microwave Computer-Aided Engineering*, 2020, vol. 30, no. 9, pp. e22273.

17. Salnikov A.S., Dobush I.M., Popov A.A., Bilevich D.V., Goryainov A.E., Kalentyev A.A., Metel A.A. Automatic golden device selection and measurement smoothing algorithms for microwave transistor small-signal noise modelin. *International Journal of Microwave and Wireless Technologies*, 2022, pp. 1–12.

Igor M. Dobush
Candidate of Science in Engineering, Engineer,
50ohm Technologies LLC, Senior Researcher, Department of Computer Control Systems and Design, Research Laboratory «50ohm Lab», Tomsk State University of Control Systems and Radioelectronics (TUSUR)
147, Krasnoarmeiskaya str., Tomsk, Russia, 634045
ORCID: 0000-0002-3626-1419
Phone: +7-923-402-92-86
Email: igor.dobush@50ohm.tech

Konstantin V. Dudinov
Candidate of Science in Engineering, Deputy-Head of Scientific-Production Complex, Research and Production Corporation Istok JSC
2A, Vokzalnaya str., Fryazino, Moscow Region, Russia, 141190
Phone: +7 (495-4) 65-86-93
Email: kvdudinov@istokmw.ru

Dmitry D. Zykov
Candidate of Science in Engineering, Associate Professor, Technical Director, Semiconductor Design and Technology Center LLC, Head of Chair «Microelectronics, Informational Technologies and Control Systems», TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0002-9587-4629
Phone: +7 (382-2) 70-15-29
Email: Dmitry.Zykov@tusur.ru

Andrei S. Salnikov
Candidate of Science in Engineering, Lead Researcher, 50ohm Technologies LLC, Head of Research Laboratory «50ohm Lab», Department of Computer Control Systems and Design, TUSUR
147, Krasnoarmeiskaya str., Tomsk, Russia, 634045
ORCID: 0000-0002-5827-9556
Phone: +7-913-886-44-65
Email: andrei.salnikov@50ohm.tech

Artem A. Popov
Researcher, 50ohm Technologies LLC, Researcher,
Department of Computer Control Systems and Design,
Research Laboratory «50ohm Lab», TUSUR
147, Krasnoarmeiskaya str., Tomsk, Russia, 634045
ORCID: 0000-0001-6010-4459
Phone: +7-913-880-78-12
Email: artem.popov@50ohm.tech

Artem M. Emelyanov
Leading Process Engineer, Research and Production
Corporation Istok JSC
2A, Vokzalnaya str., Fryazino, Moscow Region,
Russia, 141190
Phone: +7 (495-4) 65-86-93
Email: amemeljanov@istokmw.ru

Dmitry S. Bragin
Director of the Project Office of the Central Committee
of the NTI «Technologies of Trusted Interaction» TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0002-0875-3301
Phone: +7-952-151-65-48
Email: bds@csp.tusur.ru

Damir R. Khayrov
Director of Development, Semiconductor Design
and Technology Center LLC
Kulakov str., 20/1, Moscow, Russia, 123592
Phone: +7-960-372-76-73
Email: d.hairov@i-pdk.ru

УДК 621.396.1

К.Д. Зайков, А.С. Аникин, Ф.Н. Захаров, К.А. Ярков, В.И. Вебер

Методика измерения матрицы рассеяния многопортового устройства двухпортовым векторным анализатором цепей

При проектировании приёмопередающих трактов возникает задача моделирования ожидаемых характеристик отдельных составных частей проектируемых трактов. Наиболее универсальной и удобной для описания СВЧ-устройств является матрица рассеяния. Использование двухпортовых и четырёхпортовых векторных анализаторов цепей позволяет измерить параметры большинства разрабатываемых СВЧ-устройств (делители, фильтры, усилители и т.д.). Часто перед инженером стоит задача измерить двухпортовым векторным анализатором цепей параметры многопортового устройства (портов больше 4) для последующего расчёта матрицы рассеяния каскадного соединения смежных аналоговых блоков. Целью данной статьи является представление методики проведения измерения матрицы рассеяния многопортовых устройств двухпортовым векторным анализатором цепей с последующим каскадированием для получения матрицы рассеяния многоканального итогового устройства (многоканальный радиотракт). Достижение поставленной цели позволяет обеспечить необходимый базис для синтеза отечественного программного обеспечения для проектирования СВЧ-трактов с точки зрения системного анализа.

Ключевые слова: методика измерения *S*-параметров, измерение *S*-параметров, матрица рассеяния, векторный анализатор цепей, каскадирование СВЧ-устройств.
DOI: 10.21293/1818-0442-2022-25-4-48-53

При проектировании приёмопередающих трактов возникает задача моделирования ожидаемых характеристик при заданных технических требованиях к отдельным составным частям тракта. Под составными частями понимаем блоки усиления, фильтрации, преобразования частоты и т.д. Каждый блок, в основном, состоит из двухпортовых устройств (например, усилитель, фильтр, фазовращатель и т.д.), реже трёхпортовых и четырёхпортовых устройств (например, смеситель и направленный ответвитель) [1, 2]. Устройства с большим количеством портов используются крайне редко, как правило, это ключи, переключатели, делители мощности. Для описания таких устройств в современных инженерных расчётах, САПР и технической документации принято использовать матрицы параметров.

Наиболее универсальной и удобной для описания СВЧ-устройств является матрица рассеяния (**S**) [3]. Данная матрица связывает входные и выходные порты устройства, получается путем описания реакции устройства на единичные воздействия в виде падающих волн. При моделировании приемопередающих трактов необходимо знать результирующую матрицу рассеяния во всем диапазоне интересующих частот, что позволяет оценить взаимное влияние элементов тракта, неравномерность частотной характеристики в полосе пропускания и т.д.

Большинство алгоритмов было разработано в XX в., в настоящее время в журналах публикуют модифицированные методы [4, 5], которые в ряде задач уменьшают вычислительную сложность.

В современных САПР реализован расчёт матриц рассеяния каскадного соединения смежных аналоговых блоков. Однако в справочной документации к САПР отсутствуют сведения о методике расчета либо косвенно отмечается подход к расчёту результирующей матриц рассеяния [6–8]. Среди отечественных САПР, в которых был реализован расчёт матриц рассеяния каскадного соединения смежных аналоговых блоков, методика расчета не найдена.

Как правило, многоканальные радиочастотные тракты могут быть декомпозированы на простые составные части/блоки. Данные блоки изготавливаются из простых СВЧ-устройств – усилителей, фильтров, аттенюаторов, смесителей, характеристики которых, как правило, могут быть измерены двухпортовым векторным анализатором цепей (для трёх- и четырёхпортовых устройств используют четырёхпортовые векторные анализаторы цепей).

Использование двухпортовых и четырёхпортовых векторных анализаторов цепей позволяет измерить характеристики большинства разрабатываемых СВЧ-устройств. Такие векторные анализаторы цепей находятся в свободной продаже и производятся серийно [9, 10].

Для измерения характеристик устройств с большим количеством портов изготавливаются штучные векторные анализаторы цепей с произвольным чётным количеством портов. Данные приборы изготавливаются на заказ.

В связи с этим перед инженером может возникнуть задача измерить двухпортовым векторным анализатором цепей многопортовое устройство или многопортовый блок для последующего расчёта матрицы рассеяния каскадного соединения смежных аналоговых блоков.

Целью данной статьи является изложение методики проведения измерения матрицы рассеяния многопортового устройства двухпортовым векторным анализатором цепей с последующим каскадированием для получения матрицы рассеяния многоканального устройства (многоканальный радиотракт).

Постановка задачи

Наиболее распространенный метод каскадирования рассматриваемый в литературе метод блочных **S**-матриц. Для описания данного метода рассмотрим обобщенную схему каскадного соединения двух многополюсников (рис. 1).

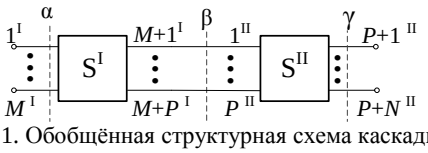


Рис. 1. Обобщённая структурная схема каскадного соединения двух многополюсников

Каждый из многополюсников имеет группу входов, не участвующих в соединении (у первого многополюсника число таких входов равно *M*, у второго *N*), и группу соединяемых входов, число которых равно *P* (см. рис. 1). Такое представление матриц называется блочным [3]. Для определения результирующей матрицы рассеяния соединения многополюсников необходимо применять определенную нумерацию входов. У многополюсника I нумеруются все свободные входы (группа входов α), а затем все выходы этого многополюсника, участвующие в соединении (группа входов β). У многополюсника II нумеруются все входы, участвующих в соединении (аналогично порядку выходных портов многополюсника I), а затем все свободные выходные порты (группа входов γ).

Используя указанную нумерацию, матрицы $\mathbf{S}^{\mathrm{I}}$ н $\mathbf{S}^{\mathrm{II}}$ можно разделить на четыре блока:

$$\mathbf{S}^{\mathrm{I}} = \begin{bmatrix} \mathbf{S}_{\alpha\alpha} & \mathbf{S}_{\alpha\beta} \\ \mathbf{S}_{\beta\alpha} & \mathbf{S}^{I}_{\beta\beta} \end{bmatrix} \quad \mathbf{S}^{\mathrm{II}} = \begin{bmatrix} \mathbf{S}^{\mathrm{II}}_{\beta\beta} & \mathbf{S}_{\beta\gamma} \\ \mathbf{S}_{\gamma\beta} & \mathbf{S}_{\gamma\gamma} \end{bmatrix}, \qquad (1)$$

где $\mathbf{S}_{\alpha\alpha}$ и $\mathbf{S}^{\mathrm{II}}{}_{\beta\beta}$ – блочные матрицы, описывающие развязку входных портов первого и второго многополюсника соответственно; $\mathbf{S}_{\beta\alpha}$ и $\mathbf{S}_{\gamma\beta}$ – блочные матрицы, описывающие прямую передачу (от входа к выходу) портов первого и второго многополюсника соответственно; $\mathbf{S}_{\alpha\beta}$ и $\mathbf{S}_{\beta\gamma}$ – блочные матрицы, описывающие обратную передачу (от выхода к входу) портов первого и второго многополюсников соответственно; $\mathbf{S}^{\mathrm{I}}{}_{\beta\beta}$ и $\mathbf{S}_{\gamma\gamma}$ – блочные матрицы, описывающие развязку выходных портов первого и второго многополюсников соответственно.

Результирующая блочная матрица рассеяния представлена в виде

$$\mathbf{S}^{\Sigma} = \begin{bmatrix} \mathbf{S}^{\Sigma}_{\alpha\alpha} & \mathbf{S}^{\Sigma}_{\alpha\gamma} \\ \mathbf{S}^{\Sigma}_{\gamma\alpha} & \mathbf{S}^{\Sigma}_{\gamma\gamma} \end{bmatrix},$$

где блочные матрицы будут вычисляться по формулам [3]:

$$\mathbf{S}^{\Sigma}_{\alpha\alpha} = \mathbf{S}_{\alpha\alpha} + \mathbf{S}_{\alpha\beta}\left(\mathbf{E} - \mathbf{S}^{II}_{\beta\beta}\mathbf{S}^{I}_{\beta\beta}\right)^{-1}\mathbf{S}^{II}_{\beta\beta}\mathbf{S}_{\beta\alpha},$$

$$\mathbf{S}^{\Sigma}_{\alpha\gamma} = \mathbf{S}_{\alpha\beta}\left(\mathbf{E} - \mathbf{S}^{II}_{\beta\beta}\mathbf{S}^{I}_{\beta\beta}\right)^{-1}\mathbf{S}_{\beta\gamma},$$

$$\mathbf{S}^{\Sigma}_{\gamma\alpha} = \mathbf{S}_{\gamma\beta}\left(\mathbf{E} - \mathbf{S}^{I}_{\beta\beta}\mathbf{S}^{II}_{\beta\beta}\right)^{-1}\mathbf{S}_{\beta\alpha},$$

$$\mathbf{S}^{\Sigma}_{\gamma\gamma} = \mathbf{S}_{\gamma\gamma} + \mathbf{S}_{\gamma\beta}\left(\mathbf{E} - \mathbf{S}^{I}_{\beta\beta}\mathbf{S}^{II}_{\beta\beta}\right)^{-1}\mathbf{S}^{I}_{\beta\beta}\mathbf{S}_{\beta\gamma}, \qquad (2)$$

где **E** – единичная матрица.

Как видно из формулы (1), рис. 1 и описания представления блочных матриц, для того чтобы корректно использовать формулу (2) для получения матрицы рассеяния двух смежно соединенных СВЧ-устройств, необходимо использовать описанную выше нумерацию портов [3].

Обзор литературы и документации к векторным анализаторам цепей показал, что отсутствует описание методики измерения матрицы рассеяния многопортовых устройств двухпортовым векторным анализатором цепей с последующим каскадированием [11–13]. Исключение составляет методика объединения измерений, реализованная в зарубежном коммерческом приложении AWR Design Environment [8]. Данное приложение позволяет сформировать матрицу рассеяния многопортового устройства по измеренным матрицам рассеяния отдельных пар портов. В качестве недостатка данного приложения можно выделить отсутствие описания методики измерения, без которой инженер может пропустить важные *S*-параметры или дублировать ранее проведённые измерения. А также к недостаткам стоит отнести отсутствие описания алгоритма каскадирования смежных СВЧ-устройств, что затрудняет анализ полученных результатов с целью определения их достоверности. Среди отечественных САПР подобных приложений не существует.

Методика измерения матрицы рассеяния многопортового устройства

Порядок измерения матрицы рассеяния аналоговых трактов рассмотрим на следующем примере.

Предположим, измеряемое устройство имеет *M* входных портов и *P* выходных портов. Общее количество портов аналогового тракта составляет *N* = *M* + *P*. Нумерация входных и выходных портов должна быть сквозной. Таким образом, аналоговый тракт представляет собой *N*-портовое устройство (рис. 2).

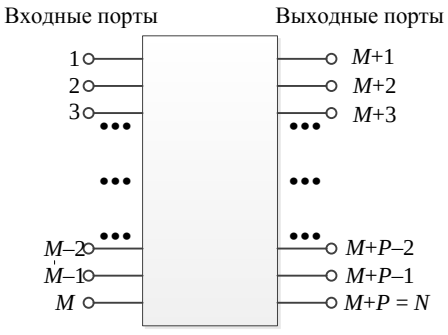


Рис. 2. Пример устройства для измерения матрицы рассеяния

Перед проведением измерений с помощью двухпортового векторного анализатора цепей следует выполнить его калибровку. Порядок измерения матрицы рассеяния для двухпортого векторного анализатора цепей следующий:

1. Первый порт векторного анализатора цепей (далее порт I) подключить к первому порту измеряемого устройства, а второй порт анализатора (далее порт II) – ко второму порту этого же устройства. Остальные порты устройства подключить к согласованной нагрузке. После подключения указанных портов выполнить измерения матрицы рассеяния в интересующем диапазоне частот. Файл с результатами измерений матрицы рассеяния сохранить с именем «1_*.s2p». Примечание: Символом «*» обозначено имя файла. Файлы формата *.s2p должны быть сохранены в отдельную папку для конкретного устройства.

2. Второй порт устройства отключить от порта II векторного анализатора цепей. Затем порт II подключить к третьему порту устройства. Остальные порты устройства нагрузить согласованной нагрузкой. Провести измерения, файл сохранить с именем «2_*.s2p».

3. Этап 2 повторить до N-го порта устройства, включительно.

4. Порт I подключить ко второму порту устройства, а порт II подключить к третьему порту устройства. Остальные порты устройства нагрузить согласованной нагрузкой. После подключения указанных портов выполнить измерения матрицы рассеяния в интересующем диапазоне частот. Файл с результатами измерений матрицы рассеяния сохранить с именем «N_*.s2p».

5. Повторить п. 3 с сохранением порядка нумерации файлов формата *.s2p.

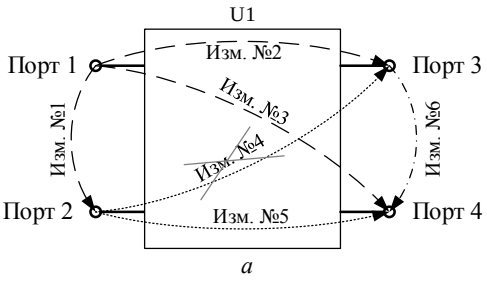
6. Повторить пп. 4, 5 для последовательности подключений порта I векторного анализатора цепей с третьего до N–1 порта измеряемого устройства (аналогового тракта).

Общее количество файлов формата *.s2p с результатами измерений должно быть равно $K = 0{,}5 \cdot N \cdot (N - 1)$.

Для того чтобы рассчитать матрицу рассеяния каскадно соединенных СВЧ-устройств, при условии, что измерение многопортовых устройств было произведено по описанной выше методике, была разработана и зарегистрирована программа ЭВМ [14].

Данная программа предназначена для считывания файлов *S*-параметров в формате Touchstone, измеренных двухпортовым векторным анализатором цепей, и расчёта результирующей матрицы рассеяния каскадного соединения СВЧ-устройств по алгоритму, описанному в [3].

В программе реализована возможность пропускать измерения. Инженер вправе решить, какие измерения можно пропустить (например, из-за большой развязки портов), при пропуске измерения должен быть пропущен соответствующий порядковый номер наименования файла. Пример пропуска и наименования файлов в папке представлен на рис. 3. На рисунке показана ситуация, когда пропущено измерение № 4 в связи с пренебрежимо малым значением модуля *S*-параметра между 2-м и 3-м портами. Измерения в папке должны быть пронумерованы так, как приведено на рис. 3, *б*.



а

Имена файлов	№ измерения
1_U1.s2p	1
2_U1.s2p	2
3_U1.s2p	3
4_U1.s2p	4
5_U1.s2p	5
6_U1.s2p	6

б

Рис. 3. Пример пропуска измерения четвертого измерения: *а* – схема, *б* – наименования файлов измерений

Верификация методики

Для верификации методики были проведены измерения *S*-параметров двух делителей мощности ДМС2А-26-13р [15] и их каскадного соединения. Измерения производились на векторном анализаторе цепей «Planar» серии «Кобальт С1220» с предварительной калибровкой. Расчет проводился в программе, изложенной в [14].

Собранная схема из делителей представлена на рис. 4. Вычисленные значения S-параметров сопоставлялись с измеренной матрицей рассеяния итогового устройства по формуле

$$\Delta S_{i,j} = \left| S_{i,j}[\text{дБ}] - S^{*}_{i,j}[\text{дБ}] \right|, \qquad (3)$$

где $S_{i,j}$ – рассчитанное значение *S*-параметров итогового устройства между *j* и *i* портами; $S^{*}_{i,j}$ – измеренное значение *S*-параметров итогового устройства между *j* и *i* портами.

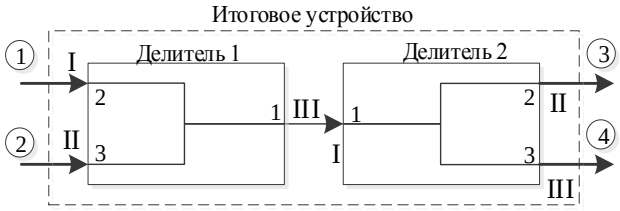


Рис. 4. Исследуемая схема

На рис. 4 арабские цифры без круга – нумерация портов устройства согласно Datasheet, римские цифры – порядок нумерации портов при измерении и расчёте, арабские цифры в круге – нумерации портов итогового устройства.

Усреднённые значения, вычисленные по формуле (3), представлены в таблице. Для примера на рис. 5 приведены сравнения вычисленных и измеренных значений *S*-параметров.

Усреднённые значения абсолютной разницы измеренной и вычисленной матриц рассеяния устройства

$\Delta S_{i,j}$, дБ		Номер порта			
		1	2	3	4
Номер порта	1	0,209	0,198	0,220	0,151
	2	0,199	0,191	0,088	0,127
	3	0,227	0,079	0,193	0,198
	4	0,155	0,123	0,199	0,272

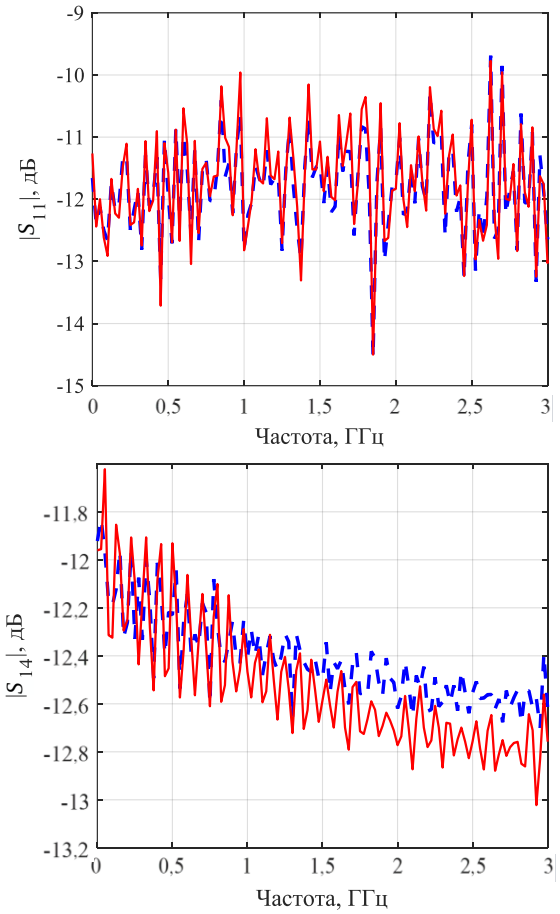


Рис. 5. Сравнение измеренных и рассчитанных *S*-параметров схемы, представленной на рис. 3 (сплошная линия – расчётные значения, пунктирная – измеренные значения)

Заключение

По данным из таблицы и рис. 5 видно, что результат вычисления итоговой матрицы совпадает с измеренными значениями с незначительной расходимостью, вызванной, главным образом, фазовой нестабильностью СВЧ-кабелей.

Достижение поставленной цели позволяет обеспечить необходимый базис для синтеза отечественного программного обеспечения для проектирования СВЧ-трактов с точки зрения системного анализа.

Описанная методика применима и для четырехпортового векторного анализатора цепей с учетом того, что вместо порта II используется группа портов II–IV векторного анализатора цепей.

Работа выполнена в рамках реализации государственного проекта Минобрнауки «Программа стратегического академического лидерства Приоритет-2030».

Литература

1. Mini Circuits – мировой лидер в области радиочастотных и микроволновых компонент [Электронный ресурс]. – Режим доступа: https://www.minicircuits.com/, свободный (дата обращения: 20.09.2022).

2. Analog Devices [Электронный ресурс]. – Режим доступа: https://www.analog.com/ru/index.html (дата обращения: 20.09.2022).

3. Сазонов Д.М. Устройства СВЧ: учеб. пособие / под ред. Д.М. Сазонова. – М.: Высш. школа, 1981. – 295 с.

4. A New Method to Calculate Cascaded S-Parameters. 2018 IEEE 27th Conference on Electrical Performance of Electronic Packaging and System [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/8534261 (дата обращения: 20.09.2022).

5. Extended S-parameters for imperfect test ports / J. Hoffmann, M. Wollensack, J. Ruefenacht, M. Zeier // Metrologia. – 2015. – Vol. 52, No. 1. – P. 121–129. DOI: 10.1088/0026-1394/52/1/121

6. MathWorks – создатели MATLAB и Simulink. Объединение S-параметров для формирования каскадной сети [Электронный ресурс]. – Режим доступа: https://se.mathworks.com/help/rf/ref/cascadesparams.html, свободный (дата обращения: 20.09.2022).

7. Qucs. Work book // QUCS Электронный ресурс]. – Режим доступа: https://qucs.sourceforge.net/docs/workbook_ru.pdf, свободный (дата обращения: 21.09.2022).

8. Combine S-Parameters // kb.awr.com [Электронный ресурс]. – Режим доступа: https://kb.awr.com/display/awrutil/Combine+S-Parameters, свободный (дата обращения: 21.09.2022).

9. Анализаторы цепей векторные // PLANAR [Электронный ресурс]. – Режим доступа: https://planarchel.ru/catalog/analizatory_tsepey_vektornye/, свободный (дата обращения: 21.09.2022).

10. Векторные анализаторы цепей // chipdip [Электронный ресурс]. – Режим доступа: https://www.chipdip.ru/search?searchtext=векторные+анализаторы+цепей, свободный (дата обращения: 21.09.2022).

11. Анализатор цепей векторный. Руководство по эксплуатации. Технические характеристики. РЭ 6687-143-21477812–2018. Версия 22.1 // PLANAR [Электронный ресурс]. – Режим доступа: https://www.planarchel.ru/uploadmedialibrary/00b/asmyfwgydtzo5ao4l0uql7l1c2m6nuih/OM_Sseries_Part1_ver22.3.pdf, свободный (дата обращения: 21.09.2022).

12. Хибель М. Основы векторного анализа цепей. – М.: МЭИ, 2018. – 500 с.

13. S-Parameters Techniques for faster, More Accurate Network Design. Agilent EEsof EDA [Электронный ресурс]. – Режим доступа: https://www.phys.hawaii.edu/~idlab/taskAndSchedule/5989-9273EN.pdf, свободный (дата обращения: 21.09.2022).

14. Свидетельство о государственной регистрации программы для ЭВМ № 2021669469 РФ. Программа расчёта матрицы рассеяния каскадного соединения СВЧ-устройств с произвольным количеством портов / К.Д. Зайков, А.С. Аникин, Ф.Н. Захаров; заявитель ФГБОУ ВО «Томский гос. ун-т систем управления и радиоэлектроники». – № 2021668682; заявл. 24.11.2021; опубл. 29.11.2021 [Электронный ресурс] – Режим доступа: https://fips.ru/publication-web/publications/document?type=doc&tab=PrEVM&id=D1B2AF4D-3F87-4A8F-9354-A18A360BD085, свободный (дата обращения: 21.09.2022).

15. Делители мощности – элементы СВЧ-тракта – Микран // АО «НПФ «Микран» [Электронный ресурс]. – Режим доступа: https://www.micran.ru/productions/IIS/accessory/divider/divider/, свободный (дата обращения: 21.09.2022).

Зайков Кирилл Денисович
Аспирант каф. радиотехнических систем (РТС),
м.н.с. НИИ РТС Томского государственного ун-та систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-952-161-04-82
Эл. почта: kirill.d.zaikov@tusur.ru

Аникин Алексей Сергеевич
Канд. техн. наук, доцент каф. РТС,
с.н.с. НИИ РТС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0001-9747-3266
Тел.: +7 (382-2) 41-38-89
Эл. почта: anikinas@main.tusur.ru

Захаров Федор Николаевич
Канд. техн. наук, доцент каф. РТС,
зав. лаб. распространения радиоволн НИИ РТС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0001-7751-557X
Тел.: +7 (382-2) 41-38-89
Эл. почта: zakharovfn@main.tusur.ru

Ярков Кирилл Алексеевич
Аспирант каф. РТС, м.н.с. НИИ РТС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-38-89
Эл. почта: kirill.a.iarkov@tusur.ru

Вебер Владислав Игоревич
Аспирант каф. РТС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-38-89
Эл. почта: vladislav.i.veber@tusur.ru

Zaikov K.D., Anikin A.S., Zakharov F.N.,
Yarkov K.A., Veber V.I.

Methodology for Measuring the Scattering Matrix of a Multiport Device with a Two-Port Vector Network Analyzer

When designing transceiver paths, the problem of modeling the characteristics of individual components arises. The most universal and convenient for describing the microwave device is the scattering matrix. The use of two-port and four-port vector network analyzers allows to adjust the parameters of most of the developed microwave devices (dividers, filters, amplifiers, etc.). Often, the task is to use a two-port vector network analyzer to measure the parameters of a multi-port device (ports more than 4) to solve the problem of calculating the scattering matrix of the bone connection of adjacent industrial units. The purpose of this article is to compile a methodology for measuring the scattering of multiport devices with a two-port vector network analyzer with a sequence to obtain a measurement of a multi-channel final device (multi-channel radio path). Achieving this goal allows us to provide the necessary basis for the synthesis of domestic software used to develop microwave paths from the point of view of an overview of system analysis.

Keywords: S-parameter measurement technique, S-parameter measurement, scattering matrix, vector network analyzer, microwave device cascading.
DOI: 10.21293/1818-0442-2022-25-4-48-53

References

1. Mini Circuits – mirovoy lider v oblasti radiochastotnykh i mikrovolnovykh komponent [Mini Circuits is the world leader in RF and microwave components]. Available at: https://www.minicircuits.com, free (Accessed: September 20, 2022) (in Russ.).

2. Analog Devices. Available at: https://www.analog.com/ru/index.html, free (Accessed: September 20, 2022).

3. Sazonov D.M. Ustroystva SVCH [*Microwave Devices*]. Moscow, Higher School Publ, 1981, 295 p. (in Russ.).

4. A New Method to Calculate Cascaded S-Parameters. 2018 IEEE 27th Conference on Electrical Performance of Electronic Packaging and System. Available at: https://ieeexplore.ieee.org/document/8534261, free (Accessed: September 20, 2022).

5. Hoffmann J., Wollensack M., Ruefenacht J., Zeier M. Extended S-parameters for imperfect test ports. *Metrologia*, 2015, vol. 52, no. 1, pp. 121–129. DOI: 10.1088/0026-1394/52/1/121

6. MathWorks – Creators of MATLAB and Simulink. Combining S-parameters to form a cascade network. Available at: https://se.mathworks.com/help/rf/ref/cascadesparams.html, free (Accessed: September 20, 2022).

7. Qucs. Work book. Available at: https://qucs.sourceforge.net/docs/workbook_ru.pdf, free (Accessed: September 20, 2022) (in Russ.).

8. Combine S-Parameters. Available at: https://kb.awr.com/display/awrutil/Combine+S-Parameters, free (accessed: September 21, 2022).

9. Analizatory tsepey vektornyye [Vector circuit analyzers] Available at: https://planarchel.ru/catalog/analyzatory_tsepey_vektornye/, free (Accessed: September 21, 2022) (in Russ.).

10. Vektornyye analizatory tsepey [Vector network analyzers] Available at: https://www.chipdip.ru/search?searchtext=vector+analyzers+circuits, free (Accessed: September 21, 2022) (in Russ.).

11. Analizator tsepey vektornyy. Rukovodstvo po ekspluatatsii. Tekhnicheskiye kharakteristiki. RE 6687-143-21477812–2018. Versiya 22.1 [Vector circuit analyzer. Manual. Specifications. RE 6687-143-21477812–2018. Version 22.1] Available at: https://www.planarchel.ru/uploadmedia-library/00b/asmyfwgydtzo5ao4l0uql7l1c2m6nuih/OM_Sseries_Part1_ver22.3.pdf, free (Accessed: September 21, 2022) (in Russ.).

12. Khibel M. Osnovy vektornogo analiza tsepey [*Fundamentals of vector circuit analysis*], Moscow, MPEI, 2018, 500 p. (in Russ.).

13. S-Parameters Techniques for faster, More Accurate Network Design. Agilent EEsof EDA. Available at: https://www.phys.hawaii.edu/~idlab/taskAndSchedule/5989-9273EN.pdf, free (Accessed: September 21, 2022).

14. Zaikov K.D., Anikin A.S., Zakharov F.N. Programma rascheta matritsy rasseyaniya kaskadnogo soyedineniya SVCh-ustroystv s proizvolnym kolichestvom portov [The program for calculating the scattering matrix of a cascade connection of microwave devices with an arbitrary number of ports] Certificate of state registration of the computer program

No. 2021669469, 2021, Available at: https://fips.ru/publication-web/publications/document?type=doc&tab=PrEVM&id=D1B2AF4D-3F87-4A8F-9354-A18A360BD085, free (Accessed: September 21, 2022) (in Russ.)..

15. Deliteli moshchnosti – Elementy SVCh-trakta [Power dividers – Elements of the microwave path – JSC «Mikran»] Available at: https://www.micran.ru/productions/IIS/accessory/divider/divider/, free (Accessed: September 21, 2022) (in Russ.).

Kirill D. Zaikov
Postgraduate student, Department of Radio Engineering Systems (RES), Junior researcher of Research Institute (RI) RES, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-952-161-04-82
Email: kirill.d.zaikov@tusur.ru

Aleksei S. Anikin
Candidate of Science in Engineering, Department of RES, Senior researcher of Research Institute of Radio Engineering, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0001-9747-3266
Phone: +7 (382-2) 41-38-89
Email: anikinas@main.tusur.ru

Fedor N. Zakharov
Candidate of Science in Engineering, Assistant Professor Department of RES, Head of Radio Wave Propagation Laboratory, Research Institute of Radio Engineering TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0001-7751-557X
Phone: +7 (382-2) 41-38-89
Email: zakharovfn@main.tusur.ru

Kirill A. Yarkov
Postgraduate student, Department of RES, Junior researcher of RI RES, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: + 7 (382-2) 41-38-89
Email: kirill.a.iarkov@tusur.ru

Vladislav I. Veber
Postgraduate student Department of RES, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 41-38-89
Email: vladislav.i.veber@tusur.ru

УДК 621.391

А. Алхадж Хасан, Т.Р. Газизов

Обзор исследований по модальному резервированию

Усложнение радиоэлектронных устройств и рост их количества приводят к необходимости их защиты и повышению их надежности. Существует множество методов обеспечения этого, и они отличаются по возможностям, эффективности и легкости реализации. Среди этих методов модальное резервирование (МР) является одним из наиболее эффективных, надежных и несложных методов, применяемых в настоящее время. Использование метода при трассировке и монтаже печатных плат позволяет обеспечить как электромагнитную совместимость, так и надежность конечного электронного устройства. Проведены многочисленные исследования по изучению и развитию МР, включая 18 патентов на изобретения. Однако до сих пор нет полного и развернутого обзора публикаций по применению этого метода для проведения исследований на его основе. В данной статье представлен обзор истории и недавних исследований по МР для выявления возможности изготовления различных макетов структур с МР для экспериментальных исследований с целью оценки уровня излучаемых эмиссий в диапазоне частот, в том числе в условиях критичных температур, при исследовании впервые обобщены основные достоинства МР.

Ключевые слова: резервирование, модальное резервирование, модальная фильтрация, электромагнитная совместимость, электромагнитные помехи, излучаемые эмиссии, линии передачи, печатная плата.
DOI: 10.21293/1818-0442-2022-25-4-54-67

Высоконадежная система требует от инженеров повышения надежности компонентов (например, изменения материала, используемого в производстве) или применения методов резервирования с использованием имеющихся ресурсов без нарушения ограничений по стоимости, массе и объему системы [1, 2]. Второй вариант предпочтительнее из-за своей простоты [3], а его первое упоминание относится к 1956 г. [4]. Резервирование, как правило, применяется в критически важных системах, где требуется непрерывная работа, а их обслуживание сложно и дорого, например в случае бортовых радиоэлектронных систем. В этом случае время работы спутников связи может длиться более 10 лет [5]. Системы или подсистемы могут быть зарезервированы в активном или неактивном режиме с более низкой вероятностью отказа, поскольку зарезервированные компоненты будут находиться в режиме ожидания до отказа [6].

Кроме того, эти типы можно комбинировать, и они также делятся на подтипы: параллельное и *k*-из-*n*-активное резервирование, а также холодное, горячее и теплое резервирование [7, 8]. Резервирование может быть использовано для повышения не только надежности, но и эффективности системы [9]. Более того, резервирование считается быстрым решением для достижения любого желаемого уровня надежности на ранней стадии проектирования [10]. Поскольку резервирование может осуществляться в различных формах, оптимизированную модель системы можно получить, достигнув баланса между стоимостью и надежностью системы.

Несколько работ посвящено разработке математических моделей для определения надежности системы [11–13] даже в приложениях реального времени [14]. Резервирование во всех его видах используется в различных сферах. Оно применяется в защите информации [15], мемристорных устройствах [16], а также в нейронных сетях [17]. Оно применялось даже в нанотехнологиях, которые характеризуются высоким уровнем дефектов [18, 19]. Более того, оно также популярно в космических [20, 21] и авиационных [22] приложениях, а также в современных системах, касающихся беспилотных летательных аппаратов, например для защиты их канала передачи данных [23].

Резервирование также используется в коммуникационных приложениях [24]. Отказы печатных плат (ПП) могут привести к критическим проблемам, и они имеют различные причины, такие как старение, нагрев и загрязнение [25]. Чтобы бороться с этими отказами, обычно рекомендуется использовать резервирование при проектировании ПП. Его использованию в этих целях посвящены работы [26, 27].

Однако использование резервирования не всегда приносит пользу, например, если система не приспособлена для борьбы с искусственными или естественными электромагнитными помехами (ЭМП), которые также могут возникать из-за самого резервирования [28]. Таким образом, обеспечение электромагнитной совместимости (ЭМС) при проектировании ПП, даже если конструкция включает резервирование, является неизбежным для борьбы с ЭМП [29, 30]. Некоторые исследователи пытались повысить надежность ПП с помощью резервирования с учетом ЭМП [31], но универсального способа для достижения этой цели нет [32, 33]. В целом можно сказать, что все традиционные способы устранения последствий ЭМП недостаточно эффективны, особенно против сверхкоротких импульсов (СКИ) [34].

Модальное резервирование (МР), которое рассматривается в данной работе, является методом, который может одновременно повысить надежность радиоэлектронных устройств с помощью холодного резервирования и обеспечить их ЭМС за счет использования модальной фильтрации [35]. Она применяется для защиты радиоэлектронных устройств

от СКИ и в бесконтактном методе обнаружения и диагностики электрических соединений, скрытых в стенах [36]. МР может использоваться в различных приложениях, наиболее важными из которых являются критические и бортовые радиоэлектронные устройства. Например, МР использовалось для повышения помехоустойчивости ПП блока цифровой обработки сигналов [37] и ПП системы питания [38] автономной системы навигации космического аппарата. МР имеет несколько типов: на основе кратности резервирования (однократное, двукратное, трехкратное) [39], на основе симметричности структуры (симметричная и асимметричная) [40] и на основе рассматриваемого объекта (плата или кабель) [41, 42]. Большинство из этих типов интенсивно исследовалось в части кондуктивных эмиссий. Чтобы полностью прояснить механизм этого метода и проанализировать его следствия, необходимо также изучить его характеристики в части излучаемых эмиссий (ИЭ). Это начали исследовать лишь в нескольких работах [43–46], но только на основе анализа результатов моделирования и без учета климатического воздействия.

Поэтому целесообразно и необходимо провести экспериментальное исследование для оценки ИЭ от структур с МР при учете климатических воздействий. Необходима проработка возможности изготовления различных макетов структур с одно-, двух- и трёхкратным МР для будущих экспериментальных исследований с целью оценки уровня ИЭ в диапазоне частот, в том числе в условиях критичных температур. Для этого будет рассмотрена история развития МР со сравнительной оценкой технологичности, применимости и эффективности использования конструкций на основе разных способов МР, что является целью данной работы.

В общем МР заключается в такой трассировке ПП, что резервируемый и резервирующий проводники ПП трассируются таким образом, что между ними достигнута сильная электромагнитная связь в неоднородной диэлектрической среде. Это позволяет использовать преимущество модальной фильтрации и применять модальное разложение для подавления кондуктивных СКИ, которые имеют сильную способность проникновения из-за их короткой длительности, высокой мощности и широкого спектра.

Для достижения модального разложения необходимо, чтобы длительность СКИ была меньше абсолютного значения разности задержек четной и нечетной мод в структуре со связанными проводниками. В результате этого СКИ разлагается на импульсы, амплитуды которых меньше, чем амплитуда исходного СКИ. По этой причине основная ПП будет защищена и ее ЭМС будет обеспечена. Более того, если резервируемая ПП испытает отказ, резервная ПП немедленно начнет работу, не влияя на функциональность устройства. Таким образом, повышается надежность устройства, определяемая кратностью резервирования и вероятностью отказа каждой резервной ПП.

История МР

Идея МР была впервые сформулирована в 2015 г., а первые работы по ней были опубликованы в 2016 г. Первый патент на способ трассировки проводников печатной схемы с резервированием получен в 2016 г. [47]. Этот способ, являющийся самым простым (рис. 1), позволил уменьшить амплитуду СКИ в два раза. В том же году в [48] предложен другой способ трассировки ПП. Амплитуды СКИ также уменьшаются в два раза, но отличие данного способа от предыдущего из [47] заключается в том, что значение относительной диэлектрической проницаемости (ε_r) диэлектрика, который заполняет зазор между резервным и резервируемым проводниками, больше, чем диэлектрика, из которого изготовлена подложка ПП (рис. 2).

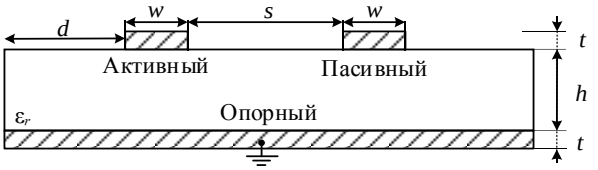


Рис. 1. Поперечное сечение структуры для способа трассировки печатных проводников схем с МР [47]

Рис. 2. Поперечное сечение структуры для способа трассировки печатных проводников с дополнительным диэлектриком для схем с МР [48]

Поскольку изменение ε_r может влиять на разницу между погонными задержками четной и нечетной мод сигнала, увеличение ε_r может быть использовано для увеличения этой разницы, тем самым повышая эффективность модальной фильтрации. В способе, предложенном в [49], резервный и резервируемый проводники располагаются друг под другом симметрично относительно подложки, а остальные электрически соединены друг с другом (рис. 3). Уменьшение амплитуды СКИ также осуществляется в два раза. Аналогичного результата можно достичь, используя способ, предложенный в [50], но уменьшив и массу ПП за счет отсутствия одного опорного проводника, однако без уменьшения уровня подавления СКИ (рис. 4).

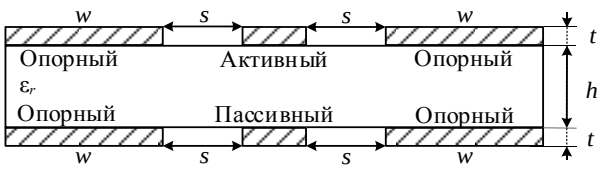


Рис. 3. Поперечное сечение структуры для способа трассировки двухсторонней ПП с МР [49]

В [51] предложен другой способ, который отличается от способа из [47]. Каждые два проводника в структуре формируют виток меандровой линии, а вместе они образуют отрезок четырехпроводной

линии передачи (рис. 5). При этом уменьшение амплитуды СКИ может достичь 4 раз.

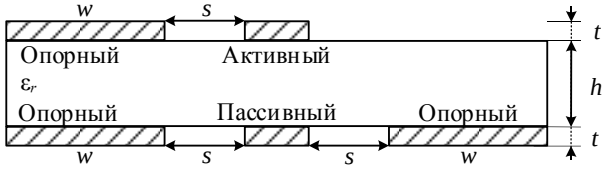


Рис. 4. Поперечное сечение структуры для способа трассировки двухсторонней ПП с МР без одного опорного проводника [50]

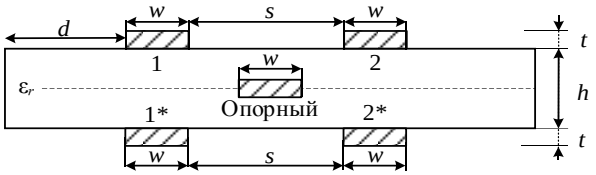


Рис. 5. Поперечное сечение структуры для способа однократного МР витков меандровой линии [51]

Одноименные проводники резервируемой и резервной цепей формируют связанную линию передачи с различными значениями погонных задержек. Проводники можно попарно соединить на одном конце на одном слое (проводники 1-2 и 1*-2* из рис. 5), на разных слоях (проводники 1-1* и 2-2* из рис. 5) или диагонально (проводники 1-2* и 2-1* из рис. 5). На основе использования различных диэлектрических материалов в [52, 53] предложены еще два способа МР. Улучшение в первом способе, относительно приведенных в [47–49], состоит в повышении надежности за счет увеличения кратности резервирования и помехоустойчивости за счет увеличения длительности СКИ, разлагаемого полностью (рис. 6, где любой проводник может быть активным). Второй способ гарантирует то же самое, но с возможностью трассировки печатных проводников на двух сигнальных слоях ПП: внешнем и внутреннем (рис. 7).

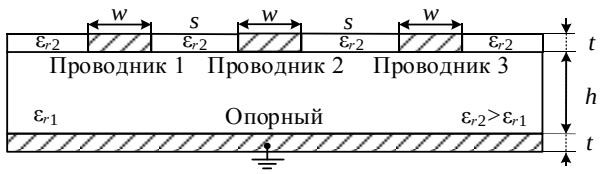


Рис. 6. Поперечное сечение структуры для способа трассировки печатных проводников с дополнительным диэлектриком для двухкратного МР [52]

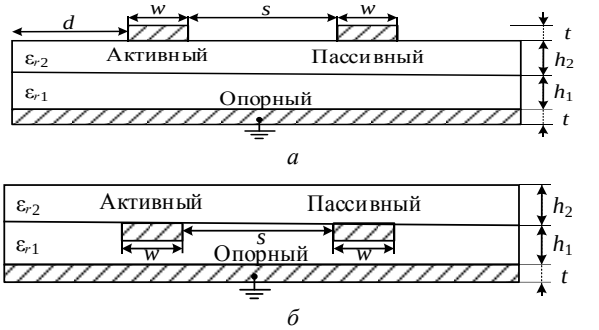


Рис. 7. Поперечное сечение структуры для способа трассировки печатных проводников на внешнем (*а*) и внутреннем (*б*) сигнальных слоях ПП с МР [53]

Способ, аналогичный описанным в [47, 51], предложен в [54]. В нём трассировка резервируемых и резервных проводников ПП выполняется попарно на каждом из основных двух слоев (рис. 8). При этом проводники имеют минимальный допустимый зазор между ними. Опорные проводники и проводники питания выполняются в виде отдельных слоев и располагаются между сигнальными слоями. При этом резервируются не только сигнальные проводники, но и проводники питания, которые выполнены с помощью зазоров в опорных проводниках и образуют связанные линии. Этот способ может уменьшить восприимчивость резервируемых проводников питания к внешним кондуктивным эмиссиям и снизить уровень кондуктивных эмиссий от них.

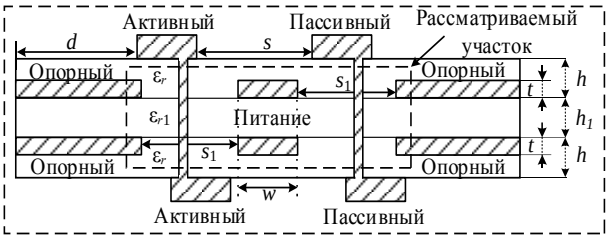


Рис. 8. Поперечное сечение структуры для способа трассировки печатных проводников питания цепей с МР [54]

Способ из [55] основан на взаимных расположении, компоновке и трассировке резервируемых и резервных ПП. Отличается он выполнением опорного проводника в виде отдельных слоев на резервируемой и резервной печатных платах, склеенных диэлектрическим слоем с ε_r большей, чем у подложек резервируемой и резервной ПП (рис. 9). ПП расположены параллельно и друг под другом, а их электронные компоненты размещены на противоположных сторонах этих ПП. Здесь амплитуда СКИ уменьшается в 2,5 раза.

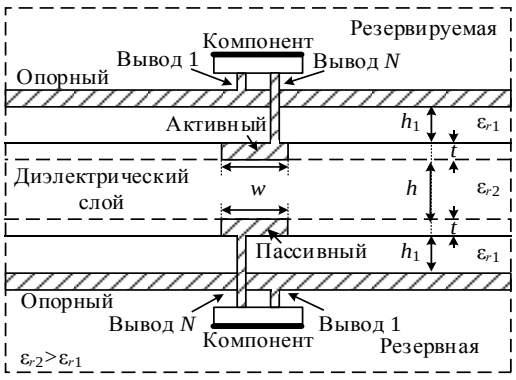


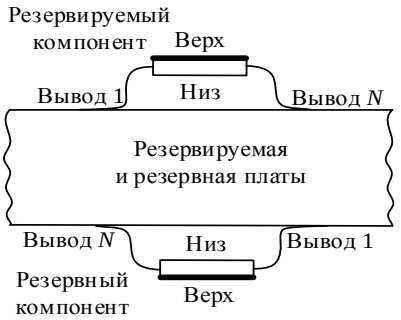
Рис. 9. Поперечное сечение структуры для метода компоновки неформованных радиоэлектронных компонентов на печатных платах для цепей с резервированием [55]

Недостаток состоит в разнице трассировки резервируемой и резервной ПП, что вызвано асимметричным расположением выводов электронных компонентов относительно диэлектрического слоя, который склеивает резервируемую и резервную платы таким образом, что одноименные выводы компонентов не находятся друг под другом. Вследствие этого

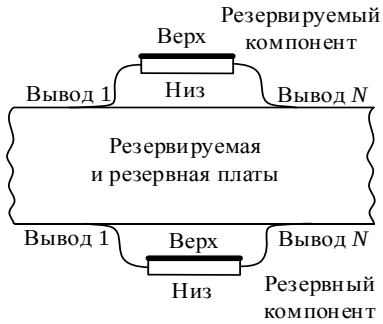
уменьшается длина отрезков электромагнитно связанных линий, формирующихся одноименными трассами резервируемой и резервной цепей, что снижает полезные связи между ними.

Способ из [56], в отличие от предыдущего из [55], использует формовку выводов резервируемых компонентов в одном направлении относительно корпуса компонента, а резервных – в противоположном, причем эти компоненты находятся друг под другом (рис. 10, 11). Это максимизирует длину связанных линий, приводя к дополнительному снижению кондуктивных эмиссий (к плате и от нее).

В [57] предложен другой способ. Его особенность заключается в расположении резервируемых и резервных компонентов на внутренней стороне ПП в слое склеивающего диэлектрика, а не на внешней (рис. 12). Уменьшение амплитуды СКИ с помощью этого способа достигает 2,25 раза.



а



б

Рис. 10. Схематическое изображение формовки корпусов радиоэлектронных компонентов и взаимного расположения выводов без (*а*) и с (*б*) использованием способа, предложенного в [56]

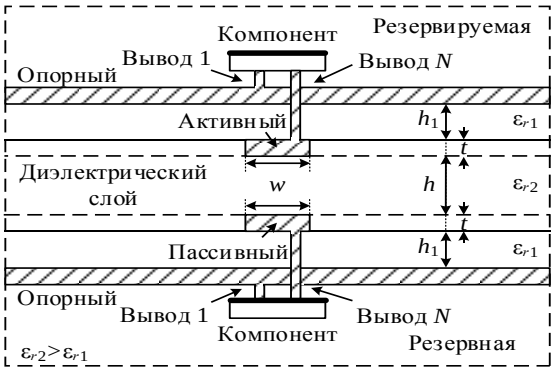


Рис. 11. Поперечное сечение структуры для способа компоновки неформованных радиоэлектронных компонентов на печатных платах с МР [56]

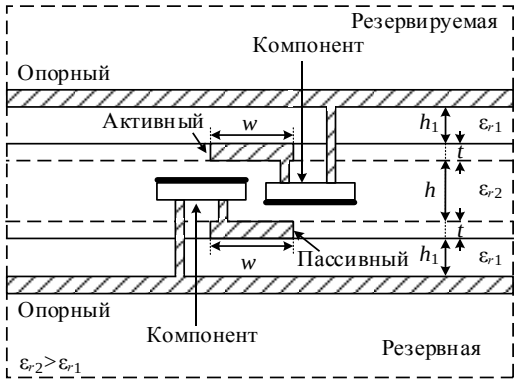


Рис. 12. Поперечное сечение структуры для способа внутренней компоновки печатных плат для цепей с МР [57]

В [58] предложен способ для резервирования плоских кабелей, где проводники резервируемого кабеля располагаются на одном уровне в диэлектрическом слое, а соответствующие одноименные резервные проводники – под ними на другом уровне (рис. 13). Эффективность использования этих способов в приложениях связи и управления оценена в [59, 60].

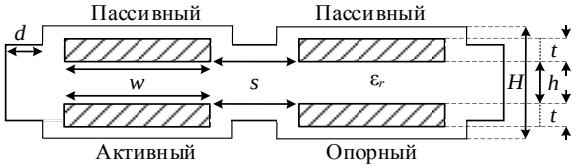


Рис. 13. Поперечное сечение структуры для способа МР плоских кабелей [58]

Для трехкратного МР первый способ представлен в [61]. Его отличие от способа из [55] состоит в добавлении двух резервных цепей для увеличения кратности резервирования (рис. 14). На одной ПП располагаются резервируемая и одна резервная цепи, а на второй – остальные две. С помощью этого способа амплитуда СКИ может быть уменьшена в 4 раза.

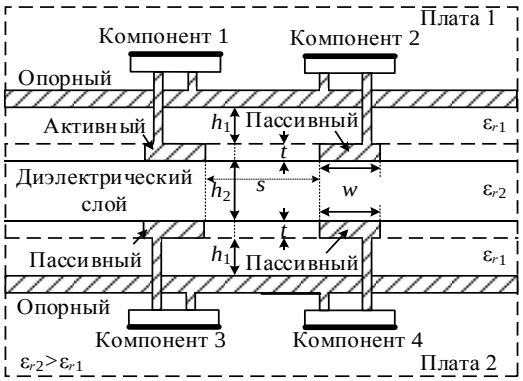


Рис. 14. Поперечное сечение структуры для способа трёхкратного МР в многослойных печатных платах [61]

В [62] предложен другой способ трехкратного МР цепи. Его отличие от способа из [49] заключается в том, что сигнальные проводники разделяются на два одинаковых проводника с минимальным зазором между ними (рис. 15). Также проведены срав-

нительные исследования по использованию этих способов.

Рис. 15. Поперечное сечение структуры для способа трехкратного МР проводников печатной платы [62]

Например, в [63] авторы доказали, что с помощью способа МР из [49] можно увеличить коэффициент ослабления помехового сигнала до 12 дБ. Они также сравнили результаты, полученные с помощью этого способа и способов из [47, 55]. Применив МР в блоке цифровой обработки сигналов автономной навигационной системы космического аппарата, авторы улучшили его помехоустойчивость.

В отличие от [47, 57], в [64] предложен другой способ МР, обеспечивающий взаимные расположение, компоновку и трассировку резервируемой и резервной плат с землей в виде отдельных двух печатных проводников в диэлектрическом слое, склеивающем эти платы (рис. 16). Это облегчает изготовление ПП и монтаж ее компонентов и снижает восприимчивость резервируемой цепи к внешним кондуктивным эмиссиям.

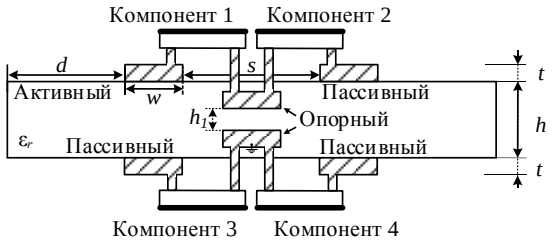


Рис. 16. Поперечное сечение структуры для способа компоновки печатных проводников с трёхкратным МР [64]

Кроме того, в [65] предложен другой способ МР. Он отличается от [55] тем, что в нем предлагается использовать дополнительные сигнальные слои таким образом, чтобы резервные и резервируемые проводники одних и тех же цепей трассировались на внешних и внутренних сигнальных слоях ПП, соединенных отверстиями (рис. 17). Земля выполнена в виде отдельных слоев, при этом резервируемая и резервная ПП изготовлены из двух диэлектрических слоев.

Поскольку одной из главных особенностей МР является надежность, необходимо изучить эффективность МР и после отказов. Поэтому в [66] исследована устойчивость к воздействию СКИ для ПП с однократным и трехкратным МР после отказов в виде короткого замыкания и холостого хода. Проведенный анализ показал, что при однократном МР ослабление после отказа уменьшилось с 2,3 до 1,7 раза. Для трехкратного МР выявлено, что после отказа предпочтительнее переключаться на цепь, электромагнитная связь которой с резервируемой цепью меньше. Это объясняется тем, что отклонение амплитуд разложенных импульсов в случае отказа на конце одного из резервных проводников от амплитуд до отказа минимально. Эти и другие результаты были обсуждены и подтверждены для однократного МР в [67] не только во временной, но и в частотной области до 2 ГГц в [68], а также до 18 ГГц с использованием квазистатического и электродинамического анализа для сравнения с результатами, полученными экспериментально в [69].

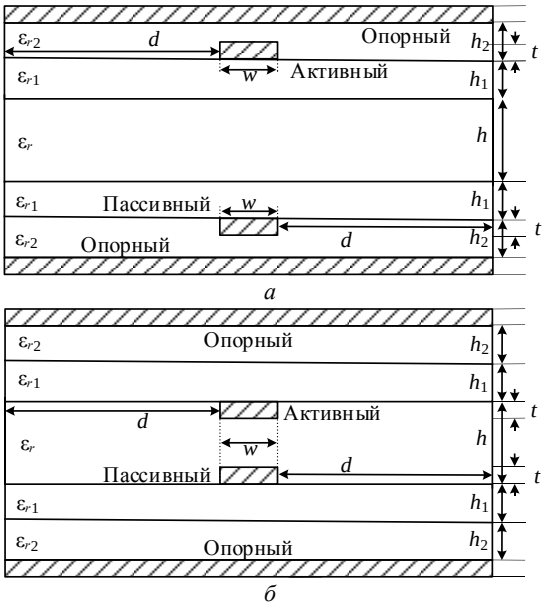


Рис. 17. Поперечное сечение структуры для способа компоновки многослойной печатной платы с МР внутренних (*а*) и внешних (*б*) сигнальных слоев [65]

Порядок переключения после отказов для двухкратного МР обсуждался в [70]. Подробно исследовался порядок переключения после отказа для трехкратного МР во временной [71] и частотной [72] областях. На основе этих исследований получены два патента на способы переключения после отказа для двухкратного [73] (рис. 18) и трехкратного [74] (рис. 19) МР.

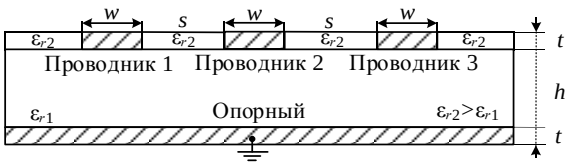


Рис. 18. Поперечное сечение структуры для способа переключения цепей с двукратным МР после отказов [73]

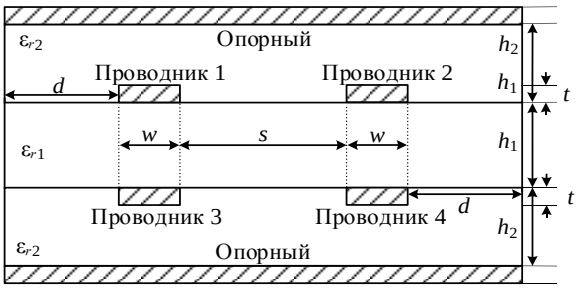


Рис. 19. Поперечное сечение структуры для способа переключения цепей с трехкратным МР после отказов [74]

Более того, исследование показало, что вероятность отказа резервной трассы при использовании МР ниже, чем у резервируемой. Это было доказано в [75, 76] для однократного и в [77] для трехкратного МР с помощью пяти *N*-норм [34], которые используются для оценки опасности воздействия СКИ на радиоэлектронные устройства.

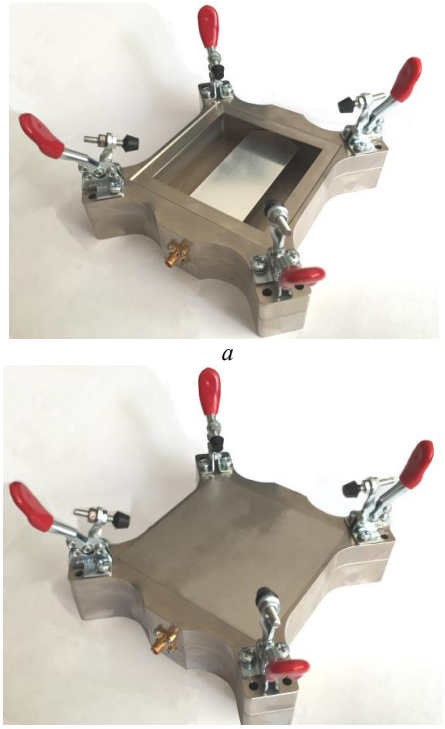
Измерительное оборудование

Соответствующие уровни помехоэмиссии и помехоустойчивости устанавливаются требованиями по ЭМС радиоэлектронной аппаратуры. Стандарты на помехоэмиссии, такие как IEC 61967-2 и IEC 62132-2, содержат информацию о порядке измерений этих уровней, необходимых приборах и оснастке. По этим стандартам ТЕМ-камера является одним из устройств, применяемых при таких видах исследований.

Такие ТЕМ-камеры на основе коаксиальной линии передачи прямоугольного сечения широко используются для тестирования на помехоэмиссии и помехоустойчивость интегральных схем. Когда генератор подает сигнал с заранее заданными характеристиками на вход тестируемого устройства, расположенного в регулярной части камеры, поперечная электромагнитная волна распространяется во внутреннем пространстве камеры, образуя однородное электромагнитное поле. Затем сигнал может быть поглощен согласованной нагрузкой, расположенной на противоположной стороне камеры. Первая резонансная частота ТЕМ-камеры определяется ее геометрическими параметрами, которые, в свою очередь, определяют верхнюю границу рабочего диапазона частот ТЕМ-камеры [78]. Используя такие камеры, можно оценить уровень излучаемых эмиссий также от ПП, поскольку он пропорционален амплитудам напряжения на концах центрального проводника камеры.

В ТУСУРе разработаны и созданы два лабораторных макета ТЕМ-камеры, отличающихся диапазоном рабочих частот. Первая камера, называемая миниатюрной мини-ТЕМ-камерой, работает до 5 ГГц [79]. Её высота составляет 31 мм, а длина регулярной части 104 мм, ширина её центрального проводника 40 мм, а его толщина 1 мм (рис. 20). Вторая, называемая классической большой ТЕМ-камерой, работает до 2 ГГц [80]. Её высота составляет 120 мм, а длина регулярной части 140 мм, ширина её центрального проводника 106,2 мм, а его толщина 2 мм (рис. 21). Исследуемое устройство (здесь ПП) при использовании этих камер должно иметь размеры 100×100 мм. Также желательно, чтобы земля ПП была сплошная и соединялась с корпусом камеры для сохранения его целостности. И поскольку важно оценить излучаемые эмиссии от ПП с МР и при разных климатических условиях, то необходимо использование специальной камеры для контроля температуры.

В ТУСУРе в таких целях используется климатическая (испытательная) камера тепла-холода ESPEC SU-262, в которой помешается только миниатюрная ТЕМ-камера. Поэтому при использовании таких измерительных приборов для проведения такого типа экспериментов необходимо учитывать много факторов, таких как термостойкость используемых материалов в изготовления ПП, гибкость и геометрия структуры самой ПП, которая является основным рассматриваемым фактором в данной работе.



а

б

Рис. 20. Лабораторный макет миниатюрной ТЕМ-камеры с открытой (*а*) и закрытой (*б*) апертурой

а

б

Рис. 21. Лабораторный макет классической ТЕМ-камеры с открытой (*а*) и закрытой (*б*) апертурой

Выбор структур для исследования эмиссий

Для проработки возможности изготовления различных макетов структур с одно-, двух- и трёхкратным МР для будущих экспериментальных исследований с целью оценки уровня излучаемых эмиссий в диапазоне частот, в том числе в условиях критичных температур, рассмотрим способы МР и проанализируем возможность их применения для этой цели.

Для однократного МР самым простым по технологичности является макет по способу [47]. Макеты такого типа уже использовались для подобного исследования, например в работе [81]. Способ из [48] немного сложнее, так как требуется добавление тонкого слоя диэлектрика между проводниками ПП.

В отличие от макетов для способов из [47, 48], изготовление макетов для способов из [49, 50] может затруднить оценку уровня излучаемых эмиссий, так как нужно будет измерять его в ТЕМ-камере с двух сторон ПП, т.е. измерять два раза. Но, несмотря на это, использование такого способа для выполнения цели работы остаётся возможным. То же самое касается изготовления макета для способа из [53], но здесь растет сложность изготовления из-за трассировки двух сигнальных слоев на макете с малыми размерами (100×100 мм), а также из-за необходимости материалов с разными значениями диэлектрической проницаемости. Тем более здесь будет увеличено влияние на характеристики линий передачи изменения диэлектрической проницаемости с изменением температуры. Поэтому здесь сложно будет оценить вклад изменения тепловых коэффициентов двух разных материалов в уровень излучаемых эмиссий.

Способы из [49, 50, 54] также усложняют задачу, поскольку в них нет сплошной земли, а это нарушает однородность поля в камере. Между тем способ из [54] соединяет сложности при использовании способов из [49, 53], тем более, что он направлен на МР не только сигнальных проводников, но и проводников питания. Поэтому использовать его в таком виде эксперимента нецелесообразно. Это же относится к способу из [50], поскольку отсутствие одного опорного проводника усложняет измерения уровня излучаемых эмиссий в камере с двух сторон ПП.

Способ из [51] не подходит для изготовления макетов с такой целью, так как опорный проводник находится внутри слоя диэлектрика. Это также относится и к способам из [55–57, 65], в которых ПП экранирована с двух сторон.

В результате способы из [48, 49, 53], несмотря на сложность изготовления макетов для них, являются оптимальным выбором для изготовления макетов с целью исследования излучаемых эмиссий от ПП с однократным МР.

Что касается многократного МР, то можно сказать, что выводы для способа [48] подходят также к способу из [52]. Здесь уровень сложности даже меньше, так как легче покрыть другим диэлектриком всю ПП, чем только зазор между проводниками. Аналогично выводы по способам из [49, 51] подходят также к способу из [62, 64] соответственно. Способ из [58] не подходит для изготовления макетов с целью исследования излучаемых эмиссий в камере, так как он направлен на резервирование сигнальных проводников в плоских кабелях.

Способ из [61] также не подходит для такого типа эксперимента по причинам, относящимся к способам из [55–57, 65]. Способы из [73, 74] предложены как способы переключения после отказов, поэтому их использование в предварительных исследованиях нецелесообразно. Между тем в будущем можно оценить уровень эмиссий после переключения, используя только способ из [73], так как в способе из [74] ПП экранирована. В результате можно сказать, что для оценки излучаемых эмиссий от ПП с двухкратным и трехкратным МР способы из [52, 62], соответственно, оптимальны для изготовления макетов.

Заключение

Модальное резервирование (МР) по существу использует избыточность полосы пропускания линий передачи, когда их верхняя частота гораздо выше верхней частоты спектра полезного сигнала. Тогда выполняется преобразование одноименных одиночных линий нескольких одинаковых цепей с резервированием за счет изготовления в единой конструкции с образованием их электромагнитной связи в связанные (однократное резервирование) или многопроводные (многократное резервирование) линии передачи. При этом верхняя частота полосы пропускания уменьшается до верхней частоты спектра полезного сигнала. Таким образом, передача полезного сигнала не нарушается. Однако у линий передачи появляются новые свойства, которые можно использовать для ослабления помеховых сигналов.

Так, на частотах выше верхней частоты спектра полезного сигнала появляются минимумы в частотной зависимости коэффициента передачи. При кондуктивном воздействии сверхширокополосного импульса опасной амплитуды на вход любой из линий этот импульс разлагается на импульсы меньшей амплитуды. В результате каждый проводник цепи с резервированием совместно с единым опорным проводником становится помехозащитным фильтром. Это достигается без введения каких-либо компонентов, а лишь конструктивно. Такие структуры взаимны или близки к ним, что позволяет ослаблять не только внешние кондуктивные воздействия, но и помехоэмиссии от компонентов резервируемых цепей. Кроме того, могут уменьшаться и излучаемые эмиссии от таких линий, позволяя ослабить требования к экранированию.

Всё это касается работы резервируемой цепи до отказа, так что эти преимущества могут использоваться довольно долго, пока резервируемая цепь не выйдет из строя. После её отказа и переключения на резервную цепь эти преимущества могут несколько измениться, но незначительно и только в участке

цепи с отказом, тогда как в остальных участках они сохранятся. В случае многократного МР возможен выбор более предпочтительной резервирующей цепи из оставшихся для переключения на неё. Отметим, что при однократном МР амплитуда воздействующего импульса может уменьшаться в 2 раза, а при трёхкратном – в 4 раза, что достигается за счет зеркальной симметрии по одной и двум плоскостям соответственно. Это получается даже при слабой электромагнитной связи, тогда как при сильной связи эти значения могут увеличиться в несколько раз. При этом увеличивается и временной интервал между импульсами, что препятствует их частичному наложению.

Таким образом, МР дает уникальную возможность не только повысить надежность критичной радиоэлектронной аппаратуры за счет её резервных цепей, но и непрерывно обеспечивать за счет них (как до, так и после выхода их из строя) ЭМС в части уменьшения кондуктивных и излучаемых эмиссий этой аппаратуры, а также ослабления воздействий на неё, особенно преднамеренных сверхкоротких импульсов, создаваемых электромагнитным оружием.

В ходе данной работы выполнен обзор исследований по МР и проанализированы все предложенные способы на его основе. В результате анализа выявлены возможные варианты изготовления макетов ПП с МР для экспериментальных исследований с целью оценки уровня излучаемых эмиссий в диапазоне частот, в том числе в условиях критичных температур.

Работа выполнена при финансовой поддержке Российского научного фонда (проекты 19-19-00424, https://rscf.ru/project/19-19-00424/, обзор по однократному МР и 20-19-00446, https://rscf.ru/project/20-19-00446/, обзор по многократному МР) в ТУСУРе.

Литература

1. Trivedi K. Reliability and Availability Engineering: Modeling, Analysis, and Applications / K. Trivedi, A. Bobbio. – Cambridge: Cambridge University Press, 2017. – 712 p. DOI: 10.1017/9781316163047.

2. Amari S.V. Redundancy optimization problem with warm-standby redundancy. / S.V. Amari, G. Dill // San Jose, CA: IEEE Proceedings - Annual Reliability and Maintainability Symposium (RAMS), 2010. – P. 1–6. DOI: 10.1109/RAMS.2010.5448068.

3. Optimal Reliability Design: Fundamentals and Applications / S.V.W. Kuo, V.R. Prasad, F.A. Tillman, C.L. Hwang. – Cambridge: Cambridge University Press, 2001. – 412 p.

4. Von Neumann J. Probabilistic logics and the synthesis of reliable organisms from unreliable components // Princeton. – Automata Studies: Princeton University Press, 1956. – P. 43–98.

5. Chen D.M. Satellite engineering series: communications satellite payload technology. – China Astronautic Publishing House, 2001.

6. Coit D.W. Maximization of System Reliability with a Choice of Redundancy Strategies // IIE Transactions. – 2003. – Vol. 35. – P. 535–543. – DOI: /10.1080/07408170304420.

7. Grida M. Repairable 3-out-of-4: Cold standby system availability / M. Grida, A. Zaid, G. Kholief // Annual Reliability and Maintainability Symposium (RAMS). – 2017. – P. 1–6. DOI: 10.1109/RAM.2017.7889797.

8. Lobur M. Modelling of type I and II errors of switching device for systems with hot and cold redundancy based on two-terminal dynamic fault tree / M. Lobur, T. Stefanovych, S. Shcherbovskykh // The 14th International Conference of The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM). – 2017. – P. 19–21. DOI: 10.1109/CADSM.2017.7916075.

9. Redundancy design of modular DC solid-state transformer based on reliability and efficiency evaluation / Y. Li, Y. Zhang, R. Cao, X. Liu, C. Lv, J. Liu // CPSS Transactions on Power Electronics and Applications. – 2021. – Vol. 6, No. 2. – P. 115–126. DOI: 10.24295/CPSSTPEA.2021.00010.

10. Design and optimization of an Integrated Reliability redundancy system with multiple constraints / G. Sankaraiah, Y. Raghunatha Reddy, C. Umasankar, B.D. Sarma // The 2nd International Conference on Reliability, Safety and Hazard – Risk-Based Technologies and Physics-of-Failure Methods (ICRESH). – 2010. – P. 118–122. DOI: 10.1109/ICRESH.2010.5779527.

11. Pan D. Study on Optimization of System Reliability Redundancy Based on Hybrid Intelligent Algorithm // The International Conference on Environmental Science and Information Application Technology. – 2009. – P. 560–563. DOI: 10.1109/ESIAT.2009.426.

12. Boland P.J. Component redundancy vs system redundancy in the hazard rate ordering / P.J. Boland, E. El-Neweihi // IEEE Transactions on Reliability. – 1995. – Vol. 44, No. 4. – P. 614–619. DOI: 10.1109/24.475980.

13. Shcherbovskykh S. Modelling features of type I and II errors of switching device for system with double hot and double cold redundancy based on two-terminal dynamic fault tree / S. Shcherbovskykh, T. Stefanovych // The 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET). – 2018. – P. 753–756. DOI: 10.1109/TCSET.2018.8336309.

14. Neves F.G.R. Comparison between Redundancy Techniques for Real Time Applications / F.G.R. Neves, O. Saotome // The fifth International Conference on Information Technology: New Generations (ITNG). – 2008. – P. 1299–1300. DOI: 10.1109/ITNG.2008.229.

15. Peterson W. Error-Correcting Codes / W. Peterson, E. Weldon. – Cambridge, MA: MIT Press, 1972. – 576 p.

16. Memristive Stateful Logic with N-Modular Redundancy Error Correction Design towards High Reliability / X. Zhu, H. Xu, H. Long, Q. Li, Z. Li, H. Liu, Y. Wang // The 5th IEEE Electron Devices Technology & Manufacturing Conference (EDTM). – 2021. – P. 1–3. DOI: 10.1109/EDTM50988.2021.9420918.

17. Logic Computing with Stateful Neural Networks of Resistive Switches / Z. Sun, E. Ambrosi, A. Bricalli, D. Ielmini // Adv. Mater. – 2018. – Vol. 30, No. 38. – P. 1–8. DOI: 10.1002/adma.201802554.

18. A performance evaluation of the Intel iAPX 432 / P. Hansen, M. Linton, R. Mayo, M. Murphy, D. Patterson // SIGARCH Comput. Archit. News. – 1982. – Vol. 10, No. 4. – P. 17–26. DOI: 10.1145/641542.641545.

19. Namazi A. Gate-Level Redundancy: A New Design-for-Reliability Paradigm for Nanotechnologies / A. Namazi, M. Nourani // IEEE Transactions on Very Large-Scale Integration (VLSI) Systems. – 2010. – Vol. 18, No. 5. – P. 775–786. DOI: 10.1109/TVLSI.2009.2016206.

20. Xiong X. Research on Redundancy Solution of Satellite Transponders Based on Reliability Analysis / X. Xiong, H.T. Zhao, T.B. Hu // The International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering

(QR2MSE). – 2019. – P. 689–694. DOI: 10.1109/QR2MSE 46217.2019.9021237.

21. Sklaroff J.R. Redundancy Management Technique for Space Shuttle Computers // IBM Journal of Research and Development. – 1976. – Vol. 20, No. 1. – P. 20–28. DOI: 10.1147/rd.201.0020.

22. Xiao C. Reliability Research on Airborne Dual Redundancy of Electrical Wiring Interconnection System / C. Xiao, L. Deng // The 11th International Symposium on Computational Intelligence and Design (ISCID). – 2018. – P. 137–140. DOI: 10.1109/ISCID.2018.10132.

23. GPR-Based EMI Prediction for UAV's Dynamic Datalink / D. Zhang, M. Zhao, E. Cheng, Y. Chen // IEEE Transactions on Electromagnetic Compatibility. – 2021. – Vol. 63, No. 1. – P. 19–29. DOI: 10.1109/TEMC.2020.3000919.

24. Rentschler M. Performance analysis of parallel redundant WLAN / M. Rentschler, P. Laukemann // Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012). – 2012. – P. 1–8. DOI: 10.1109/ETFA.2012.6489647.

25. Introduction to printed circuit board failures / D. Slee, J. Stepan, W. Wei, J. Swart // IEEE Symposium on Product Compliance Engineering. – 2009. – P. 1–8. DOI: 10.1109/PSES.2009.5356012.

26. Heterogeneous Redundancy for PCB Track Failures: An Automotive Example / M.G. Labib, D.G. Mahmoud, G.I. Alkady, I. Adly, H.H. Amer, R.M. Daoud, H.M. ElSayed // The 14th International Conference on Computer Engineering and Systems (ICCES). – 2019. – P. 189–194. – DOI: 10.1109/ICCES48960.2019.9068123.

27. Chen H.C. Improvement of High-Current Density PCB Design with PSU Load Balance and Redundancy on a High End Server System / H.C. Chen, Y.W. Bai // Canadian Journal of Electrical and Computer Engineering. – 2014. – Vol. 37, No. 4. – P. 203–211. DOI: 10.1109/CJECE.2014.2327091.

28. Functional safety standard's techniques and measures in light of electromagnetic interference / J.V. Waes, J. Vankeirsbilck, D. Pissoort, J. Boydens // XXVI International Scientific Conference Electronics (ET). – 2017. – P. 1–4. DOI: 10.1109/ET.2017.8124403.

29. Pissoort D. Why is the IEEE developing a standard on managing risks due to EM disturbances? / D. Pissoort, K. Armstrong // IEEE International Symposium on Electromagnetic Compatibility (EMC). – 2016. – P. 78–83. DOI: 10.1109/ISEMC.2016.7571612.

30. Resilience of Error Correction Codes Against Harsh Electromagnetic Disturbances: Fault Mechanisms / J.V. Waes, D. Vanoost, J. Vankeirsbilck, J. Lannoo, D. Pissoort, J. Boydens // IEEE Transactions on Electromagnetic Compatibility. – 2020. – Vol. 62, No. 4. – P. 1017–1027. DOI: 10.1109/TEMC.2019.2931369.

31. Luo S. A review of distributed power systems. Part II. High frequency AC distributed power systems / S. Luo, I. Batarseh // IEEE Aerospace and Electronic Systems Magazine. – 2006. – Vol. 21, No. 6. – P. 5–14. DOI: 10.1109/MAES.2006.1662037.

32. Techniques and measures to achieve EMI resilience in mission- or safety-critical systems / D. Pissoort, J. Lannoo, J.V. Waes, A. Degraeve, J. Boydens // IEEE Electromagnetic Compatibility Magazine. – 2017. – Vol. 6, No. 4. – P. 107–114. DOI: 10.1109/MEMC.0.8272297.

33. Study on the use of different transmission line termination strategies to obtain EMI-diverse redundant systems / J. Lannoo, A. Degraeve, D. Vanoost, J. Boydens, D. Pissoort // IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC). – 2018. – P. 210–215. DOI: 10.1109/ISEMC.2018.8393768.

34. Study and Classification of Potential IEMI Sources / N. Mora, F. Vega, G. Lugrin, F. Rachidi, M. Rubinstein // System Design and Assessment Notes. – 2014. – P. 1–43.

35. Gazizov T.R. New approach to EMC protection / T.R. Gazizov, A.M. Zabolotsky // The 18th International Zurich Symposium on Electromagnetic Compatibility. – 2007. – P. 273–276. DOI: 10.1109/EMCZUR.2007.4388248.

36. Orlov P.E. Contactless Modal Phenomena Based Approach to Detecting, Identifying, and Diagnosing of Electrical Connections / P.E. Orlov, T.R. Gazizov // Complexity. – 2018. – Vol. 2018. – P. 5081684. DOI: 10.1155/2018/5081684.

37. Quasistatic simulation of ultrashort pulse propagation in the spacecraft autonomous navigation system circuit with modal reservation / P.E. Orlov, A.V. Medvedev, V.R. Sharafutdinov, I.F. Kalimulin // International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). – 2017. – P. 495–500. DOI: 10.1109/SIBIRCON.2017.8109935.

38. Orlov P.E. Quasistatic Simulation of Ultrashort Pulse Propagation in the Spacecraft Autonomous Navigation System Power Circuit with Modal Reservation / P.E. Orlov, A.V. Medvedev, V.R. Sharafutdinov // The 19th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM). – 2018. – P. 1–6. DOI: 10.1109/EDM.2018.8435026.

39. Method of lay-out of a multilayer PCB for circuits with triple reservation / P.E. Orlov, E.N. Buichkin, A.O. Belousov, T.R. Gazizov // International Siberian Conference on Control and Communications (SIBCON). – 2017. – P. 1–4. DOI: 10.1109/SIBCON.2017.7998528.

40. From Symmetry to Asymmetry: The Use of Additional Pulses to Improve Protection against Ultrashort Pulses Based on Modal Filtration / A.O. Belousov, E.B. Chernikova, M.A. Samoylichenko, A.V. Medvedev, A.V. Nosov, T.R. Gazizov, A.M. Zabolotsky // Symmetry. – 2020. – Vol. 12, No. 7. – P. 1117. DOI: 10.3390/sym12071117.

41. Orlov P.E. Quasistatic and electromagnetic simulation of interconnects of printed circuit boards with modal reservation / P.E. Orlov, E.N. Buichkin // The 18th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM). – 2017. – P. 54–58. DOI: 10.1109/EDM.2017.7981707.

42. Optimization of stack parameters of multi-layer PCB for circuits with redundancy by genetic algorithm / P.E. Orlov, T.R. Gazizov, V.R. Sharafutdinov, I.F. Kalimulin // International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). – 2017. – P. 463–467. DOI: 10.1109/SIBIRCON.2017.8109928.

43. Hasan A.A. Approach to Estimation of Radiated Emission from Circuits with Modal Reservation / A.A. Hasan, A.A. Kvasnikov, T.R. Gazizov // The 21st International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM). – 2020. – P. 169–173. DOI: 10.1109/EDM49804.2020.9153498.

44. Hasan A.A. Estimation of the Radiated Emission from a Single and Coupled Wires with Insulation above the Ground Plane / A.A. Hasan, T.R. Gazizov // IEEE 22nd International Conference of Young Professionals in Electron Devices and Materials (EDM). – 2021. – P. 149–152. DOI: 10.1109/EDM52169.2021.9507613.

45. Hasan A.A. Estimation of radiated emissions from a structure with a single modal reservation / A.A. Hasan, Y.S. Zhechev, T.R. Gazizov // Journal of Physics: Conference Series. – 2021. – Vol. 1862, No. 1. 012003. DOI: 10.1088/1742-6596/1862/1/012003.

46. Hasan A.A. Comparing the Estimates of the Radiated Emission from a Structure with Modal Reservation by Two

Approaches / A.A. Hasan, T.R. Gazizov // IEEE 22nd International Conference of Young Professionals in Electron Devices and Materials (EDM). – 2021. – P. 145–148. DOI: 10.1109/EDM52169.2021.9507636.

47. Пат. 2 603 850 РФ, МПК H 04 B 15/02. Способ трассировки печатных проводников цепей с резервированием / Т.Р. Газизов, П.Е. Орлов, В.Р. Шарафутдинов и др. – 2 015 129 253 / 07; заявл. 16.07.15; опубл. 10.12.2016, Бюл. № 34. – 7 с.

48. Пат. 2 603 851 РФ, МПК H 04 B 15/00. Способ трассировки печатных проводников с дополнительным диэлектриком для цепей с резервированием / Т.Р. Газизов, П.Е. Орлов, В.Р. Шарафутдинов и др. – 2 015 129 263 / 07; заявл. 16.07.15; опубл. 10.12.2016, Бюл. № 34. – 8 с.

49. Пат. 2 603 843 РФ, МПК H 04 B 15/02. Способ резервирования для печатных плат / Т.Р. Газизов, П.Е. Орлов, В.Р. Шарафутдинов и др. – 2 015 137 547 / 07; заявл. 02.09.15; опубл. 10.12.2016, Бюл. № 34. – 8 с.

50. Пат. 2 762 336 РФ, МПК H 05 K 3/00, H 04 B 15/02. Способ трассировки двухсторонней печатной платы для цепей с модальным резервированием / Т.Р. Газизов, М. Самойличенко. – 2 021 105 511; заявл. 04.03.21; опубл. 20.12.2021, Бюл. № 35. – 7 с.

51. Пат. 2 732 607 РФ, МПК H 04 B 15/00, H 01 P 11/00. Способ однократного модального резервирования межсоединений / Т.Р. Газизов, А.О. Белоусов, Е. Черникова. – 2 019 140 187; заявл. 09.12.19; опубл. 25.09.2020, Бюл. № 27. – 7 с.

52. Пат. 2 752 232 РФ, МПК H 04 B 15/02, H 01 P 11/00. Способ трассировки печатных проводников с дополнительным диэлектриком для цепей с двукратным резервированием / Т.Р. Газизов, А.В. Медведев. – 2 019 140 181; заявл. 19.12.19; опубл. 23.07.2021, Бюл. № 16. – 7 с.

53. Пат. 2 752 233 РФ, МПК H 04 B 15/02. Способ трассировки печатных проводников на двуслойной печатной плате для цепей с резервированием / Т.Р. Газизов, А.В. Медведев. – 2 020 122 274; заявл. 06.07.20; опубл. 23.07.2021, Бюл. № 21. – 8 с.

54. Пат. 2 779 536 РФ, МПК H 04 B 15/02. Способ трассировки печатных проводников цепей питания с резервированием / Т.Р. Газизов, А.В. Медведев и др. – 2 021 115 972; заявл. 03.06.21; опубл. 08.09.2022, Бюл. № 25. – 6 с.

55. Пат. 2 614 156 РФ, МПК H 04 B 15/02, H 03 H 3/00, H 05 K 3/36. Способ компоновки печатных плат для цепей с резервированием / Т.Р. Газизов, П.Е. Орлов, В.Р. Шарафутдинов и др. – 2 015 137 532; заявл. 02.09.15; опубл. 06.03.2017, Бюл. № 7. – 10 с.

56. Пат. 2 693 838 РФ, МПК H 04 B 15/02. Способ компоновки неформованных радиоэлектронных компонентов на печатных платах для цепей с резервированием / Т.Р. Газизов, П.Е. Орлов, В.Р. Шарафутдинов. – 2 018 124 928; заявл. 06.07.18; опубл. 05.07.2019, Бюл. № 19. – 12 с.

57. Пат. 2 624 637 РФ, МПК H 04 B 15/02, H 03 H 3/00, H 05 K 3/36. Способ внутренней компоновки печатных плат для цепей с резервированием / Т.Р. Газизов, П.Е. Орлов, В.Р. Шарафутдинов и др. – 2 015 137 548; заявл. 02.09.15; опубл. 05.07.2017, Бюл. № 19. – 10 с.

58. Пат. 2 603 848 РФ, МПК H 04 B 15/02. Способ резервирования плоских кабелей / Т.Р. Газизов, П.Е. Орлов, В.Р. Шарафутдинов и др. – 2 015 156 667 / 07; заявл. 28.12.15; опубл. 10.12.2016, Бюл. № 34. – 6 с.

59. Orlov P.E. Evaluation of efficiency of modal filtration in different types of redundant electrical connections / P.E. Orlov, T.R. Gazizov, E.N. Buichkin // International Siberian Conference on Control and Communications (SIBCON). – 2016. – P. 1–3. DOI: 10.1109/SIBCON.2016.7491786.

60. Orlov P.E. Method of lay-out of multilayer PCBs for circuits with redundancy / P.E. Orlov, E.N. Buichkin, T.T. Gazizov // The 17th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM). – 2016. – P. 155–158. DOI: 10.1109/EDM.2016.7538715.

61. Пат. 2 663 230 РФ, МПК H 04 B 15/02. Способ трехкратного резервирования цепей в многослойных печатных платах / Т.Р. Газизов, П.Е. Орлов, В.Р. Шарафутдинов. – 2 017 113 045; заявл. 14.04.17; опубл. 02.08.2018, Бюл. № 22. – 8 с.

62. Пат. 2 738 955 РФ, МПК H 04 B 15/02. Способ трёхкратного резервирования межсоединений / Т.Р. Газизов, А.В. Медведев, В.Р. Шарафутдинов. – 2 019 138 502; заявл. 27.11.19; опубл. 21.12.2020, Бюл. № 36. – 8 с.

63. Methods for increasing noise immunity of radio electronic systems with redundancy / P.E. Orlov, A.V. Medvedev, V.R. Sharafutdinov, T.R. Gazizov, A.V. Ubaichin // Journal of Physics: Conference Series. – 2018. – Vol. 1015, No. 5. – P. 052022. DOI: 10.1088/1742-6596/1015/5/052022.

64. Пат. 2 751 672 РФ, МПК H 04 B 15/02, H 01 P 11/00. Способ компоновки печатных проводников для цепей с модальным резервированием / Т.Р. Газизов, Е.С. Жечев, А.О. Белоусов и др. – 2 020 126 549; заявл. 10.08.20; опубл. 15.07.2021, Бюл. № 20. – 9 с.

65. Пат. 2 754 078 РФ, МПК H 04 B 15/02, H 05 K 3/00. Способ компоновки многослойных печатных плат для цепей с резервированием / Т.Р. Газизов, А.В. Медведев и др. – 2 020 122 293; заявл. 06.07.20; опубл. 26.08.2021, Бюл. № 24. – 7 с.

66. Sharafutdinov V.R. Using Modal Reservation for Ultrashort Pulse Attenuation After Failure / V.R. Sharafutdinov, A.V. Medvedev // International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). – 2019. – P. 0293–0296. DOI: 10.1109/SIBIRCON48586.2019.8958018.

67. Medvedev A.V. Evaluating modal reservation efficiency before and after failure / A.V. Medvedev, T.R. Gazizov, Y.S. Zhechev // Journal of Physics: Conference Series. – 2020. – Vol. 1488, No. 1. – P. 012015. DOI: 10.1088/1742-6596/1488/1/012015.

68. Medvedev A.V. Analysis of frequency characteristics of a structure with single modal reservation before and after failure / A.V. Medvedev, Y.S. Zhechev // Journal of Physics: Conference Series. – 2020. – Vol. 862, No. 2. – P. 022037. DOI: 10.1088/1757-899x/862/2/022037.

69. Medvedev A.V. Experimental Study of a Structure With Single Modal Reservation Before and After Failure / A.V. Medvedev, Y.S. Zhechev, T.R. Gazizov // IEEE Transactions on Electromagnetic Compatibility. – 2022. – Vol. 64, No. 4. – P. 1171–1181. DOI: 10.1109/TEMC.2022.3171770.

70. Medvedev A.V. Studying the switching order for a three-wire structure with modal reservation after failures. – Journal of Physics: Conference Series. – 2020. – Vol. 919, No. 5. – P. 052022. DOI: 10.1088/1757-899x/919/5/052022.

71. Medvedev A.V. Studying the circuit switching order after failures for a shielded structure with triple modal reservation / A.V. Medvedev, T.R. Gazizov // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – 2021. – P. 0427–0430. DOI: 10.1109/USBEREIT51232.2021.9455028.

72. Switching Order after Failures in Symmetric Protective Electrical Circuits with Triple Modal Reservation / A.O. Belousov, A.V. Medvedev, E.B. Chernikova, T.R. Gazizov, A.M. Zabolotsky // Symmetry. – 2021. – Vol. 13, No. 6. – P. 1074. DOI: 10.3390/sym13061074.

73. Пат. 2 770 516 РФ, МПК H 04 B 15/02. Способ переключения цепей с двукратным резервированием после

отказов / Т.Р. Газизов, А.В. Медведев. – 2 021 115 974; заявл. 03.06.21; опубл. 18.04.2022, Бюл. № 11. – 7 с.

74. Пат. 2 767 190 РФ, МПК H 02 H 3/05. Способ переключения цепей с трехкратным резервированием после отказов / Т.Р. Газизов, А.В. Медведев и др. – 2 021 116 338; заявл. 07.06.21; опубл. 16.03.2022, Бюл. № 8. – 7 с.

75. Using N-norms for analysing a device with a single modal reservation / Y.S. Zhechev, A.V. Zhecheva, A.V. Medvedev, T.R. Gazizov // Journal of Physics: Conference Series. – 2020. – Vol. 1611, No. 1. – P. 012065. DOI: 10.1088/1742-6596/1862/1/012003.

76. Gazizov R.R. Using Portraits of N-Norms for Large-Scale Investigation of Circuits with Modal Reservation / R.R. Gazizov, A.V. Medvedev, T.R. Gazizov // Dynamics of Systems, Mechanisms and Machines (Dynamics). – 2021. – P. 1–4. DOI: 10.1109/Dynamics52735.2021.9653464.

77. Using N-norms for analyzing symmetric protective electrical circuits with triple modal reservation / Y.S. Zhechev, A.V. Zhecheva, A.A. Kvasnikov, A.M. Zabolotsky // Symmetry. – 2021. – Vol. 13, No. 12. – P. 2390. DOI: 10.3390/sym 13122390.

78. Demakov A.V. Improved TEM-cell for EMC tests of integrated circuits / A.V. Demakov, M.E. Komnatnov // IEEE International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). – 2017. – P. 399–402. DOI: 10.1109/SIBIRCON.2017.8109915.

79. Пат. 2 727 075 РФ, МПК H 01 P 1/00. ТЕМ-камера для оценки помехоэмиссии и помехоустойчивости интегральных схем / Т.Р. Газизов, А.В. Демаков, М.Е. Комнатнов. – 2 019 140 183; заявл. 09.12.19; опубл. 17.07.2020, Бюл. № 20. – 12 с.

80. Пат. 2 606 173 РФ, МПК H 01 P 1/00. ТЕМ-Камера / Т.Р. Газизов, М.Е. Комнатнов. – 2 015 156 668; заявл. 28.12.15; опубл. 10.01.2017, Бюл. № 1. – 15 с.

81. Hasan A.A. Frequency Characteristics of PCB with Modal Reservation before and after Failure Using TALGAT / A.A. Hasan, T.R. Gazizov // IEEE 23rd International Conference of Young Professionals in Electron Devices and Materials (EDM). – 2022. – P. 140–146. DOI: 10.1109/EDM55285.2022.9855089.

Алхадж Хасан Аднан
Аспирант каф. телевидения и управления (ТУ)
Томского государственного университета
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0001-7403-7023
Тел.: +7-996-957-97-63
Эл. почта: alhaj.hasan.adnan@yandex.ru

Газизов Тальгат Рашитович
Д-р техн. наук каф. ТУ ТУСУРа
Ленина пр-1, 40, г. Томск, Россия, 634050
ORCID: 0000-0002-1192-4853
Тел.: +7-913-826-07-24
Эл. почта: talgat@tu.tusur.ru

Alhaj Hasan A., Gazizov T.R.

A review of studies on modal reservation

A growing number and increasing complexity of radioelectronic devices leads to the need to protect them from interference and enhance their reliability. There are many methods to ensure this, and they differ in capability, efficiency, and ease of implementation. Among these methods, a modal reservation (MR) is one of the most effective, reliable, and uncomplicated methods currently in use. Using this method in PCB tracing and assembling ensures both electromagnetic compatibility and reliability of the final electronic device. Much research has been performed on the study and development of MR, including 18 patents for inventions. However, there is still no a complete and extensive review of this method in order to perform research based on it. Therefore, this article presents a review of history and recent research on MR to identify the possibility of making various prototypes of MR-based structures. These structures could be used for experimental studies to estimate the level of radiated emissions in the frequency range, including the situations when the temperatures are extreme. In the conclusion, the main advantages of MR are summarized for the first time.

Keywords: redundancy, modal reservation, modal filtering, electromagnetic compatibility, electromagnetic interference, radiated emissions, transmission lines, printed circuit board.
DOI: 10.21293/1818-0442-2022-25-4-54-67

References

1. Trivedi K., Bobbio A. *Reliability and Availability Engineering: Modeling, Analysis, and Applications*. Cambridge. Cambridge University Press, 2017. 712 p. DOI: 10.1017/9781316163047.

2. Amari S.V., Dill G. Redundancy optimization problem with warm-standby redundancy. *Annual Reliability and Maintainability Symposium (RAMS)*, 2010, pp. 1–6. DOI: 10.1109/RAMS.2010.5448068.

3. Kuo S.V.W., Prasad V.R., Tillman F.A., Hwang C.L. *Optimal Reliability Design: Fundamentals and Applications*. Cambridge. Cambridge University Press, 2001, 412 p.

4. Von Neumann J. *Probabilistic logics and the synthesis of reliable organisms from unreliable components*. Automata Studies, Princeton University Press, 1956, pp. 43–98.

5. Chen D.M. *Satellite engineering series: communications satellite payload technology*. China Astronautic Publishing House, 2001.

6. Coit D.W. Maximization of System Reliability with a Choice of Redundancy Strategies. *IIE Transactions*, 2003, vol. 35, pp 535–543. DOI: /10.1080/07408170304420.

7. Grida M., Zaid A., Kholief G. Repairable 3-out-of-4: Cold standby system availability. *Annual Reliability and Maintainability Symposium (RAMS)*, 2017, pp. 1–6. DOI: 10.1109/RAM.2017.7889797.

8. Lobur M., Stefanovych T., Shcherbovskykh S. Modelling of type I and II errors of switching device for systems with hot and cold redundancy based on two-terminal dynamic fault tree. *The 14th International Conference of The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, 2017, pp. 19–21. DOI: 10.1109/CADSM.2017.7916075.

9. Li Y., Zhang Y., Cao R., Liu X., Lv C., Liu J. Redundancy design of modular DC solid-state transformer based on reliability and efficiency evaluation. *CPSS Transactions on Power Electronics and Applications*, 2021, vol. 6, no. 2, pp. 115–126. DOI: 10.24295/CPSSTPEA.2021.00010.

10. Sankaraiah G., Raghunatha Reddy Y., Umasankar C., Sarma B. D. Design and optimization of an Integrated Reliability redundancy system with multiple constraints. *The 2nd International Conference on Reliability, Safety and Hazard - Risk-Based Technologies and Physics-of-Failure Methods (ICRESH)*, 2010, pp. 118–122. DOI: 10.1109/ICRESH.2010.5779527.

11. Pan D. Study on Optimization of System Reliability Redundancy Based on Hybrid Intelligent Algorithm. *The In-*

ternational Conference on Environmental Science and Information Application Technology, 2009, pp. 560–563. DOI: 10.1109/ESIAT.2009.426.

12. Boland P.J., El-Neweihi E. Component redundancy vs system redundancy in the hazard rate ordering. *IEEE Transactions on Reliability*, 1995, vol. 44, no. 4, pp. 614–619. DOI: 10.1109/24.475980.

13. Shcherbovskykh S., Stefanovych T. Modelling features of type I and II errors of switching device for system with double hot and double cold redundancy based on two-terminal dynamic fault tree. *The 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, 2018, pp. 753–756. DOI: 10.1109/TCSET.2018.8336309.

14. Neves F.G.R., Saotome O. Comparison between Redundancy Techniques for Real Time Applications. *The fifth International Conference on Information Technology: New Generations (ITNG)*, 2008, pp. 1299–1300. DOI: 10.1109/ITNG.2008.229.

15. Peterson W., Weldon E. *Error-Correcting Codes*. Cambridge, MA: MIT Press, 1972, 576 p.

16. Zhu X. et al. Memristive Stateful Logic with N-Modular Redundancy Error Correction Design towards High Reliability. *The 5th IEEE Electron Devices Technology & Manufacturing Conference (EDTM)*, 2021, pp. 1–3. DOI: 10.1109/EDTM50988.2021.9420918.

17. Sun Z., Ambrosi E., Bricalli A., Ielmini D. Logic Computing with Stateful Neural Networks of Resistive Switches. *Advanced Materials*, 2018, vol. 30, no. 38, pp. 1–8. DOI: 10.1002/adma.201802554.

18. Hansen P., Linton M., Mayo R., Murphy M., Patterson D. A performance evaluation of the Intel iAPX 432. *SIGARCH Computer Architecture News*, 1982, vol. 10, no. 4, pp. 17–26. DOI: 10.1145/641542.641545.

19. Namazi A., Nourani M. Gate-Level Redundancy: A New Design-for-Reliability Paradigm for Nanotechnologies. *IEEE Transactions on Very Large-Scale Integration (VLSI) Systems*, 2010, vol. 18, no. 5, pp. 775–786. DOI: 10.1109/TVLSI.2009.2016206.

20. Xiong X., Zhao H.T., Hu T.B. Research on Redundancy Solution of Satellite Transponders Based on Reliability Analysis. *The International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE)*, 2019, pp. 689–694. DOI: 10.1109/QR2MSE46217.2019.9021237.

21. Sklaroff J.R. Redundancy Management Technique for Space Shuttle Computers. *IBM Journal of Research and Development*, 1976, vol. 20, no. 1, pp. 20–28. DOI: 10.1147/rd.201.0020.

22. Xiao C., Deng L. Reliability Research on Airborne Dual Redundancy of Electrical Wiring Interconnection System. *The 11th International Symposium on Computational Intelligence and Design (ISCID)*, 2018, pp. 137–140. DOI: 10.1109/ISCID.2018.10132.

23. Zhang D., Zhao M., Cheng E., Chen Y. GPR-Based EMI Prediction for UAV's Dynamic Datalink. *IEEE Transactions on Electromagnetic Compatibility*, 2021, vol. 63, no. 1, pp. 19–29. DOI: 10.1109/TEMC.2020.3000919.

24. Rentschler M., Laukemann P. Performance analysis of parallel redundant WLAN. *Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012)*, 2012, pp. 1–8. DOI: 10.1109/ETFA.2012.6489647.

25. Slee D., Stepan J., Wei W., Swart J. Introduction to printed circuit board failures. *IEEE Symposium on Product Compliance Engineering*, 2009, pp. 1–8. DOI: 10.1109/PSES.2009.5356012.

26. Labib M.G., et al. Heterogeneous Redundancy for PCB Track Failures: An Automotive Example. *The 14th International Conference on Computer Engineering and Systems (ICCES)*, 2019, pp. 189–194. DOI: 10.1109/ICCES48960.2019.9068123.

27. Chen H.C., Bai Y.W. Improvement of High-Current Density PCB Design with PSU Load Balance and Redundancy on a High-End Server System. *Canadian Journal of Electrical and Computer Engineering*, 2014, vol. 37, no. 4, pp. 203–211. DOI: 10.1109/CJECE.2014.2327091.

28. Waes J.V., Vankeirsbilck J., Pissoort D., Boydens J. Functional safety standard's techniques and measures in light of electromagnetic interference. *XXVI International Scientific Conference Electronics (ET)*, 2017, pp. 1–4. DOI: 10.1109/ET.2017.8124403.

29. Pissoort D., Armstrong K. Why is the IEEE developing a standard on managing risks due to EM disturbances?. *IEEE International Symposium on Electromagnetic Compatibility (EMC)*, 2016, pp. 78–83. DOI: 10.1109/ISEMC.2016. 7571612.

30. Waes J.V., Vanoost D., Vankeirsbilck J., Lannoo J., Pissoort D., Boydens J. Resilience of Error Correction Codes Against Harsh Electromagnetic Disturbances: Fault Mechanisms. *IEEE Transactions on Electromagnetic Compatibility*, 2020, vol. 62, no. 4, pp. 1017–1027. DOI: 10.1109/TEMC.2019.2931369.

31. Luo S., Batarseh I. A review of distributed power systems. Part II. High frequency AC distributed power systems. *IEEE Aerospace and Electronic Systems Magazine*, 2006, vol. 21, no. 6, pp. 5–14. DOI: 10.1109/MAES.2006.1662037.

32. Pissoort D., Lannoo J., Waes J.V., Degraeve A., Boydens J. Techniques and measures to achieve EMI resilience in mission- or safety-critical systems. *IEEE Electromagnetic Compatibility Magazine*, 2017, vol. 6, no. 4, pp. 107–114. DOI: 10.1109/MEMC.0.8272297.

33. Lannoo J., Degraeve A., Vanoost D., Boydens J., Pissoort D. Study on the use of different transmission line termination strategies to obtain EMI-diverse redundant systems. *IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*, 2018, pp. 210–215. DOI: 10.1109/ISEMC.2018.8393768.

34. Mora N., Vega F., Lugrin G., Rachidi F., Rubinstein M. Study and Classification of Potential IEMI Sources. *System Design and Assessment Notes*, 2014, pp. 1–43.

35. Gazizov T.R., Zabolotsky A.M. New approach to EMC protection. *The 18th International Zurich Symposium on Electromagnetic Compatibility*, 2007, pp. 273–276. DOI: 10.1109/EMCZUR.2007.4388248.

36. Orlov P.E., Gazizov T. R. Contactless Modal Phenomena Based Approach to Detecting, Identifying, and Diagnosing of Electrical Connections. *Complexity*, 2018, vol. 2018. p. 5081684. DOI: 10.1155/2018/5081684.

37. Orlov P.E., Medvedev A.V., Sharafutdinov V.R., Kalimulin I.F. Quasistatic simulation of ultrashort pulse propagation in the spacecraft autonomous navigation system circuit with modal reservation. *International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)*, 2017, pp. 495–500. DOI: 10.1109/SIBIRCON.2017.8109935.

38. Orlov P.E., Medvedev A.V., Sharafutdinov V.R. Quasistatic Simulation of Ultrashort Pulse Propagation in the Spacecraft Autonomous Navigation System Power Circuit with Modal Reservation. *The 19th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM)*, 2018, pp. 1–6. DOI: 10.1109/EDM.2018.8435026.

39. Orlov P.E., Buichkin E.N., Belousov A.O., Gazizov T.R. Method of lay-out of a multilayer PCB for circuits with triple reservation. *International Siberian Conference on Control and Communications (SIBCON)*, 2017, pp. 1–4. DOI: 10.1109/SIBCON.2017.7998528.

40. Belousov A.O., Chernikova E.B., Samoylichenko M.A., Medvedev A.V., Nosov A.V., Gazizov T.R., Zabolotsky A.M. From Symmetry to Asymmetry: The Use of Additional Pulses to Improve Protection against Ultrashort Pulses Based on Modal Filtration. *Symmetry*, 2020, vol. 12, no. 7, p. 1117. DOI: 10.3390/sym12071117.

41. Orlov P.E., Buichkin E.N. Quasistatic and electromagnetic simulation of interconnects of printed circuit boards with modal reservation. *The 18th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM)*, 2017, pp. 54–58. DOI: 10.1109/EDM.2017.7981707.

42. Orlov P.E., Gazizov T.R., Sharafutdinov V.R., Kalimulin I.F. Optimization of stack parameters of multi-layer PCB for circuits with redundancy by genetic algorithm. *International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)*, 2017, pp. 463–467. DOI: 10.1109/SIBIRCON.2017.8109928.

43. Hasan A.A., Kvasnikov A.A., Gazizov T.R. Approach to Estimation of Radiated Emission from Circuits with Modal Reservation. *The 21st International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM)*, 2020, pp. 169–173. DOI: 10.1109/EDM 49804.2020.9153498.

44. Hasan A.A., Gazizov T.R. Estimation of the Radiated Emission from a Single and Coupled Wires with Insulation above the Ground Plane. *IEEE 22nd International Conference of Young Professionals in Electron Devices and Materials (EDM)*, 2021, pp. 149–152. DOI: 10.1109/EDM52169.2021.9507613.

45. Hasan A.A., Zhechev Y.S., Gazizov T.R. Estimation of radiated emissions from a structure with a single modal reservation. *Journal of Physics: Conference Series*, 2021, vol. 1862, no. 1, p. 012003. DOI: 10.1088/1742-6596/1862/1/012003.

46. Hasan A.A., Gazizov T.R. Comparing the Estimates of the Radiated Emission from a Structure with Modal Reservation by Two Approaches. *IEEE 22nd International Conference of Young Professionals in Electron Devices and Materials (EDM)*, 2021, pp. 145–148. DOI: 10.1109/EDM52169.2021.9507636.

47. Gazizov T.R., Orlov P.E., SHarafutdinov V.R., Kuznetsova-Tadzhibaeva O.L., Zabolotskij A.M., Kuksenko S.P., Buichkin E.N. *Sposob trassirovki pechatnyh provodnikov tsepej s rezervirovaniem* [Method of routing printed conductors of circuits with redundancy] Patent RF, no. 2603850, 2016 (in Russ).

48. Gazizov T.R., Orlov P.E., SHarafutdinov V.R., Kuznetsova-Tadzhibaeva O.L., Zabolotskij A.M., Kuksenko S.P., Buichkin E.N. *Sposob trassirovki pechatnyh provodnikov s dopolnitelnym dielektrikom dlya tsepej s rezervirovaniem* [Method of routing printed conductors with additional dielectric for circuits with redundancy]. Patent RF, no. 2603851, 2016 (in Russ).

49. Gazizov T.R., Orlov P.E., Sharafutdinov V.R., Kuznetsova-Tadzhibaeva O.L., Zabolotskij A.M., Kuksenko S.P., Buichkin E.N. *Sposob rezervirovaniya dlya pechatnyh plat* [Reservation method for printed circuit boards]. Patent RF, no. 2603843, 2016 (in Russ).

50. Samoilichenko M., Gazizov T.R. *Sposob trassirovki dvuhstoronnej pechatnoj platy dlya tsepej s modalnym rezervirovaniem* [Method for tracing a double-sided printed board for circuits with modal redundancy]. Patent RF, no. 2762336, 2021 (in Russ.).

51. Belousov A.O., Chernikova E., Gazizov T.R. *Sposob odnokratnogo modalnogo rezervirovaniya mezhsoedinenij* [Method of single modal backup of interconnections]. Patent RF, no. 2732607, 2020 (in Russ.).

52. Medvedev A.V., Gazizov T.R. *Sposob trassirovki pechatnyh provodnikov s dopolnitelnym dielektrikom dlya tsepej s dvukratnym rezervirovaniem* [Method for routing printed conductors with additional dielectric for dual redundancy circuits]. Patent RF, no. 2752232, 2021 (in Russ.).

53. Medvedev A.V., Alhaj Hasan A., Kuznetsova-Tadzhibaeva O.L., Gazizov T.R. *Sposob trassirovki pechatnyh provodnikov na dvuslojnoj pechatnoj plate dlya tsepej s rezervirovaniem* [Method for routing printed conductors on two-layered printed circuit board for circuits with redundancy]. Patent RF, no. 2752233, 2021 (in Russ.).

54. Medvedev A.V., Kuznetsova-Tadzhibaeva O.L., Gazizov T.R. *Sposob trassirovki pechatnyh provodnikov tsepej pitaniya s rezervirovaniem* [Method for routing conductor strips of redundant power circuits]. Patent RF, no. 2779536, 2022 (in Russ.).

55. Gazizov T.R., Orlov P.E., SHarafutdinov V.R., Kuznetsova-Tadzhibaeva O.L., Zabolotskij A.M., Kuksenko S.P., Buichkin E.N. *Sposob komponovki pechatnyh plat dlya tsepej s rezervirovaniem* [Printed circuit boards with reserve circuits arrangement method]. Patent RF, no. 2614156, 2017 (in Russ.).

56. Sharafutdinov V.R., Orlov P.E., Gazizov T.R. *Sposob komponovki neformovannyh radioelektronnyh komponentov na pechatnyh platah dlya tsepej s rezervirovaniem* [Method of assembling non-molded radioelectronic components on printed circuit boards for circuits with redundancy]. Patent RF, no. 2693838, 2019 (in Russ.).

57. Gazizov T.R., Orlov P.E., Sharafutdinov V.R., Kuznetsova-Tadzhibaeva O.L., Zabolotskij A.M., Kuksenko S.P., Buichkin E.N. *Sposob vnutrennej komponovki pechatnyh plat dlya tsepej s rezervirovaniem* [Printed circuit boards with reserve circuits arrangement method]. Patent RF, no. 624637, 2017 (in Russ).

58. Gazizov T.R., Orlov P.E., Sharafutdinov V.R., Kuznetsova-Tadzhibaeva O.L., Zabolotskij A.M., Kuksenko S.P., Buichkin E.N. *Sposob rezervirovaniya ploskih kabelej* [Method of flat cables backing up]. Patent RF, no. 2603848, 2016 (in Russ.).

59. Orlov P.E., Gazizov T.R., Buichkin E.N. Evaluation of efficiency of modal filtration in different types of redundant electrical connections. *International Siberian Conference on Control and Communications (SIBCON)*, 2016, pp. 1–3. DOI: 10.1109/SIBCON.2016.7491786.

60. Orlov P.E., Buichkin E.N., Gazizov T.T. Method of lay-out of multilayer PCBs for circuits with redundancy. *The 17th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM)*, 2016, pp. 155–158. DOI: 10.1109/EDM.2016.7538715.

61. Gazizov T.R., Orlov P.E., Sharafutdinov V.R. *Sposob trekhkratnogo rezervirovaniya tsepej v mnogoslojnyh pechatnyh platah* [Method of circuit triple reservation in multilayered printed circuit boards]. Patent RF, no. 2663230, 2018 (in Russ.).

62. Sharafutdinov V.R., Gazizov T.R., Medvedev A.V. *Sposob tryohkratnogo rezervirovaniya mezhsoedinenij* [Method of triple backup of interconnections]. Patent RF, no. 2738955, 2020 (in Russ.).

63. Orlov P.E., Medvedev A.V., Sharafutdinov V.R., Gazizov T.R., Ubaichin A.V. Methods for increasing noise immunity of radio electronic systems with redundancy. *Journal of Physics: Conference Series*, 2018, vol. 1015, no. 5, p. 052022. DOI: 10.1088/1742-6596/1015/5/052022.

64. Zhechev E.S., Belousov A.O., Gazizov T.R., Zabolotskii A.M., Chernikova E.B. *Sposob komponovki pechatnyh provodnikov dlya tsepej s modalnym rezervirovaniem* [Method for arranging printed conductors for circuits with modal redundancy]. Patent RF, no. 2751672, 2021 (in Russ.).

65. Medvedev A.V., Kuznetsova-Tadzhibaeva O.L., Gazizov T.R. *Sposob komponovki mnogoslojnyh pechatnyh plat dlya tsepej s rezervirovaniem* [Method for arranging multilayer PCB for redundant circuits]. Patent RF, no. 2754078, 2021 (in Russ.).

66. Sharafutdinov V.R., Medvedev A.V. Using Modal Reservation for Ultrashort Pulse Attenuation After Failure. *International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)*, 2019, pp. 0293–0296. DOI: 10.1109/SIBIRCON48586.2019.8958018.

67. Medvedev A.V., Gazizov T.R., Zhechev Y.S. Evaluating modal reservation efficiency before and after failure. *Journal of Physics: Conference Series*, 2020, vol. 1488, no. 1, p. 012015. DOI: 10.1088/1742-6596/1488/1/012015.

68. Medvedev A.V., Zhechev Y.S. Analysis of frequency characteristics of a structure with single modal reservation before and after failure. *Journal of Physics: Conference Series*, 2020, vol. 862, no. 2, p. 022037. DOI: 10.1088/1757-899x/862/2/022037.

69. Medvedev A.V., Zhechev Y.S., Gazizov T.R. Experimental Study of a Structure with Single Modal Reservation Before and After Failure. *IEEE Transactions on Electromagnetic Compatibility*, 2022, vol. 64, no. 4, pp. 1171–1181. DOI: 10.1109/TEMC.2022.3171770.

70. Medvedev A.V. Studying the switching order for a three-wire structure with modal reservation after failures. *Journal of Physics: Conference Series*, 2020, vol. 919, no. 5, p. 052022. DOI: 10.1088/1757-899x/919/5/052022.

71. Medvedev A.V., Gazizov T.R. Studying the circuit switching order after failures for a shielded structure with triple modal reservation. *Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, 2021, pp. 0427–0430. DOI: 10.1109/USBEREIT 51232.2021.9455028.

72. Belousov A.O., Medvedev A.V., Chernikova E.B., Gazizov T.R., Zabolotsky A.M. Switching Order after Failures in Symmetric Protective Electrical Circuits with Triple Modal Reservation. *Symmetry*, 2021, vol. 13, no. 6, p. 1074. DOI: 10.3390/sym13061074.

73. Medvedev A.V., Gazizov T.R. *Sposob pereklyucheniya tsepej s dvukratnym rezervirovaniem posle otkazov* [Method for switching circuits with double redundancy after failures]. Patent RF, no. 2770516, 2022 (in Russ.).

74. Medvedev A.V., Gazizov T.R., Zabolotskii A.M. *Sposob pereklyucheniya tsepej s trekhkratnym rezervirovaniem posle otkazov* [Method for switching circuits with triple redundancy after failures]. Patent RF, no. 2767190, 2022 (in Russ.).

75. Zhechev Y.S., Zhecheva A.V., Medvedev A.V., Gazizov T.R. Using N-norms for analyzing a device with a single modal reservation. *Journal of Physics: Conference Series*, 2020, vol. 1611, no. 1, p. 012065. DOI: 10.1088/1742-6596/1862/1/012003.

76. Gazizov R.R., Medvedev A.V., Gazizov T.R. Using Portraits of N-Norms for Large-Scale Investigation of Circuits with Modal Reservation. *Dynamics of Systems, Mechanisms and Machines (Dynamics)*, 2021, pp. 1–4. DOI: 10.1109/Dynamics52735.2021.9653464.

77. Zhechev Y.S., Zhecheva A.V., Kvasnikov A.A., Zabolotsky A.M. Using N-norms for analyzing symmetric protective electrical circuits with triple modal reservation. *Symmetry*, 2021, vol. 13, no. 12, p. 2390. DOI: 10.3390/sym13122390.

78. Demakov A.V., Komnatnov M.E. Improved TEM-cell for EMC tests of integrated circuits. *IEEE International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)*, 2017, pp. 399–402. DOI: 10.1109/SIBIRCON.2017.8109915.

79. Gazizov T.R., Demakov A.V., Komnatnov M.E. *TEM-kamera dlya otsenki pomekhoemissii i pomekhoustojchivosti integralnyh skhem* [TEM Test Cell for Estimating Noise Emission and Noise Immunity of Integrated Circuits]. Patent RF, no. 2727075, 2020 (in Russ.).

80. Komnatnov M.E., Gazizov T.R. *TEM-kamera* [TEM Chamber]. Patent RF, no. 2606173, 2017 (in Russ).

81. Hasan A.A., Gazizov T.R. Frequency Characteristics of PCB with Modal Reservation before and after Failure Using TALGAT. *IEEE 23rd International Conference of Young Professionals in Electron Devices and Materials (EDM)*, 2022, pp. 140–146. DOI: 10.1109/EDM55285.2022.9855089.

Adnan Alhaj Hasan
Postgraduate student, Department of Television and Control,
Tomsk State University of Control Systems
and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0001-7403-7023
Phone: +7-996-957-97-63
Email: alhaj.hasan.adnan@yandex.ru

Talgat Rashitovich Gazizov
Doctor of Science in Engineering,
Department of Television and Control, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0002-1192-4853
Phone: +7-913-826-07-24
Email: talgat@tu.tusur.ru

УПРАВЛЕНИЕ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА

УДК 004.023+004.413+004.891

К.В. Попов, П.А. Шелупанова

Информационные системы для анализа угроз национальной безопасности

Информационные технологии играют значительную роль в такой области знаний, которая получила название «вычислительная социальная наука» (computational social science). Разработка онлайн-технологий и цифровых методов исследований в предметных областях общественных наук связана с применением новых междисциплинарных подходов и интеграцией исследователей из различных областей знания. В качестве эффективного и перспективного инструмента для исследователей в области изучения насильственных идеологий, дестабилизирующих общественный строй, в статье рассматриваются примеры баз данных, сервисов и платформ для многомерного анализа. Обозначены возможности и ограничения настройки процесса сбора, обработки и представления данных. Представлен обзор специфических характеристик баз данных, сервисов и платформ, размещенных на веб-сайте исследовательского центра START. Сделаны выводы о том, какие возможности такого рода инструменты открывают для исследователей, и обозначены перспективы реализации наиболее интересных решений для совершенствования процесса автоматизации анализа данных.

Ключевые слова: национальная безопасность, экстремизм, терроризм, радикализация, база данных, Web Mining, big data, исследовательские инструменты, управление.
DOI: 10.21293/1818-0442-2022-25-4-71-79

Возникновение насильственных идеологий связано с различными социальными, политическими и экономическими факторами, которые различаются от страны к стране и меняются со временем [1]. Общими угрозами национальной безопасности, независимо от страны, определяются угрозы терроризма, насильственного экстремизма.

В настоящее время в общественных науках сложилось более-менее единое мнение на природу экстремизма и терроризма, условия их возникновения, методы борьбы с ними и профилактику этих явлений. Значительных расхождений по данным вопросам в публикациях отечественных и зарубежных исследователей не прослеживается.

Поскольку термин «радикализация» используется слишком часто и попадает в различные риторические атрибуты, важно опираться на происхождение этого термина, которое связано со словом «корень», т.е. фундаментальным происхождением идеи или причиной. Таким образом, радикализация в своем эпистемологическом смысле означает привязку себя к своим знаниям, мнениям, ценностям и убеждениям для определения своего поведения [2]. Поэтому мы не будем акцентировать свое внимание на отдельных незначительных расхождениях во взглядах на понятийный аппарат данной проблемы, а сформулируем устоявшееся общественное представление о природе экстремизма и терроризма.

Наиболее полное определение терроризму дал в своей работе Тодд Сандлер: «Терроризм – это преднамеренное применение или угроза применения насилия отдельными лицами или субнациональными группами для достижения политической или социальной цели путем запугивания большой аудитории, помимо непосредственных жертв» [3].

Терроризм, насильственный экстремизм имеют общий предиктор, о котором ученые заговорили еще в начале этого века. Предиктором инцидентов террористической и экстремистской направленности является радикализация. В самом общем виде под радикализацией понимается процесс перехода от ненасильственных форм выражения мнения к насильственным действиям. Насильственный экстремизм рассматривается как «поощрение, оправдание или поддержка совершения насильственного действия для достижения политической цели, идеологических, религиозных, социальных или экономических целей» [4]. Вопрос о том, как и почему одиночки, автономные ячейки, сообщества и целые движения радикализуются, осуществляя переход от насильственного экстремизма, преступлений на почве ненависти к терроризму, является актуальным в сегодняшней повестке обеспечения национальной безопасности как в России, так и во всем мире.

За прошедшие двадцать лет было много исследований, которые применяют эмпирические и теоретические методы изучения насильственных проявлений. Первым способствовала повышенная доступность данных о террористических событиях. В первую очередь, это разработки в области создания инновационных, совместимых между собой исследовательских инструментов и сервисов, которые облегчают поиск, добычу, аналитическое хранилище данных, позволяют заинтересованным субъектам решать сложные исследовательские задачи.

Например, это организации, которые занимались или продолжают заниматься сбором данных, способствуя работе аналитиков, политиков и практиков в понимании тенденций террористической деятельности. Наиболее известные из них – исследовательская организация RAND Corporation [5], Мемориальный институт по предотвращению терроризма (Memorial Institute for the Prevention of Terrorism (MIPT)) [6], Национальный консорциум по изучению терроризма и ответам на террористическую угрозу университета Мэриленд (National

Consortium for the Study of Terrorism and Responses to Terrorism University of Maryland (START)) [7], Национальный контртеррористический центр (The National Counterterrorism Center (NCTC)) [8], Канадская сеть исследований терроризма, безопасности и общества (Canadian network for research on terrorism, security and society (TSAS)) [9], Центр исследований экстремизма (Center for Research on Extremism (C-REX)) [10], Международный центр по борьбе с терроризмом – Гаага (International Centre for Counter-Terrorism, The Netherlands (ICCT)) [11], Международный центр по изучению радикализации (The International Centre for the Study of Radicalisation (ICSR)) [12], Центр изучения терроризма и политического насилия Ханда (The Handa Centre for the Study of Terrorism and Political Violence (CSTPV)) [13], Международный центр исследований терроризма (International Center for Terrorism Studies (ICTS)) [14], Международный центр исследований политического насилия и терроризма (International Centre for Political Violence and Terrorism Research (PSiS)) [15], Центр контртеррористических исследований китайских институтов современных международных отношений (China Institutes of Contemporary International Relations (CICIR)) [16] и др. [17].

Несмотря на то, что каждый центр имеет либо региональную, национальную или конкретную предметную специфику, общим для них является создание и использование баз данных для проведения исследований, касающихся установления рисков и уязвимостей, связанных с насильственным поведением. Собранные данные расширяют возможности исследователей выявлять атрибуты террористических событий, получать доступ к длинному набору данных (за большой временной период). Использование временных рядов и панелей оценки подкрепляет новые эмпирические исследования. Одна вещь остается неизменной в борьбе с терроризмом и насильственным экстремизмом – это информация о радикальных личностях, будь то личная, демографическая, социальная, экономическая или иная информация. Возможность идентифицировать, классифицировать и создавать профили потенциальных радикалов на основе такой информации привлекательна для аналитиков, исследователей, экспертов по всему миру.

Фундаментальные и прикладные научные исследования в цифровой среде привели к созданию новой области знаний, которая получила название «вычислительная социальная наука» (computational social science), которая основана на применении в социальных исследованиях нового поколения онлайн-технологий и цифровых методов исследований. Это опосредованные компьютерными технологиями методы сбора, анализа и обработки данных, которые обеспечивают большой методологический потенциал для исследований во всех областях общественных наук. Эта область знаний выстраивается на применении междисциплинарных подходов и методов, а также объединении специалистов предметной области, специалистов Data Science и поставщиков профессиональных услуг (разработчиков программного продукта) [18–20].

Для получения представления о существующей схеме работы по выявлению действий насильственной идеологии отобразим ее графически в виде нотаций IDEF0 на рис. 1.

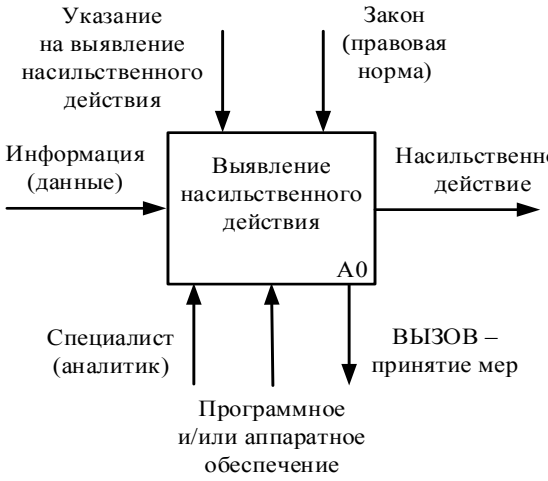


Рис. 1. Контекстная диаграмма процесса выявления насильственного действия

Входящая стрелка – «Информация» (сообщения средств массовой информации, в социальных сетях и мессенджерах). Управляющая – «Указание на выявление насильственных действий». Ограничительная – «Закон (правовая норма)». В роли «механизмов» выступают специалисты (силы) и программное и/или аппаратное обеспечение (средства). Аналитик в ходе своей деятельности получает классифицированный, стандартизированный продукт наполнения базы данных.

Несмотря на рост количества открытых сервисов для исследователей по всему миру в виде баз данных, существует ряд задач, которые до сих пор остаются нерешенными, вследствие чего набор данных по-прежнему дает нам лишь небольшой процент знаний. Условно такого рода задачи можно разделить на несколько уровней, отражающих весь процесс сбора, обработки и представления данных, влияющий на эффективность автоматизации процесса анализа.

Первый уровень. Задача создания архитектуры баз данных и комплектования функций прототипа для набора данных [21–23]. Часто применяются методы, позволяющие исследовать закономерности только по одному измерению за определенный временной промежуток. Например, данные могут быть изучены в хронологическом порядке, чтобы определить скорость изменений (меняющиеся временные тенденции). Данные также могут быть организованы географически путем создания картограммы или карты плотности (например, по конкретной стране/географические вариации) [24–26]. Данные также могут быть обобщены по целевым типам, чтобы понять характеристики инцидентов/измене-

ние характеристик [27, 28]. Например, разработчики глобальной базы данных о терроризме (The Global Terrorism Database™ (GTD)) [29] используют метод разбиения больших данных о террористических инцидентах на типы событий и предложили метод калибровки, который позволил выявлять потенциальные погрешности в GTD в результате недоучета или переучета террористических инцидентов. Эти же авторы применили методы векторной авторегрессии (vector autoregression – VAR) для исследования реакции, вызванной шоком, метод декомпозиции дисперсии (variance decomposition) и тесты на причинно-следственную связь по Грейнджеру (Granger-causality tests), расширив тем самым возможности аналитиков в работе с базой данных GTD [30, 31].

Второй уровень. Задача визуализации данных. Трудно визуализировать данные по нескольким параметрам (включая географию, время и несколько атрибутов) и представить их в доступной для понимания форме. Например, если исследователь хочет изучить пространственные вариации целевых кластеров или какие цели выбирают террористы в конкретной стране. Поэтому, чтобы получить полное представление о данных, необходимо визуализировать их с разных точек зрения и искать разные типы закономерностей.

Возможности для решения этой задачи открываются в применении многомерных пространственных моделей. Особой подзадачей визуализации данных становится многомерное картирование для создания единой среды визуализации, которая может гибко поддерживать визуализацию: пространственно-многомерных, пространственно-временных, временных многомерных и пространственно-временных многомерных моделей [32, 33]. Наиболее перспективными в многомерной визуализации на данный момент времени выделяются пиксельно-ориентированные подходы (pixel-oriented approaches). Это связано с возможностями их широкого использования.

Во-первых, они могут использоваться в качестве автономных инструментов исследования. Во-вторых, могут быть интегрированы в методы интеллектуального анализа данных, объединяя и усиливая существующие алгоритмы и участие человека. В-третьих, они могут быть использованы в кластеризации атрибутов по сходству для улучшения методов многомерной визуализации [34–37].

Помимо способности построить целостное визуальное представление сложных шаблонов базы данных, система многомерной визуализации поддерживает различные взаимодействия с пользователем, чтобы помочь аналитику понять закономерности. Многомерная система визуализации по своей природе относительно сложнее, чем традиционные подходы. В целом обозначенные выше подходы к моделированию основаны на строгих статистических или математических моделях, сформулированы с использованием априорных теоретических гипотез и откалиброваны с помощью данных наблюдений. Поэтому подходы, основанные на применении как визуальных, так и вычислительных методов, могут многое предложить при создании баз данных для изучения насильственных проявлений. Это позволит аналитикам выявлять неизвестные ранее тенденции или закономерности, таким образом побуждая к дальнейшим размышлениям и формулировке новых гипотез.

Третий уровень. Задачи интеллектуального анализа данных социальных медиа. За последнее десятилетие использование социальных сетей для распространения насильственных идеологий, дестабилизирующих общественный строй среди пользователей, резко возросло. Задача сбора информации из социальных сетей, даже при наличии ограничений, устанавливаемых провайдерами социальных сетей, является к настоящему моменту решенной благодаря разработкам и совершенствованию методов в области Web Mining. Проблема в качестве формализации переменных, кодировании исходных данных и точности установления корреляционной зависимости между значениями различных параметров.

Процесс интеллектуального анализа данных представим в виде блок-схемы на рис. 2.

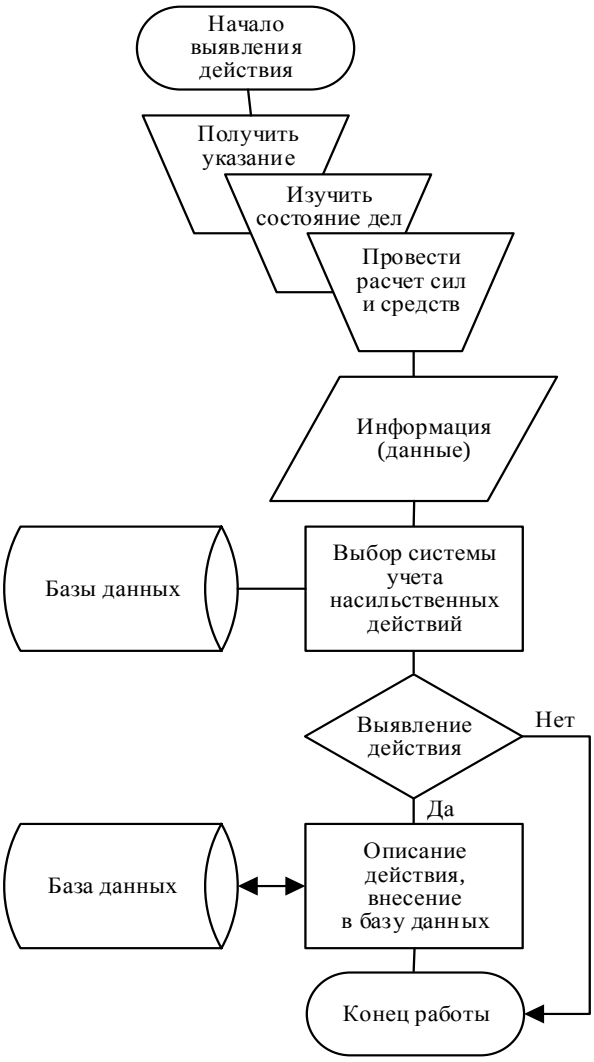


Рис. 2. Блок-схема выявления насильственного действия

Новые методы сбора данных предлагают огромные возможности, которые приводят к обработке все большего и большего количества геопространственных данных, а также связанной с ней увеличивающейся вычислительной нагрузкой. Анализ этих данных становится сложной задачей из-за размера наборов данных, их сложности, проблем с масштабированием и скрытых закономерностей. Применяемые на сегодняшний день статистические методы, искусственный интеллект (с использованием систем на основе правил и деревьев решений), искусственные нейронные сети представляют собой новое решение для анализа данных и распознавания образов. Среди моделей нейронных сетей самоорганизующаяся карта (SOM) часто рассматривается как многообещающий метод исследовательского анализа данных [24].

В качестве примеров рассмотрим несколько наиболее известных открытых баз данных, доступных исследователям со всего мира, обозначим их отличительные характеристики, а также аффилированные с базами данных инструменты и сервисы для анализа.

Одна из первых открытых баз данных – Всемирная система отслеживания инцидентов (Worldwide Incidents Tracking System (WITS)) [38] – начала формироваться в 2003 г. на базе Национального контртеррористического центра (The National Counterterrorism Center (NCTC)) [39]. Содержит информацию о глобальных насильственных экстремистских и террористических инцидентах с 2005 г.

База данных построена на основе переупорядочиваемой матрицы (reorderable matrices), т.е. организована как таблица данных с переменными в виде столбцов и элементами данных в виде строк. Каждый элемент данных (строка) имеет значение для каждой переменной (столбца). Переупорядочиваемая матрица может отсортировывать столбцы и строки так, чтобы похожие столбцы или похожие строки располагались рядом друг с другом.

Таким образом, появляются шаблоны для нескольких переменных и нескольких элементов данных. Значительные ограничения для аналитиков в работе с этой базой заключались в том, что в ней содержалась выборочная информация, не по всем странам. Кроме того, было ограниченное число переменных для анализа, соответственно, это ограничивало возможности прогнозировать тенденции в течение определенного периода времени. С 2012 г. WITS интегрирована в GTD.

GTD создана в 2005 г. на базе Национального консорциума по изучению терроризма и ответов на террористическую угрозу (National Consortium for the Study of Terrorism and Responses to Terrorism (START)) [40]. Представляет собой базу данных с открытым исходным кодом, включая информацию о террористических инцидентах по всему миру с 1970 по 2021 г. (с ежегодными обновлениями, запланированными на будущее). В отличие от многих других баз данных инцидентов GTD включает систематические данные о внутренних, а также международных террористических инцидентах, которые произошли в течение этого периода времени.

Содержит информацию по меньшей мере о 45 переменных для каждого инцидента, включая информацию о более чем 120 переменных. Более 100 структурированных переменных характеризуют местоположение, тактику, оружие, жертвы, пострадавших, а также общую информацию, такую как критерии определения и связи между скоординированными атаками. Это самая полная неклассифицированная база данных о террористических событиях в мире с открытым доступом. Но аналитикам, заинтересованным в работе с базой, открытый доступ предоставляется только по семи переменным (дата, регион, страна, преступные группы, оружие, тип атаки, цель атаки).

По остальным переменным можно получить данные только по запросу с обоснованием. Для того чтобы скачать данные и применить собственные параметры выборки, также необходимо прислать запрос с обоснованием и получить разрешение на использование данных. Файлы могут быть загружены непосредственно с веб-сайта START. Неструктурированные переменные включают краткое описание атак и более подробную информацию об используемом оружии, конкретных мотивах атакующих, имущественном ущербе и требованиях о выкупе (если применялся) [41].

Ключевые характеристики: информация из открытых источников, применение группы методов Web Mining (извлечение и уточнение знаний о людях, сообществах, структурах, системах, организациях, событиях, их взаимосвязях и взаимном влиянии), автоматический и полуавтоматический сбор данных, модели машинного обучения (ML), установленные правила кодирования (для оценки вкл./не вкл. инцидента в базу), критерии для переменных разработаны социологами, аналитика проводится рабочими группами.

Профили индивидуальной радикализации в США (Profiles of Individual Radicalization in the United States – PIRUS (Keshif)) [42]. PIRUS появилась в открытом доступе в 2014 г. Профили индивидуальной радикализации в наборе данных PIRUS содержат идентифицированную информацию по отдельным лицам: предыстории (предикторы процесса радикализации – формализованные переменные), атрибуты (неизменные признаки), фоновая аналитика (формализованные переменные) более 3000 насильственных и ненасильственных экстремистов. Самая большая открытая база данных в США и в мире. Она построена на изучении по четырем категориям идеологических платформ: крайне правые, крайне левые, исламисты, «одинокие волки».

Информация собирается только по экстремистам, радикализовавшимся в США, за период с 1948 г. по настоящее время (постоянно обновляется). В базе зашита обработанная информация, собранная из общедоступных источников информации. Персо-

нальные данные радикалов недоступны, им присвоен идентификационный номер. Создатели базы данных заявляют о 147 переменных, которые доступны для анализа. Но в открытом доступе для аналитиков представлена информация только по 49 переменным. Остальные доступны только по запросу с обоснованием. Инструмент (алгоритм) визуализации данных – Keshif – основан на использовании методов многомерной визуализации, таких как временная визуализация (temporal visualization), пиксельные методы (pixel-based techniques) и анимированные карты (animated maps). Агрегация и преобразование данных во всем наборе геокодирования трансформируются «на лету».

Матрица знаний I-VEO (I-VEO Knowledge Matrix) [43] (IVEO – Influencing Violent Extremist Organizations (влияние на воинствующие экстремистские организации)) – это пример сервиса, который адаптирован под кроссплатформенную интеграцию нескольких баз данных для решения исследовательских задач. Матрица появилась в 2011 г. как первая попытка синтезировать теоретические и эмпирические знания, накопленные в START об операциях влияния на воинствующие экстремистские организации.

Междисциплинарный проект, в который интегрированы специалисты из различных областей: политологии, криминологии, государственной политики, психологии, международных отношений и computer science. В качестве эмпирических данных в матрице I-VEO используются данные GTD и PIRUS. Проект по созданию матрицы направлен на то, чтобы объединить теоретические знания с эмпирически проверенными фактами. Матрица содержит 183 гипотезы о том, как влиять на VEO. Каждая гипотеза опирается на анализ качественных и/или количественных исследований. Для функциональности все гипотезы и связанные с ними обзоры литературы отсортированы по темам и могут быть заданы исследователями самостоятельно по нескольким схемам в соответствии с конкретными интересами.

Еще более широкие возможности для исследователей, аналитиков, практиков и заинтересованных лиц открываются на платформе базы данных о терроризме и экстремистском насилии в США (Terrorism and Extremist Violence in the United States (TEVUS) Database and Portal (TEVUS Portal)) [44, 45]. Этот новый инструмент для анализа терроризма и насильственного экстремизма базируется на интеграции информации из четырех баз данных: база данных американского исследования терроризма (American Terrorism Study (ATS)), GTD, база экстремистских преступлений (U.S. Extremist Crime Database (ECDB)), база профилей виновных в терроризме в Соединенных Штатах (Profiles of Perpetrators of Terrorism in the United States (PPT-US)).

Каждая из этих четырех баз данных имеет уникальные особенности как с точки зрения организации и интеграции в единое хранилище эмпирических данных, так и в возможностях многоуровневого представления данных, зашитых в интерфейс. На платформе TEVUS аккумулированы ключевые переменные (поведенческие, географические и временные характеристики) экстремистского насилия в Соединенных Штатах начиная с 1970 г. Через портал пользователи могут создавать поисковые запросы на основе четырех типов данных, включая конкретные события, исполнителей террористического акта или экстремистские преступления, группы и/или судебные дела, связанные с терроризмом и экстремистской преступностью в Соединенных Штатах. За счет интеграции такого массива данных из разных баз данных и разработки удобного веб-интерфейса для доступа к ним платформа TEVUS позволяет пользователям проводить многомерный анализ. Это самая полная база данных о терроризме и экстремистском насилии в Соединенных Штатах.

Все представленные примеры относятся только к одному исследовательскому центру START и имеют национальную специфику. Но именно эти образцы являются наиболее показательными в части организации сбора, обработки, хранения и анализа данных. На основе этих образцов в дальнейшем появились и, безусловно, будут появляться базы данных в разных регионах мира.

Примером обобщенного видения формирования базы данных является блок-схема выявления признаков насильственных действий, представленная на рис. 3.

Представленный обзор информационных систем страдает определенной неполнотой. В нем отсутствуют разработанные и используемые отечественные аналитические информационные системы, доступные в сегменте интернета.

Все поиски открытых баз данных в интересующей нас тематике не привели к положительному результату, хотя силовые структуры Российской Федерации, безусловно, не могут не использовать в своей деятельности по профилактике насильственных идеологий IT-разработки, связанные с формированием, созданием, построением подобных баз данных. Соответственно, не представляется возможным провести оценку ни функционала, ни содержания, ни алгоритмов, используемых в их работе.

Поэтому основное внимание в данной статье обращено на общедоступные базы данных, которые представляют исключительно зарубежные разработки.

Справедливости ради стоит отметить, что попытки создания подобных баз данных, размещенных в свободном доступе, предпринимались в нашей стране.

Информационно-аналитический центр «СОВА» (ИАЦ «СОВА») основан в октябре 2002 г. [46]. Сфера центра – проблемы национализма и ксенофобии, взаимоотношения религии и общества, политический радикализм. Статистику, собираемую по преступлениям ненависти и по антиэкстремистскому правоприменению, можно изучить в открытой базе данных. Данные о совершенных по мотиву ненависти насильственных преступлениях и актах ванда-

лизма (но не о пропагандистской деятельности), а также данные о приговорах по всем статьям УК, относящимся к «экстремистским», накапливаются в трех соответствующих базах данных. Данные систематически вводились с начала 2007 г. и доступны по месяц, закончившийся за 3 месяца до даты запроса. 30 декабря 2016 г. организация внесена в реестр некоммерческих организаций, выполняющих функции иностранного агента.

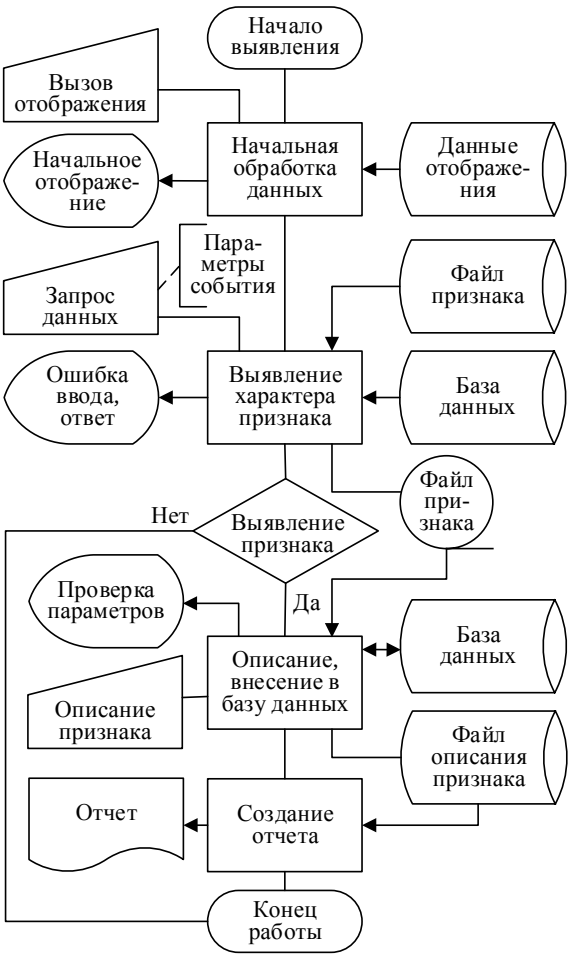


Рис. 3. Блок-схема выявления признаков насильственных действий

Основной недостаток ИАЦ «СОВА», не позволяющий ставить ее в один ряд с обозреваемыми зарубежными, – это отсутствие возможности формирования профиля нарушителя. Следовательно, о выявлении предпосылок возникновения угрозы насильственных актов, а также возможности предупреждения и профилактики этих явлений говорить не приходится.

Именно информационные технологии должны, на наш взгляд, кратно повысить эффективность работы по определению, выявлению и профилактике подобных угроз.

Выводы

В сегодняшней повестке ведется широкое обсуждение практических аспектов сбора данных в интернете как эффективном инструменте для исследований, позволяющем осуществлять быстрый и экономичный сбор данных, доступ к большим выборкам и различным группам населения. Преимущества, которые такой инструмент, как открытые базы данных, представляет для исследователей, заключаются в возможности интегрировать в единый репозиторий накопленный массив уже имеющихся данных, рассредоточенный по разным хранилищам. Это сократит время на поиск исследователями тематической и эмпирической информации.

Базы данных с заданными переменными позволяют исследователям практически мгновенно составить «картину» по заданным параметрам. Например, по конкретному лицу можно увидеть весь профиль с сопутствующими многомерными характеристиками. Кроме того, на материалах базы данных можно создать методологию исследования процесса, конкретного феномена, а также проводить сравнительный анализ сходств и различий проявлений и динамики процесса/феномена на региональном, федеральном, международном уровне. К тому же мы до конца не понимаем, что скрывается за «черным ящиком» алгоритмов описанных зарубежных баз данных в силу их недоступности.

В статье дан обзор существующего порядка вещей, обозначены проблемы и вызовы в стремлении систематизировать, структурировать, а далее автоматизировать систему анализа данных в нашей стране. Технически алгоритмы уже не представляют сложности, но должны быть адаптированы под конкретные задачи, диагностики, прогнозирования, предупреждения угроз и рисков национальной безопасности в Российской Федерации.

Статья подготовлена в рамках реализации программы ЛИЦ «Доверенные сенсорные системы» (договор № 009/20 от 10.04.2020) при финансовой поддержке Минкомсвязи России и АО «РВК». Идентификатор соглашения о предоставлении субсидии – 0000000007119P190002.

Литература

1. Попов К.В. Новые вызовы: стохастические угрозы национальной безопасности / К.В. Попов, А.А. Шелупанов // Доклады ТУСУР. – 2020. – Т. 23, № 4. – С. 23–29. DOI: 10.21293/1818-0442-2020-23-4-23-29.

2. Alava S. Youth and Violent Extremism on Social Media: Mapping the research / S. Alava, D. Frau-Meigs, G. Hassan // United Nations Educational, Scientific and Cultural Organization. – 2017. – URL: https://unesdoc.unesco.org/ark:/48223/pf0000260382 (дата обращения: 28.09.2022).

3. Sandler T. New frontiers of terrorism research: An introduction // Journal of Peace Research. – 2011. – Vol. 48, No. 3. – P. 279–286. DOI: 10.1177/0022343311399131.

4. Borum R. Radicalization into Violent Extremism I: A Review of Social Science Theories // Journal of Strategic Security. – 2011. – Vol. 4, No. 4. – P. 7–36.

5. RAND Corporation. – URL: https://www.rand.org/ (дата обращения: 28.09.2022).

6. Memorial Institute for the Prevention of Terrorism (MIPT). – URL: https://web.archive.org/web/20130620070250/https://www.mipt.org/Home.aspx (дата обращения: 28.09.2022).

7. National Consortium for the Study of Terrorism and Responses to Terrorism (START). – URL: https://www.start.umd.edu/ (дата обращения: 28.09.2022).

8. The National Counterterrorism Center (NCTC). – URL: https://www.dni.gov/index.php/nctc-newsroom/nctc-resources (дата обращения: 28.09.2022).

9. Canadian network for research on terrorism, security and society (TSAS). – URL: https://www.tsas.ca/ (дата обращения: 28.09.2022).

10. Center for Research on Extremism (C-REX). – URL: https://www.sv.uio.no/c-rex/english/ (дата обращения: 28.09.2022).

11. International Centre for Counter-Terrorism, The Netherlands (ICCT). – URL: https://icct.nl/ (дата обращения: 28.09.2022).

12. The International Centre for the Study of Radicalisation (ICSR). – URL: https://icsr.info/ (дата обращения: 28.09.2022).

13. The Handa Centre for the Study of Terrorism and Political Violence (CSTPV). – URL: https://cstpv.wp.st-andrews.ac.uk/ (дата обращения: 28.09.2022).

14. International Center for Terrorism Studies (ICTS). – URL: https://www.potomacinstitute.org/academic-centers/international-center-for-terrorism-studies-icts (дата обращения: 28.09.2022).

15. International Centre for Political Violence and Terrorism Research (PSiS). – URL: https://www.rsis.edu.sg/research/icpvtr/ (дата обращения: 28.09.2022).

16. China Institutes of Contemporary International Relations (CICIR). – URL: http://www.cicir.ac.cn/NEW/en-us/Institution.html?subtype=America&&type=region (дата обращения: 28.09.2022).

17. Freedman B. Terrorism Research Centres: 100 Institutes, Programs and Organisations in the Field of Terrorism, Counter-Terrorism, Radicalisation and Asymmetric Warfare Studies // Perspectives on Terrorism. – 2010. – Vol. 4, No. 5. – P. 48–56.

18. Ультраправая радикализация: методика автоматизированного выявления угроз методами web mining / А.Ю. Карпова, А.О. Савельев, А.Д. Вильнин, А.Ю. Кайда, С.А. Кузнецов, Н.Г. Максимова, Д.В. Чайковский // Вестник Российского фонда фундаментальных исследований. Гуманитарные и общественные науки. – 2020. – № 5 (102). – С. 30–43.

19. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

20. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях их возникновения / В.Г. Миронова, А.А. Шелупанов // Изв. Южного федерального ун-та. Технические науки. – 2012. – Т. 137, № 12. – С. 39–45.

21. The high-level overview of social media content search engine / A.O. Savelev, A.Yu. Karpova, D.V. Chaykovskiy, A.D. Vilnin, A.Yu. Kaida, S.A. Kuznetsov, L.O. Igumnov, N.G. Maksimova // Proceedings of the 14th International Forum on Strategic Technology (IFOST 2019). – Tomsk: Polytechnic University, 2019. – P. 306–309.

22. Лопарев С.А. Анализ инструментальных средств оценки рисков утечки информации в компьютерной сети предприятия / С.А. Лопарев, А.А. Шелупанов // Вопросы защиты информации. – 2003. – № 4(63). – С. 2–5.

23. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Н.Т. Югов // Доклады ТУСУР. – 2011. – № 2 (24), ч. 3. – С. 206–210.

24. Koua E.L. Using self - organizing maps for information visualization and knowledge discovery in complex geospatial datasets // In Proceedings of the 21st International Cartographic Conference (ICC) 10–16 Aug 2003. Durban. South Africa. – URL: https://webapps.itc.utwente.nl/library www/papers_2003/art_proc/koua.pdf (дата обращения: 28.09.2022).

25. Цифровизация финансово-кредитной сферы в современной России / Е.В. Агеева, М.А. Афанасова, А.С. Баландина [и др.]; под общ. ред. М.Г. Жигас, А.А. Шелупанова. – Москва; Берлин: Директ-Медиа, 2019. – 408 с. – URL: https://biblioclub.ru/index.php?page=book&id=565080 (дата обращения: 30.09.2022). DOI: 10.23681/565080.

26. Евсютин О.О. Приложения клеточных автоматов в области информационной безопасности и обработки данных / О.О. Евсютин, А.А. Шелупанов // Доклады ТУСУР. – 2012. – № 1 (25), ч. 2. – С. 119–125.

27. Chase L. Internet Research / L. Chase, J. Alvarez // Library & Information Science Research. – 2000. – Vol. 22, No. 4. – P. 357–369. DOI: 10.1016/s0740-8188(00)00050-5.

28. Hewson C. Internet Research Methods / C. Hewson, C. Vogel, D. Laurent // Internet Research Methods (2nd ed.). – London: Sage. – 2016. DOI: 10.4135/9781473920804.

29. The Global Terrorism Database™ (GTD). – URL: https://www.start.umd.edu/gtd/ (дата обращения: 28.09.2022).

30. Enders W. Domestic versus transnational terrorism: Data, decomposition, and dynamics / W. Enders, T. Sandler, K. Gaibulloev // Journal of Peace Research. – 2011. – Vol. 48, No. 3. – P. 319–338. – DOI: 10.1177/0022343311398926.

31. Sandler T. New frontiers of terrorism research: An introduction // Journal of Peace Research. – 2011. – Vol. 48, No. 3. – P. 279–286. DOI: 10.1177/0022343311399131.

32. Guo D. Visualizing patterns in a global terrorism incident database / D. Guo, K. Liao, M. Morgan // Environment and Planning B: Planning and Design. – 2007. – Vol. 34. – P. 767–784.

33. Модель угроз безопасности информации и ее носителей / А.К. Новохрестов, А.А. Конев, А.А. Шелупанов, Н.С. Егошин // Вестник Иркутского государственного технического университета. – 2017. – Т. 21, № 12 (131). – С. 93–104. DOI: 10.21285/1814-3520-2017-12-93-104.

34. Ankers M. Visual Data Mining with Pixel-oriented Visualization Techniques // The Boeing Company. P.O. Box 3707 MC 7L-70, Seattle, WA 98124. – URL: https://www.ics.uci.edu/~kobsa/courses/ICS280/notes/papers/ankerst-kdd2001.pdf (дата обращения: 28.09.2022).

35. Xu D. Comprehensive Survey of Clustering Algorithms / D. Xu, Y. Tian // Annals of Data Science. – 2015. – Vol. 2. – P. 165–193.

36. Wegmann M. A review of systematic selection of clustering algorithms and their evaluation / M. Wegmann, D. Zipperling, J. Hillenbrand, J. Fleischer. – 2021. – URL: https://arxiv.org/ftp/arxiv/papers/2106/2106.12792.pdf (дата обращения: 28.09.2022).

37. Shelupanov A. Information Security Methods-Modern Research Directions / A. Shelupanov, O. Evsyutin, A. Konev, E. Kostyuchenko, D. Kruchinin, D. Nikiforov // Symmetry. – 2019. – Vol. 11, No. 2. – P. 150. DOI: 10.3390/sym11020150.

38. Worldwide Incidents Tracking System (WITS). – URL: https://knoema.ru/tyytrod/violence-statistics-from-worldwide-incidents-tracking-system-wits (дата обращения: 28.09.2022).

39. The National Counterterrorism Center (NCTC). – URL: https://www.dni.gov/index.php/nctc-newsroom/nctc-resources (дата обращения: 28.09.2022).

40. National Consortium for the Study of Terrorism and Responses to Terrorism (START). – URL: https://www.start.umd.edu/ (дата обращения: 28.09.2022).

41. National Consortium for the Study of Terrorism and Responses to Terrorism (START). – URL: http://www.start-dev.umd.edu/gtd/using-gtd/ (дата обращения: 28.09.2022).

42. Profiles of Individual Radicalization in the United States – PIRUS (Keshif). – URL: https://www.start.umd.edu/profiles-individual-radicalization-united-states-pirus-keshif (дата обращения: 28.09.2022).

43. I-VEO Knowledge Matrix. – URL: http://start.foxtrotdev.com/ (дата обращения: 28.09.2022).

44. Terrorism and Extremist Violence in the United States (TEVUS) Database and Portal (TEVUS Portal). – URL: https://tap.cast.uark.edu/ (дата обращения: 28.09.2022).

45. Terrorism and Extremist Violence in the United States (TEVUS) Database and Portal (TEVUS Portal). – URL: https://www.start.umd.edu/tevus-portal (дата обращения: 28.09.2022).

46. Информационно-аналитический центр «СОВА» (ИАЦ «СОВА»). – URL: https://www.sova-center.ru/database/ (дата обращения: 28.09.2022).

Попов Константин Васильевич
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)
Томского государственного университета
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-913-850-98-17
Эл. почта: pokkos@mail.ru

Шелупанова Полина Александровна
Канд. экон. наук, доцент,
зав. каф. экономической безопасности ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 90-71-55
Эл. почта: polina.a.shelupanova@fb.tusur.ru

Popov K.V., Shelupanova P.A.
Information systems for national security threat analysis

Information technology plays a significant role in what has become known as «computational social science». The development of online technologies and digital research methods in the subject areas of social science is associated with the application of new interdisciplinary approaches and the integration of researchers from different fields of knowledge. As an effective and promising tool for researchers in the study of violent ideologies that destabilize the social order, the article discusses examples of databases, services and platforms for multivariate analysis. Opportunities and limitations of customizing data collection, processing, and presentation are outlined. An overview of the specific characteristics of the databases, services and platforms on the START Research Center website is presented. Conclusions are made about what opportunities such tools open for researchers and the prospects of realization of the most interesting solutions for improving the process of automation of data analysis are outlined.
Keywords*:* national security, extremism, terrorism, radicalization, database, web mining, big data, research tools.
DOI: 10.21293/1818-0442-2022-25-4-71-79

References

1. Popov K.V., Shelupanov A.A. [New challenges: stochastic threats to national security]. *Proceedings of TUSUR University*, 2020, vol. 23, no. 4, pp. 23–29. DOI: 10.21293/1818-0442-2020-23-4-23-29 (in Russ.).

2. Alava S., Frau-Meigs D., Hassan G. Youth and Violent Extremism on Social Media: Mapping the research, United Nations Educational, Scientific and Cultural Organization, 2017. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000260382, free (Accessed: September 28, 2022).

3. Sandler T. New frontiers of terrorism research: An introduction. *Journal of Peace Research*, 2011, vol. 48(3), pp. 279–286. DOI: 10.1177/0022343311399131.

4. Borum R. Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security*, 2011, vol. 4(4), pp. 7–36.

5. RAND Corporation. Available at: https://www.rand.org/, free (Accessed: September 28, 2022).

6. Memorial Institute for the Prevention of Terrorism (MIPT). Available at: https://web.archive.org/web/20130620070250/https://www.mipt.org/Home.aspx, free (Accessed: September 28, 2022).

7. National Consortium for the Study of Terrorism and Responses to Terrorism (START). Available at: https://www.start.umd.edu/, free (Accessed: September 28, 2022).

8. The National Counterterrorism Center (NCTC). Available at: https://www.dni.gov/index.php/nctc-newsroom/nctc-resources, free (Accessed: September 28, 2022).

9. Canadian network for research on terrorism, security and society (TSAS). Available at: https://www.tsas.ca/, free (Accessed: September 28, 2022).

10. Center for Research on Extremism (C-REX). Available at: https://www.sv.uio.no/c-rex/english/, free (Accessed: September 28, 2022).

11. International Centre for Counter-Terrorism, The Netherlands (ICCT). Available at: https://icct.nl/, free (Accessed: September 28, 2022).

12. The International Centre for the Study of Radicalisation (ICSR). Available at: https://icsr.info/, free (Accessed: September 28, 2022).

13. The Handa Centre for the Study of Terrorism and Political Violence (CSTPV). Available at: https://cstpv.wp.st-andrews.ac.uk/, free (Accessed: September 28, 2022).

14. International Center for Terrorism Studies (ICTS). Available at: https://www.potomacinstitute.org/academic-centers/international-center-for-terrorism-studies-icts, free (Accessed: September 28, 2022).

15. International Centre for Political Violence and Terrorism Research (PSiS). Available at: https://www.rsis.edu.sg/research/icpvtr/, free (Accessed: September 28, 2022).

16. China Institutes of Contemporary International Relations (CICIR). Available at: http://www.cicir.ac.cn/NEW/en-us/Institution.html?subtype=America&&type=region, free (Accessed: September 28, 2022).

17. Freedman B. Terrorism Research Centres: 100 Institutes, Programs and Organisations in the Field of Terrorism, Counter-Terrorism, Radicalisation and Asymmetric Warfare Studies. Perspectives on Terrorism, 2010, vol. 4(5), pp. 48–56.

18. Karpova A.Yu., Savelev A.O., Vilnin A.D., Kaida A.Yu., Kuznetsov S.A., Maksimova N.G., Chaykovskiy D.V. [Ultra-right-wing radicalization: a methodology for automated threat detection using web mining methods]. *Vestnik Rossijskogo fonda fundamental'nyh issledovanij*. Gumanitarnye i obshchestvennye nauki, 2020, vol. 5(102), pp. 30–43 (in Russ.).

19. Prishchep S.V., Timchenko S.V., Shelupanov A.A. [Approaches and criteria for assessing information security

risks]. Bezopasnost' informatsionnykh tekhnologiy, 2007, no. 4, pp. 15–21 (in Russ.).

20. Mironova V.G., Shelupanov A.A. [Methodology for the formation of threats to the security of confidential information in uncertain conditions of their occurrence]. Izvestiya Yuzhnogo federalnogo universiteta. Tekhnicheskiye nauki, 2012, vol. 137, no. 12, pp. 39–45 (in Russ.).

21. Savelev A.O., Karpova A.Yu., Chaykovskiy D.V., Vilnin A.D., Kaida A.Yu., Kuznetsov S.A., Igumnov L.O., Maksimova N.G. [The high-level overview of social media content search engine]. *Proceedings of the 14th International Forum on Strategic Technology (IFOST 2019)*. Tomsk, Tomsk Polytechnic University, 2019, pp. 306–309 (in Russ.).

22. Loparev S.A., Shelupanov A.A. [Analysis of tools for assessing the risks of information leakage in the computer network of an enterprise]. *Voprosy zashchity informatsii*, 2003, no. 4(63), pp. 2–5 (in Russ.).

23. Mironova V.G., Shelupanov A.A., Yugov N.T. [Implementation of Take-Grant model as a representation of user access rights differentiation system in the building]. *Proceedings of TUSUR University*, 2011, no. 2(24), part 3, pp. 206–210 (in Russ.).

24. Koua E.L. Using self – organizing maps for information visualization and knowledge discovery in complex geospatial datasets, Proceedings of the 21st International Cartographic Conference (ICC), 10-16 Aug 2003. Durban. South Africa. Available at: https://webapps.itc.utwente.nl/library www/papers_2003/art_proc/koua.pdf, free (Accessed: September 28, 2022).

25. Ageeva E.V., Afanasova M.A., Balandina A.S. [and others]; under total ed. Zhigas M.G., Shelupanov A.A. Tsifrovizatsiya finansovo-kreditnoy sfery v sovremennoy Rossii [Digitalization of the financial and credit sphere in modern Russia]. Moscow; Berlin, Direct-Media, 2019. 408 p. Available at: https://biblioclub.ru/index.php?page=book&id=565080, free (Accessed: September 28, 2022). DOI 10.23681/565080 (in Russ.).

26. Evsutin O.O., Shelupanov A.A. [Applications of cellular automata in the field of information security and data processing]. *Proceedings of TUSUR University*, 2012, no. 1(25), part 2, pp. 119–125 (in Russ.).

27. Chase L., Alvarez J. Internet Research. Library & Information Science Research, 2000, vol. 22(4), pp. 357–369. DOI: 10.1016/s0740-8188(00)00050-5.

28. Hewson C., Vogel C., Laurent D. Internet Research Methods. Internet Research Methods (2nd ed). London: Sage, 2016. DOI: 10.4135/9781473920804.

29. The Global Terrorism Database™ (GTD). Available at: https://www.start.umd.edu/gtd/, free (Accessed: September 28, 2022).

30. Enders W., Sandler T., Gaibulloev K. Domestic versus transnational terrorism: Data, decomposition, and dynamics. *Journal of Peace Research*, 2011, vol. 48(3), pp. 319–338. DOI: 10.1177/0022343311398926.

31. Sandler T. New frontiers of terrorism research: An introduction. *Journal of Peace Research*, 2011, vol. 48(3), pp. 279–286. DOI: 10.1177/0022343311399131.

32. Guo D., Liao K., Morgan M. Visualizing patterns in a global terrorism incident database. *Environment and Planning B: Planning and Design*, 2007, vol. 34, pp. 767–784.

33. Novokhrestov A.K., Konev A.A., Shelupanov A.A., Egoshin N.S. [Information and information carrier security threat model]. *Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta*, 2017, vol. 21, no. 12, pp. 93–104. DOI: 10.21285/1814-3520-2017-12-93-104 (in Russ.).

34. Ankers M. Visual Data Mining with Pixel-oriented Visualization Techniques, The Boeing Company. P.O. Box 3707 MC 7L-70, Seattle, WA 98124. Available at: https://www.ics.uci.edu/~kobsa/courses/ICS280/notes/papers/ankerst-kdd2001.pdf, free (Accessed: September 28, 2022).

35. Xu Dongkuan, Ying-jie Tian. Comprehensive Survey of Clustering Algorithms. *Annals of Data Science*, 2015, vol. 2, pp. 165–193.

36. Wegmann M., Zipperling D., Hillenbrand J., Fleischer J. A review of systematic selection of clustering algorithms and their evaluation, 2021. Available at: https://arxiv.org/ftp/arxiv/papers/2106/2106.12792.pdf, free (Accessed: September 28, 2022).

37. Shelupanov A., Evsyutin O., Konev A., Kostyuchenko E., Kruchinin D., Nikiforov D. Information Security Methods-Modern Research Directions. Symmetry, 2019, vol. 11 (2), pp. 150. DOI: 10.3390/sym11020150.

38. Worldwide Incidents Tracking System (WITS). Available at: https://knoema.ru/tyytrod/violence-statistics-from-worldwide-incidents-tracking-system-wits, free (Accessed: September 28, 2022).

39. The National Counterterrorism Center (NCTC). Available at: https://www.dni.gov/index.php/nctc-newsroom/nctc-resources, free (Accessed: September 28, 2022).

40. National Consortium for the Study of Terrorism and Responses to Terrorism (START). Available at: https://www.start.umd.edu/, free (Accessed: September 28, 2022).

41. National Consortium for the Study of Terrorism and Responses to Terrorism (START). Available at: http://www.start-dev.umd.edu/gtd/using-gtd/, free (Accessed: September 28, 2022).

42. Profiles of Individual Radicalization in the United States – PIRUS (Keshif). Available at: https://www.start.umd.edu/profiles-individual-radicalization-united-states-pirus-keshif, free (Accessed: September 28, 2022).

43. I-VEO Knowledge Matrix. Available at: http://start.foxtrotdev.com/, free (Accessed: September 28, 2022).

44. Terrorism and Extremist Violence in the United States (TEVUS) Database and Portal (TEVUS Portal). Available at: https://tap.cast.uark.edu/, free (Accessed: September 28, 2022).

45. Terrorism and Extremist Violence in the United States (TEVUS) Database and Portal (TEVUS Portal). Available at: https://www.start.umd.edu/tevus-portal, free (Accessed: September 28, 2022).

46. SOVA Center for Information and Analysis. Available at: https://www.sova-center.ru/database/, free (Accessed: September 28, 2022) (in Russ.).

Konstantin V. Popov
Postgraduate Student, Department of Integrated Information Security of Electronic Computing Systems
Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-913-850-98-17
Email: pokkos@mail.ru

Polina A. Shelupanova
Candidate of Economic Sciences, Associate Professor,
Head of the Department of Economic Security TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 90-71-55
Email: polina.a.shelupanova@fb.tusur.ru

УДК 004.056.53

А.А. Конев

Модель угроз безопасности защищенного микроконтроллера и обрабатываемой им информации

Рассмотрены и разбиты на категории угрозы, позволяющие получить доступ к хранящимся и обрабатываемым на защищенном микроконтроллере данным с целью скомпрометировать конечное устройство. Категории включают угрозы, направленные на саму информацию, обрабатываемую на микроконтроллере, и угрозы, направленные непосредственно на сам микроконтроллер и его компоненты. Полученная модель угроз позволяет формализовать построение перечня угроз для дальнейшего формирования требований безопасности, предъявляемых к микроконтроллеру во время его разработки, и критериев оценки его защищённости на этапе тестирования.
Ключевые слова: модель угроз, доверие, микросхема, конфиденциальность.
DOI: 10.21293/1818-0442-2022-25-4-80-87

В настоящее время «умные» устройства получили широкое распространение в различных сферах, таких как интернет вещей, автомобильная промышленность, «умные» сети, индустрия пластиковых карт и многие другие. В связи с этим необходимо обеспечивать определенный уровень защищенности, чтобы избежать потенциального нарушения функционирования автоматизированных систем из-за вмешательства злоумышленника.

Для решения проблем безопасности все чаще применяются аппаратные методы обеспечения защищенности устройств. Устройства, реализующие аппаратные механизмы защищенности, известны как защищенные микроконтроллеры [1]. Аппаратная реализация механизмов безопасности показывает высокую эффективность при низком потреблении ресурсов приложений интернета вещей [2]. Также в защищенных микроконтроллерах применяются меры для защиты от внешнего воздействия на микросхему с целью получения доступа к хранящимся или обрабатываемым данным.

Построение модели угроз безопасности защищенного микроконтроллера и обрабатываемой им информации позволяет обнаружить и устранить потенциальные уязвимости на этапе разработки микросхемы и ПО к ней. Построение модели угроз выполняется в несколько шагов – сначала описывается система, выявляются компоненты системы и связи между ними, а потом для каждого элемента составляется перечень угроз.

Под угрозами безопасности понимаются угрозы несанкционированного изменения состояния автоматизированной системы или ее структуры [3], а также несанкционированного доступа к системе (например, угроза несанкционированной замены компонентов и др. [4]). Также угрозы можно разделить на две категории: угрозы безопасности непосредственно системы и угрозы безопасности средствам защиты информации системы.

Проблема построения модели угроз состоит в сложности составления наиболее полного перечня потенциальных угроз для защищаемого объекта. Существующие модели угроз не описывают в полной мере всевозможные угрозы безопасности. Так, в статьях [5–7] представлены списки угроз для устройств интернета вещей, однако они не охватывают все возможные угрозы, потому что при составлении списка угроз не применяется системный подход к построению модели угроз.

Целью данной статьи является демонстрация системного подхода к описанию угроз на примере защищенного микроконтроллера.

Описание типовой защищенной микросхемы

Защищенная микросхема представляет собой программно-аппаратный модуль, предназначенный для обеспечения безопасного хранения и передачи информационных ресурсов (представляющих собой определенную ценность), реализующих выполнение базовых криптографических функций, а также возможность обеспечения доверенного привилегированного управления.

Типовая защищенная микросхема представляет собой [8, 9] интегрированные между собой компоненты: 32-битный (либо 64) RISC-процессор, а также криптографический сопроцессор с возможностью выполнения различных алгоритмов шифрования, например, RSA, ECC, AES, DES, ГОСТ Р 34.12–2015 и др. Как правило, микросхема имеет до 30 КБ статической оперативной памяти (SRAM) и до 1 МБ энергонезависимой памяти, а также защищенный блок управления памятью (MMU). Структура защищенной микросхемы включает в себя различные периферийные интерфейсы для обеспечения взаимодействия с внешней средой, блок управления питанием и генераторы тактовой частоты для обеспечения работы процессора.

Упрощенная блок-схема защищенной микросхемы представлена на рис. 1.

Построение модели угроз

В литературе [10–14], посвященной описанию угроз микросхемы, обычно рассматривают существующие способы проведения атак и механизмы обеспечения защиты. В работе [15] дополнительно рассматриваются источники появления угроз, такие как персонал, несанкционированные компоненты, вредоносное ПО и направления проведения атак на микросхему.

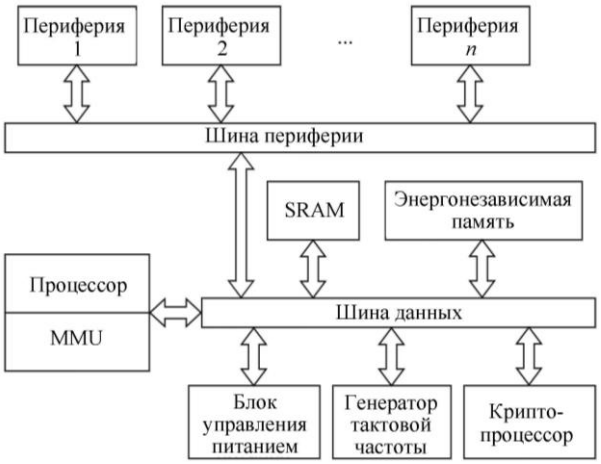


Рис. 1. Структурная схема типовой защищенной микросхемы

Основываясь на моделях, представленных в статьях [3, 4], была представлена модель угроз, которая описывает все потенциально возможные угрозы для защищенных микроконтроллеров за счет выделения отдельных компонентов (и разделения их на те, которые работают или не работают с информацией) и за счет разделения угроз по целям безопасности – конфиденциальности, целостности и защищенности (рис. 2).

Вкратце эту модель угроз можно выразить формулой

$$G = (C_i, CT_i, SG_i),$$

где C_i – наименование компонента, CT_i – тип компонента (взаимодействует с информацией, не взаимодействует с информацией), SG_i – цели безопасности (конфиденциальность, целостность, доступность).

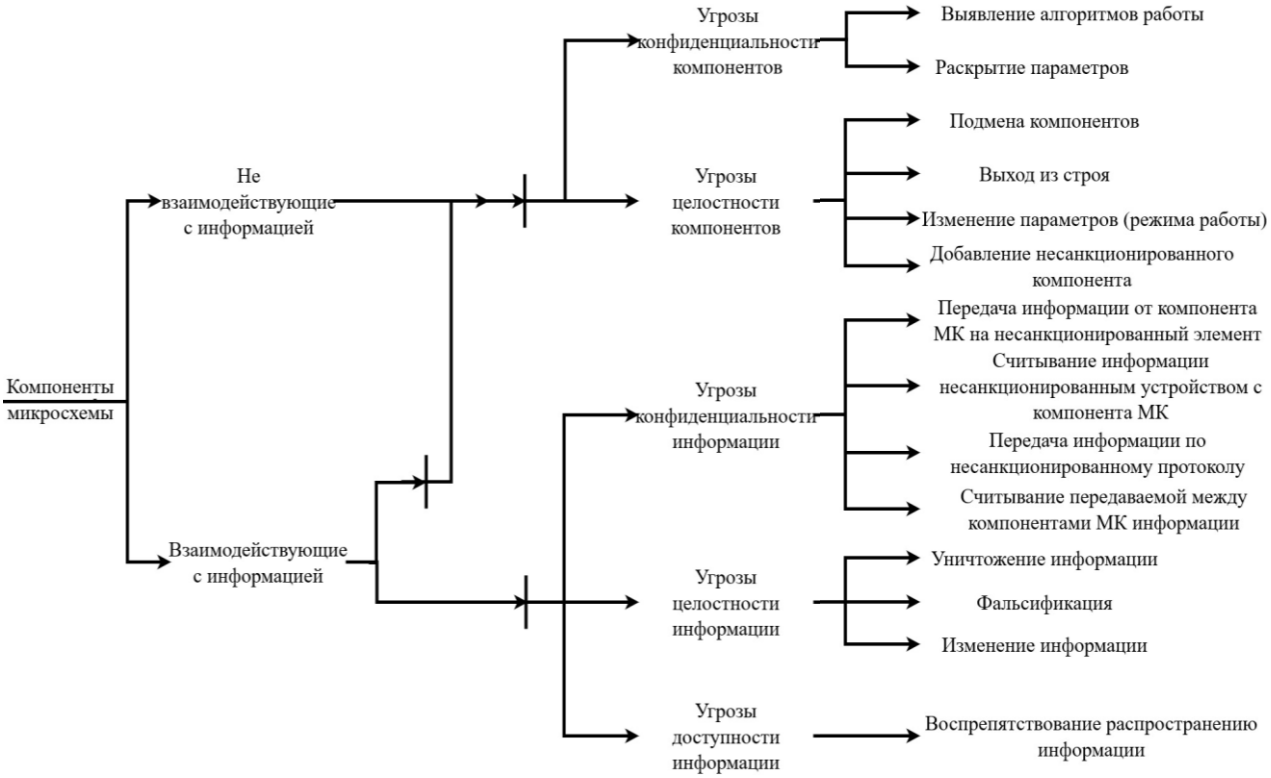


Рис. 2. Категории угроз

В связи с тем, что разработка аппаратной архитектуры микросхемы происходит до либо во время разработки программного обеспечения, невозможно обеспечить исправление аппаратных уязвимостей путем обновления по аналогии с обновлением программного обеспечения. Разработка аппаратного и программного обеспечения должна вестись с учётом всех рисков реализации угроз безопасности в аппаратной архитектуре защищенных микросхем, обеспечивая превентивное решение для достижения высокого уровня доверия.

Для определения характера и направленности потенциальной угрозы введены следующие категории: угрозы конфиденциальности компонентов (УКК) микросхемы, угрозы целостности компонентов (УЦК) микросхемы, угрозы конфиденциальности информации (УКИ), угрозы целостности информации (УЦИ) и угрозы доступности информации (УДИ).

Разделение на данные категории обусловлено возможностью нарушения одного из свойств обеспечения информационной безопасности. Например, для категории УКК актуальны угрозы, связанные с нарушением конфиденциальности архитектурных особенностей непосредственно самих компонентов защищенной микросхемы. Зная структурные особенности реализации компонентов микросхемы, злоумышленник может попытаться изменить режим функционирования микросхемы и впоследствии несанкционированно овладеть конфиденциальной информацией. Также непосредственно сами компоненты могут стать целью злоумышленников, так как

они представляют собой интеллектуальную собственность.

Для компонентов микросхемы, взаимодействующих с информацией, помимо угроз конфиденциальности и целостности компонентов существуют угрозы, связанные с конфиденциальностью, целостностью и доступностью информации.

Для компонентов микросхемы, не взаимодействующих с информацией, существуют только угрозы, связанные с конфиденциальностью и целостностью компонентов микросхемы.

К категории угроз конфиденциальности компонентов (УКК) относятся угрозы, связанные с несанкционированным и вредоносным воздействием на элементы МК с целью нарушения их конфиденциальности (табл. 1).

Таблица 1

Угрозы конфиденциальности компонентов

Наименование	Описание
Выявление алгоритмов работы	К данной подкатегории относятся угрозы, связанные с выявлением информации об алгоритмах работы компонентов МК и использованием ее для реализации атаки на устройство
Раскрытие параметров	К данной подкатегории относятся угрозы, связанные с раскрытием информации о параметрах компонентов МК и использованием ее для осуществления успешной атаки на устройство

К категории угроз целостности компонентов (УЦК) относятся угрозы, связанные с вредоносным воздействием на компоненты МК с целью нарушения их целостности (табл. 2).

Таблица 2

Угрозы целостности компонентов

Наименование	Описание
Подмена компонентов	К данной подкатегории относятся угрозы, связанные с подменой компонентов МК на компоненты, содержащие определенные уязвимости, на этапе проектирования либо на этапе производства микросхемы
Выход из строя	К данной подкатегории относятся угрозы, связанные с уничтожением или отключением компонентов МК
Изменение параметров (режима работы)	К данной подкатегории относятся угрозы, связанные с изменением параметров (режима работы) компонентов МК
Добавление несанкционированного компонента	К данной подкатегории относятся угрозы, связанные с добавлением новых компонентов, содержащих определенные уязвимости, на этапе проектирования либо на этапе производства микросхемы

К категории угроз конфиденциальности информации (УКИ) относятся угрозы, связанные с вредоносным воздействием на компоненты МК с целью нарушения конфиденциальности информации, хранящейся на данном компоненте (табл. 3).

К категории угрозы целостности информации (УЦИ) относятся угрозы, связанные с вредоносным воздействием на компоненты МК с целью нарушения целостности информации, хранящейся на данном компоненте (табл. 4).

К категории угроз доступности информации (УДИ) относятся угрозы, связанные с вредоносным воздействием на компоненты МК с целью нарушения доступности передаваемой информации (табл. 5).

Таблица 3

Угрозы конфиденциальности информации

Наименование	Описание
Передача информации от компонента МК на несанкционированный элемент	К данной подкатегории относятся угрозы, связанные с передачей информации от компонента МК на несанкционированный элемент, внедренный злоумышленником
Считывание информации несанкционированным устройством с компонента МК	К данной подкатегории относятся угрозы, связанные со считыванием информации несанкционированным устройством с компонента МК
Передача информации по несанкционированному протоколу	К данной подкатегории относятся угрозы, связанные с передачей информации по каналу, который не обеспечивает должный уровень защиты передаваемой информации
Считывание передаваемой между компонентами МК информации	К данной подкатегории относятся угрозы, связанные с воздействием на каналы передачи данных между компонентами МК, например, с помощью электромагнитного излучения

Таблица 4

Угрозы целостности информации

Наименование	Описание
Уничтожение информации	К данной подкатегории относятся угрозы, связанные с уничтожением хранимой на компонентах МК информации
Фальсификация	К данной подкатегории относятся угрозы, связанные с подменой информации, хранящейся на компонентах МК
Изменение информации	К данной подкатегории относятся угрозы, связанные с изменением информации вследствие помех или намеренной модификации

Таблица 5

Угрозы доступности информации

Наименование	Описание
Воспрепятствование распространению информации	К данной подкатегории относятся угрозы, связанные с доступностью информации

На рис. 2 представлена блок-схема категорий угроз. Таблицы 6–10 содержат примеры угроз с описанием для каждой категории угроз.

Таблица 6

Угроза конфиденциальности компонентов

Ид.	Наименование угрозы	Описание
УКК1.1	Угроза предсказания результатов генератора случайных чисел	Угроза заключается в возможности обнаружения уязвимостей в алгоритмах генерации псевдослучайных либо случайных чисел, а также непосредственно в реализациях данных компонентов микросхемы. Данная угроза обусловлена недостаточным уровнем надежности алгоритмов генерации псевдослучайных либо случайных чисел, а также наличием уязвимостей непосредственно в самих реализуемых компонентах микросхемы. Реализация угрозы возможна при наличии у злоумышленника сведений о применяемых в микросхеме механизмах генерации псевдослучайных либо случайных чисел, а также сведений о реализованных в них алгоритмах, конфигурационных параметрах, на основании которых злоумышленник может делать предсказания
УКК1.2	Угроза выявления слабостей реализации криптографических алгоритмов	Угроза заключается в возможности определения уязвимостей криптографических алгоритмов, а также уязвимостей непосредственно самих компонентов, реализующих данные алгоритмы. Данная угроза обусловлена недостаточным уровнем надежности криптографического алгоритма, а также ошибками проектирования криптографических компонентов, уязвимостями в линиях взаимодействий с внешними компонентами, неправильными параметрами конфигурации. Реализация угрозы возможна при наличии у злоумышленника сведений о применяемых в микросхеме механизмах шифрования, а также их алгоритмах и конфигурационных параметрах
УКК1.3	Угроза выявления уязвимостей в реализации ядра	Угроза заключается в возможности определения уязвимостей в архитектуре ядра микросхемы, а также уязвимостей в реализующих данную архитектуру компонентах микросхемы. Данная угроза обусловлена недостаточным уровнем надежности реализации архитектурных возможностей ядра микросхемы. Реализация угрозы возможна при наличии у злоумышленника сведений об архитектуре ядра либо сведений о реализации данной архитектуры на компоненте микросхемы
УКК1.4	Угроза выявления уязвимостей в реализации запоминающих компонентов	Угроза заключается в возможности определения уязвимостей запоминающих устройств микросхемы. Данная угроза обусловлена наличием уязвимостей реализации механизмов запоминающих устройств либо наличием неправильных конфигурационных параметров. Реализация угрозы возможна при наличии у злоумышленника сведений об архитектуре запоминающих устройств, при существовании уязвимостей в линиях взаимодействия с внешними компонентами, а также при неправильных параметрах конфигурации
УКК1.5	Угроза обнаружения недекларированных возможностей	Угроза заключается в возможности определения незаявленных либо не соответствующих описанию в документации функциональных возможностей. Данная угроза обусловлена неправильным подходом к разработке защищенных микросхем, устаревшей документации либо несанкционированным внедрением аппаратных закладок в архитектуру компонента микросхемы. Реализация угрозы возможна при наличии у злоумышленника сведений о недекларированных возможностях, либо функциях, не соответствующих заявленной документации
УКК2.1	Угроза определения параметров объектов защиты	Угроза заключается в возможности определения конфигурационных параметров защищенных компонентов, механизмов обеспечения шифрования и других компонентов, связанных с криптографией. Данная угроза обусловлена неправильной установкой конфигурационных параметров либо использованием слабых значений защитных механизмов. Реализация угрозы возможна при наличии у злоумышленника сведений об уязвимостях механизмов защиты
УКК2.2	Угроза определения режима работы ядра	Угроза заключается в возможности определения режима работы устройства для последующего анализа функционирования встроенной программы. Данная угроза обусловлена использованием слабых или неправильных значений параметров конфигурации работы ядра. Реализация угрозы возможна в случае наличия у злоумышленника физического доступа к устройству для выполнения инвазивного либо неинвазивного анализа целевого устройства

Таблица 7

Угрозы целостности компонентов

Ид.	Наименование угрозы	Описание
УЦК1.1	Угроза подделки компонента	Угроза заключается в возможности подмены легитимного компонента на сторонний компонент. Данная угроза обусловлена недостаточным контролем на этапе разработки и производства компонентов микросхемы. Реализация угрозы возможна в случае использования сторонних либо недоверенных компонентов (например, лицензируемых компонентов с неизвестной реализацией архитектуры, а также при использовании зарубежных IP-блоков, произведенных на зарубежных мощностях)
УЦК1.2	Угроза подмены компонента разработки	Угроза заключается в возможности подмены легитимных компонентов отладки и разработки (JTAG, SWD), имеющих привилегированный доступ к различным ресурсам микросхемы, на сторонний компонент. Данная угроза обусловлена недостаточным контролем на этапе разработки и производства компонентов микросхемы. Реализация угрозы возможна в случае использования сторонних либо недоверенных компонентов (например, лицензируемых компонентов с неизвестной реализацией архитектуры)
УЦК2.1	Угроза намеренного вывода из строя компонента	Угроза заключается в возможности вывода из строя компонента, путем вредоносного воздействия на физическую структуру данного компонента. Данная угроза обусловлена недостаточным контролем на этапе разработки и производства компонентов микросхемы. Реализация угрозы возможна в случае использования сторонних либо недоверенных компонентов (например, лицензируемых компонентов с неизвестной реализацией архитектуры)
УЦК2.2	Угроза случайного вывода из строя компонента	Угроза заключается в возможности непреднамеренного вывода из строя компонента путем повреждения физической структуры компонента из-за поражения статическим зарядом либо ввиду неправильной конфигурации. Данная угроза обусловлена недостаточным уровнем обеспечения защиты компонента либо отсутствующим механизмом защиты компонента микросхемы. Реализация угрозы возможна в случае отсутствия требуемой компетенции проектировщиков либо разработчиков компонентов микросхемы
УЦК2.3	Угроза намеренного отключения компонента	Угроза заключается в возможности отключения компонента путем вредоносного воздействия на структуру данного компонента. Данная угроза обусловлена недостаточным уровнем обеспечения защиты от несанкционированного вторжения. Реализация угрозы возможна в случае наличия физического доступа злоумышленника к компонентам системы
УЦК2.4	Угроза случайного отключения компонента	Угроза заключается в возможности непреднамеренного отключения компонента путем повреждения физической структуры компонента из-за поражения статическим зарядом. Данная угроза обусловлена непродуманной системой конфигурации микросхемы. Реализация угрозы возможна в случае отсутствия должных компетенций у проектировщиков либо разработчиков компонентов микросхемы
УЦК3.1	Угроза несанкционированного изменения режима работы компонента	Угроза заключается в возможности несанкционированной модификации режима функционирования компонентов микросхемы. Изменение режима функционирования может быть достигнуто за счёт изменения параметров функционирования микросхемы, таких как частота и входное напряжение. Данная угроза обусловлена недостаточным уровнем обеспечения защиты от вредоносного инвазивного и неинвазивного воздействия. Реализация угрозы возможна в случае, когда злоумышленнику известно расположение компонентов и их назначение
УЦК4.1	Угроза добавления несанкционированного/вредоносного компонента	Угроза заключается в возможности занесения уязвимостей и слабостей вместе с добавлением несанкционированного компонента. Данная угроза обусловлена отсутствием контроля на этапе проектирования и производства МК. Реализация угрозы возможна в случае использования зарубежных IP-блоков, проектирования МК иностранными специалистами и производстве МК на чужих мощностях

Таблица 8

Угрозы конфиденциальности информации

Ид.	Наименование угрозы	Описание
УКИ1.1	Угроза НСД к информации	Угроза заключается в возможности получения несанкционированного доступа к информации путем подмены принимающего компонента МК. Данная угроза обусловлена незащищенной от внешнего воздействия реализацией компонентов МК, а также возможностью злоумышленника подключиться к внешним выводам интерфейсов связи. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, а также о размещении внешних выводов интерфейсов связи и наличии физического доступа к МК, позволяющего применить инвазивный и/или неинвазивный метод для НСД к информации, передаваемой между компонентами МК или МК и внешним устройством
УКИ2.1	Угроза считывания содержимого ОЗУ несанкционированным устройством	Угроза заключается в возможности получения несанкционированного доступа к информации путем подключения ОЗУ МК к внешнему элементу, выдающему себя за компонент МК. Данная угроза обусловлена незащищенной от внешнего воздействия реализацией компонентов МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме и наличии физического доступа к МК, позволяющего применить инвазивный метод для считывания содержимого ОЗУ
УКИ3.1	Угроза передачи данных по незащищенному каналу (интерфейсу)	Угроза заключается в возможности получения несанкционированного доступа к информации, передаваемой по интерфейсу, не обеспечивающему соответствующий уровень защищенности. Данная угроза обусловлена незащищенной от внешнего воздействия реализацией компонентов МК, а также возможностью злоумышленника подключиться к внешним выводам интерфейсов связи. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, а также о размещении внешних выводов интерфейсов связи и наличии физического доступа к МК, позволяющего применить инвазивный и/или неинвазивный метод для НСД к информации, передаваемой по незащищенному каналу между компонентами МК или МК и внешним устройством
УКИ3.2	Угроза использования слабостей кодирования входных данных	Угроза заключается в возможности отключения мер защиты канала связи для дальнейшего считывания передаваемой по нему информации. Данная угроза обусловлена незащищенной от внешнего воздействия реализацией компонентов МК, а также возможностью злоумышленника подключиться к внешним выводам интерфейсов связи. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, а также о размещении внешних выводов интерфейсов связи и наличии физического доступа к МК, позволяющего применить инвазивный и/или неинвазивный метод для отключения мер защиты канала связи и НСД к информации, передаваемой между компонентами МК или МК и внешним устройством
УКИ4.1	Угроза перехвата данных	Угроза заключается в возможности получения несанкционированного доступа к информации путем утечки информации по электромагнитным и электрическим каналам, возникающим за счет побочных электромагнитных излучений передачи информации. Данная угроза обусловлена незащищенной от внешнего воздействия реализацией компонентов МК, отсутствием экранирования. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме и наличии физического доступа к МК, позволяющего применить инвазивный метод для считывания передаваемой между компонентами МК информации

Таблица 9

Угрозы целостности информации

Ид.	Наименование угрозы	Описание
1	2	3
УЦИ1.1	Угроза несанкционированного удаления информации	Угроза заключается в возможности злоумышленника воздействовать на компонент МК таким образом, чтобы хранимая на нем информация была удалена. Данная угроза обусловлена не защищенной от внешнего воздействия реализацией компонентов МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме и наличии физического доступа к МК, позволяющего применить инвазивный метод для удаления информации

Окончание табл. 9

1	2	3
УЦИ2.1	Угроза подмены данных	Угроза заключается в возможности злоумышленника воздействовать на компонент МК таким образом, чтобы на него была добавлена фальшивая информация. Данная угроза обусловлена не защищенной от внешнего воздействия реализацией компонентов МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме и наличии физического доступа к МК, позволяющего применить инвазивный метод для подмены информации
УЦИ3.1	Угроза несанкционированной модификации данных	Угроза заключается в возможности злоумышленника воздействовать на компонент МК таким образом, чтобы хранимая на нем информация была изменена. Данная угроза обусловлена не защищенной от внешнего воздействия реализацией компонентов МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме и наличии физического доступа к МК, позволяющего применить инвазивный метод для изменения информации
УЦИ3.2	Угроза нарушения целостности данных в связи с помехами	Угроза заключается в возможности злоумышленника воздействовать на компонент МК таким образом, чтобы передаваемая по нему информация была изменена случайным образом вследствие помех. Данная угроза обусловлена не защищенной от внешнего воздействия реализацией компонентов МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, наличии физического доступа к МК и специальной аппаратуры генерации помех

Таблица 10

Угрозы доступности информации

Ид.	Наименование угрозы	Описание
УДИ1.1	Угроза блокирования доступа к информации	Угроза заключается в возможности блокирования процесса обмена информацией между компонентами МК. Данная угроза обусловлена использованием не защищенного от блокирования канала, возможностью злоумышленника подключиться к внешним выводам интерфейсов связи, а также отсутствием резервного канала связи между компонентами МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, а также о размещении внешних выводов интерфейсов связи и наличии физического доступа к МК, позволяющего применить инвазивный и/или неинвазивный метод для блокирования доступа к информации
УДИ1.2	Угроза отказа в обслуживании	Угроза заключается во вмешательстве в процесс обмена информацией между компонентами МК с целью подмены передаваемой информации. Данная угроза обусловлена использованием канала, к которому может подключиться злоумышленник и передавать данные для отказа в обслуживании, а также отсутствием резервного канала связи между компонентами МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, а также о размещении внешних выводов интерфейсов связи и наличии физического доступа к МК, позволяющего применить инвазивный и/или неинвазивный метод для организации отказа в обслуживании

Заключение

В статье были представлены 26 угроз получения доступа к хранящимся и обрабатываемым на защищенном микроконтроллере данным, из которых 12 угроз нарушения конфиденциальности, 12 угроз нарушения целостности и 2 угрозы нарушения доступности. Данные угрозы были разделены на категории в соответствии с особенностями компонентов, на которые они воздействуют, а именно на компоненты, которые обрабатывают или не обрабатывают информацию, а также на подкатегории согласно основным целям безопасности.

Статья подготовлена в рамках реализации программы ЛИЦ «Доверенные сенсорные системы» (договор № 009/20 от 10.04.2020) при финансовой поддержке Минкомсвязи России и АО «РВК». Идентификатор соглашения о предоставлении субсидии – 0000000007119P190002.

Литература

1. Lee B. Design and Implementation of Secure Cryptographic System on Chip for Internet of Things / B. Lee, I.-G. Lee, M. Kim // IEEE Access. – 2022. – Vol. 10. – P. 18730–18742.

2. Ramalingam S. A Holistic Systems Security Approach Featuring Thin Secure Elements for Resilient IoT Deployments / S. Ramalingam, H. Gan, G. Epiphaniou, E. Mistretta // Sensors. – 2020. – Vol. 20, No. 18. – P. 5252.

3. Новохрестов А.К. Модель угроз безопасности информации и ее носителей / А.К. Новохрестов, А.А. Конев, А.А. Шелупанов, Н.С. Егошин // Вестник Иркутского государственного технического университета. – 2017. – Т. 21, № 12. – С. 93–104.

4. Новохрестов А.К. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов / А.К. Новохрестов, Д.С. Никифоров, А.А. Конев, А.А. Шелупанов // Доклады ТУСУР. – 2016. – Т. 19, № 3. – С. 111–114.

5. A survey on internet of things security: Requirements, challenges, and solutions / H. HaddadPajouh, A. Dehghantanha, R.M. Parizi, M. Aledhari, H. Karimipour // Internet of Things. – 2021. – Vol. 14. – P. 100129.

6. Security Considerations for Internet of Things: A Survey / A. Jurcut, T. Niculcea, P. Ranaweera, N.-A. Le-Khac // SN Computer Science. – 2020. – Vol. 1, No. 4. – P. 1–19.

7. Jurcut A.D. Introduction to IoT Security / A.D. Jurcut, P. Ranaweera, L. Xu // Wiley 5G Ref. – 2019. – P. 27–64.

8. Performance Analysis of Secure Elements for IoT / M. Noseda, L. Zimmerli, T. Schläpfer, A. Rüst // IoT. – 2021. – Vol. 3, No. 1. – P. 1–28.

9. Deshpande V. PulSec: Secure Element based framework for sensors anomaly detection in Industry 4.0 / V. Deshpande, L. George, H. Badis // IFAC-PapersOnLine. – 2019. – Vol. 52, No. 13. – P. 1204–1209.

10. Yu Q. Proactive Defense Against Security Threats on IoT Hardware / Q. Yu, Z. Zhang, J. Dofe // Modeling and Design of Secure Internet of Things. – 2020. – P. 407–433.

11. He Y. The Study on Hardware Security and Its Defense Measures // SHS Web Conf. – 2022. – Vol. 144. – P. 1–5.

12. Using Honeypots for ICS Threats Evaluation / N. Dutta N. Jadav N. Dutiya D. Joshi // Recent Developments on Industrial Control Systems Resilience – 2019 – P. 175–196.

13. Nagata M. Physical Attack Protection Techniques for IC Chip Level Hardware Security / M. Nagata, T. Miki, N. Miura // IEEE Transactions on Very Large Scale Integration (VLSI) Systems. – 2022. – Vol. 30, No. 1. – P. 5–14.

14. An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools / W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, H. Li // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2021. – Vol. 40, No. 6. – P. 1010–1038.

15. Flaus J.-M. Threats and Attacks to ICS // Cybersecurity of Industrial Systems. – 2019. – P. 91–120.

Конев Антон Александрович
Канд. техн. наук, доцент каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)
Томского государственного университета систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0002-3222-9956
Тел.: +7 (382-2) 70-15-29
Эл. почта: kaa@fb.tusur.ru

Konev A.A.

Security threat model for protected microcontroller and the information it processes

The threats that allow access to data stored and processed on a secure microcontroller in order to compromise the end device are considered and divided into categories. The categories include threats that target the proper information processed on the microcontroller and threats that target the microcontroller itself and its components directly. The resulting threat model allows formalizing the construction of a list of threats for further formation of security requirements for the microcontroller during its development, and criteria for assessing its security at the testing stage.

Keywords: threat model, trust, chip, privacy.
DOI: 10.21293/1818-0442-2022-25-4-80-87

References

1. Lee B., Lee I.-G., Kim M., Design and Implementation of Secure Cryptographic System on Chip for Internet of Things, IEEE Access, 2022, vol. 10. pp. 18730–18742.

2. Ramalingam S., Gan H., Epiphaniou G., Mistretta E., A Holistic Systems Security Approach Featuring Thin Secure Elements for Resilient IoT Deployments, Sensors, 2020, vol. 20, no. 18. MDPI AG, p. 5252.

3. Novokhrestov A. K., Konev A.A., Shelupanov A.A., N.S Egoshin. A Model of Threats to the Security of Information and its Carriers. *Vestnik of the Irkutsk State Technical University*, vol. 21, no. 12 (131), 2017, pp. 93–104 (in Russ.).

4. Novokhrestov A.K. et al. Model of threats to automatic system for commercial accounting of power consumption. *Proceedings of TUSUR University*, vol. 19, no. 3. Tomsk State University of Control Systems and Radioelectronics (TUSUR), pp. 111–114, 2016 (in Russ.).

5. HaddadPajouh H., Dehghantanha A., Parizi R. M., Aledhari M., Karimipour H. A survey on internet of things security: Requirements, challenges, and solutions, *Internet of Things*, 2021, vol. 14. Elsevier BV, p. 100129.

6. Jurcut A., Niculcea T., Ranaweera P., Le-Khac N.-A. Security Considerations for Internet of Things: A Survey. *SN Computer Science*, 2020, vol. 1, no. 4. Springer Science and Business Media LLC.

7. Jurcut A.D., Ranaweera P., Xu L. *Introduction to IoT Security*. Wiley 5G Ref. Wiley, 2019, pp. 1–39.

8. Noseda M., Zimmerli L., Schläpfer T., Rüst A. Performance Analysis of Secure Elements for IoT. *IoT*, 2021, vol. 3, no. 1, MDPI AG, pp. 1–28.

9. Deshpande V., George L., Badis H. PulSec: Secure Element based framework for sensors anomaly detection in Industry 4.0. *IFAC-PapersOnLine*, 2019, vol. 52, no. 13, Elsevier BV, pp. 1204–1209.

10. Yu Q., Zhang Z., Dofe J. Proactive Defense Against Security Threats on IoT Hardware, Modeling and Design of Secure Internet of Things, 2020, Wiley, pp. 407–433.

11. He Y. The Study on Hardware Security and Its Defense Measures. *SHS Web of Conferences*, 2022, vol. 144, EDP Sciences, p. 02011.

12. Dutta N., Jadav N., Dutiya N., Joshi D. Using Honeypots for ICS Threats Evaluation, Recent Developments on Industrial Control Systems Resilience. Springer International Publishing, pp. 175–196, 2019.

13. Nagata M., Miki T., Miura N. Physical Attack Protection Techniques for IC Chip Level Hardware Security. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2022, vol. 30, no. 1. Institute of Electrical and Electronics Engineers (IEEE), pp. 5–14.

14. Hu W., Chang C.-H., Sengupta A., Bhunia S., Kastner R., Li H. An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2021, vol. 40, no. 6, pp. 1010–1038.

15. Flaus J.- M. Threats and Attacks to ICS, Cybersecurity of Industrial Systems. 2019, Wiley, pp. 91–120.

Anton A. Konev
Candidate of Science in Engineering, Assistant Professor,
Department of Complex Information Security of Electronic Computing Systems (KIBEVS), Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
ORCID 0000-0002-3222-9956
Phone: +7 (382-2) 70-15-29
Email: kaa@fb.tusur.ru

УДК 004.056

В.В. Баранов, А.А. Шелупанов

Методика и алгоритмы расчета защищенности элементов распределенных информационных систем в условиях деструктивного воздействия

Проведено обоснование актуальности разработки методического аппарата и алгоритмов определения объектов деструктивного воздействия и расчета параметров защищенности распределенных информационных систем. Осуществлен анализ исследований в данной области, сформулированы требования к функциональным возможностям методики. Выбран математический аппарат, разработаны методика и алгоритмы определения объектов деструктивного воздействия на различных уровнях интегрированных онтологических структурно-функциональных нейро-байесовских моделей, а также степени их критичности для функциональной и структурной живучести типовых информационных модулей распределённых информационных систем. Дан порядок расчета параметров защищенности типовых информационных модулей и оценки эффективности защитных мер.
Ключевые слова: онтологическая модель, нейро-байесовская модель, объекты воздействия, уязвимости, структурная живучесть, функциональная живучесть, меры защиты информации.
DOI: 10.21293/1818-0442-2022-25-4-88-100

Обеспечение надежной защиты распределенных информационных систем (РИС) требует разработки методического аппарата моделирования процессов их функционирования в условиях деструктивного воздействия (ДВ) различных категорий нарушителей и расчета параметров их защищенности. На практике данная задача осложняется вероятностной оценкой, неполными данными и большой степенью неопределенности в характере действий нарушителя, выборе им тех или иных способов реализации угроз безопасности информации (УБИ).

Научная ценность данного исследования заключается в том, что представленные методика и алгоритмы позволяют определять объекты ДВ на различных уровнях типовых информационных модулей распределенных информационных систем (ТИМ РИС), осуществлять расчет степени их критичности для функциональной и структурной живучести системы. Разработан новый способ моделирования ТИМ РИС, заключающийся в интеграции онтологических структурно-функциональных и нейро-байесовских моделей (ОСФ-НБМ). Такой подход вносит определенный вклад в развитие теории и методологии информационной безопасности (ИБ) и является логическим продолжением проведенных ранее авторами исследований.

В работе принят ряд ограничений. Так, не рассматриваются алгоритмы разработки интегрированных ОСФ-НБМ ТИМ РИС. Концептуально представлен облик нейро-байесовских моделей (НБМ). Данные области можно определить как направления дальнейших исследований.

Ключевым аспектом в процессе решения рассматриваемой в работе проблемы является обеспечение требуемого уровня результатов моделирования событий ИБ, связанных с оценкой численных значений показателей способов реализации УБИ и применения организационных и технических мер защиты информации (МЗИ). На этапе функционирования в условиях динамично меняющегося ДВ система защиты РИС требует непрерывного мониторинга и адекватного реагирования на новые риски реализации УБИ. Данное обстоятельство определяет потребность моделирования динамики изменения событий ИБ и отражения их показателей. В этих целях применяется математический аппарат многокритериальной оценки (методов MCDM). Из множества альтернативных вариантов решений по нескольким критериям выбирается наиболее эффективный для складывающейся обстановки вариант. Обзор таких методов приведен в [1, 2].

В работе [3] предложен оригинальный гибридный многокритериальный метод оценки AHP-TOPSIS-2N, представляющий собой интеграцию процесса аналитической иерархии (Analytic Hierarchy Process, AHP), метода предпочтения порядка по сходству с идеальным решением (Technique for Order Preference by Similarity to Ideal Solution, TOPSIS) и двух процедур нормализации (2N).

Подход к решению задачи моделирования процесса оценки защищенности РИС, которая послужила основой для создания системы поддержки принятия решений (СППР) должностных лиц органов управления (ДЛ ОУ) в области ИБ, представлен в [4]. Он заключается в интеграции онтологических структурно-функциональных и нейро-байесовских моделей для составления ациклического графа, отражающего вероятностные показатели структурно-функциональных связей событий ИБ различного генеза.

Для решения проблемы разработки представленной в работе методики был проанализирован ряд научных исследований и регулятивных документов в данной области.

В [5, 6] представлены основные понятия и критерии оценки защищенности РИС. Защита от УБИ осуществляется применением МЗИ. МЗИ подразделяются на технические меры (ТМ), реализуемые

средствами защиты информации (СЗИ), и организационные меры (ОМ), реализуемые режимными мероприятиями. Совокупность применяемых ОМ и ТМ представляет собой способ защиты информации. При этом вклад указанных видов МЗИ в процесс защиты не всегда симметричен.

В [7] определено, что объекты воздействия должны быть установлены на аппаратном, программном, прикладном, сетевом и пользовательском уровнях. Приведены примеры сценариев, тактик и техник атак. Предложен экспертный метод оценки актуальности УБИ.

В исследовании [8] предлагается с помощью адаптивного мониторинга определять объекты ДВ, наиболее подверженные атакам, и акцентировать внимание на их защите.

В научной работе [9] представлена методика риск-ориентированного моделирования атак, основанная на ранжировании рисков получения ущерба и позволяющая выявить наиболее «опасные» с этой точки зрения объекты.

Процесс передачи и хранения данных отображает открытая сетевая модель «Basic Reference Model Open Systems Interconnection model», или сокращенно OSI/ISO, которая имеет семь уровней [10]. С ее помощью легко определить структурно-функциональные связи элементов локальных информационно-вычислительных сетей (ЛИВС) и РИС в целом. Данная модель также описывает все, что происходит при отправке и приеме данных, а также участвующие в этом процессе физические и логические устройства, интерфейсы и протоколы.

Современные подходы, связанные с разработкой СППР и применением искусственного интеллекта для решения задач управления, представлены в [11, 12].

Объекты воздействия на разных уровнях реализуют процессы различной степени критичности для обеспечения устойчивого функционирования РИС и ее элементов. В настоящее время их взаимное влияние и показатели безопасности на интегративном уровне слабо исследованы [13].

Проведенный ранее анализ показал, что существующие методические подходы не содержат апробированный математический аппарат расчета зависимости показателей защищенности РИС от тех или иных способов реализации УБИ. Поэтому принимаемые решения в большей степени носят субъективный характер, достоверность которых зависит от качества имеющихся исходных данных по складывающейся обстановке, а также практического опыта экспертов.

Данное обстоятельство определяет **научную задачу исследования**, которая заключается в разработке новых и совершенствовании существующих методических и инструментальных средств расчета численных значений показателей событий ИБ различного генеза.

Научную задачу, поставленную в исследовании, целесообразно декомпозировать на две подзадачи. Первая будет касаться процесса моделирования объектов ДВ в ТИМ РИС, а вторая – методов и алгоритмов расчета параметров их защищенности.

В ходе анализа существующих методов моделирования были выбраны следующие наиболее подходящие для моделирования объектов ДВ в ТМ РИС. Это метод онтологий для формирования онтологических структурно-функциональных моделей (ОСФМ) [14, 15] и метод байесовских сетей для формирования нейро-байесовской модели (НБМ) [16, 17].

Онтологии служат для систем организации знаний и применяются в тех областях, где требуется обнаружить инфраструктурную интеграцию, выявить скрытые взаимосвязи между элементами. Основной постулат онтологии: если в базе знаний отсутствуют некоторые объекты или связи между ними, то это не значит, что они не существуют, а просто они не описаны.

Онтология может быть представлена в виде графа, вершины которого – это сущности (концепты), а ребра – отношения между сущностями. Если любое утверждение можно представить в виде простых предложений, то из них можно извлечь данные по упомянутым в них сущностям (концептам) и отношениям между ними. В зависимости от целей и задач может быть построено онтологическое пространство знаний, включающее в себя модули подсистем с отражением реализуемых ими процессов [18].

В области ИБ и применительно к данному исследованию это свойство онтологий может быть реализовано для построения онтологического пространства знаний, включающего онтологии ТИМ РИС с требуемой степенью детализации, онтологии объектов ДВ в ТИМ РИС и их уязвимостей, онтологии рисков УБИ, способов и сценариев их реализации, а также онтологии защитных мероприятий [19].

Важным преимуществом онтологий является их наглядность. Это дает возможность построения ОСФМ объектов ДВ в ТИМ РИС любой сложности, а также определение путей (маршрутов) реализации сценария УБИ внутри системы, идентификацию, анализ и оценивание рисков инцидентов, а также способы и точки нейтрализации УБИ и (или) уязвимостей.

Для полноценной работы модели необходима вероятностная оценка наступления взаимоувязанных событий ИБ. Например, вероятность риска инцидента при реализации с определенной вероятностью сценария УБИ. Такая вероятность называется условной, т.е. она для одного события наступает при условии, что другое событие (по подтверждённому или неподтверждённому доказательством утверждению) уже произошло. Для вычисления таких вероятностей применяется теорема Байеса, суть которой описывает следующая формула:

$$P(A|B)\,P(B) = P(B|A)\,P(A), \qquad (1)$$

где P – условная вероятность событий A и B.

Графическая модель данной зависимости представляет собой байесовскую сеть доверия – направ-

ленный ациклический граф, т.е. граф, в котором не существует направленного маршрута, начинающегося и заканчивающегося в одной и той же вершине [20].

Вершины сети представляет собой множество случайных величин, определяющих состояние событий ИБ и подчиняющихся закону Гаусовского распределения. Вершины могут описываться с помощью набора переменных, для которых задаются взвешенные параметры и формируется множество гипотез.

В исследовании вершинами графа байесовской модели приняты концепты онтологической модели ДВ в ТИМ РИС. Это позволило определить значения условных вероятностей функциональных связей концептов, которые являются ребрами графа. Таким образом, можно заключить, что в ходе исследования выявлено свойство интегративности ОСФМ и НБМ, которое и будет применено для моделирования объектов ДВ в ТИМ РИС.

Для решения второй подзадачи научного исследования применены методы алгебраических матриц, элементы теории графов, методы многокритериальной оценки (MCDM), методы теории нейро-сетевого анализа.

В ряде работ [21, 22] события ИБ деструктивного характера формализованно представлены в виде векторов атак, отражающих показатели их существенных свойств и точки (объекты) воздействия.

Для представления множества показателей защищенности объектов ДВ разных уровней ТИМ РИС применен метод алгебраических матриц, позволяющий формализовать и структурировать их в соответствии с целями исследования [23].

В научной работе [24] была предложена новая гибридная методика PROMETHEE-SAPEVO-M1, основанная на многокритериальных методах оценки. Она реализована на основе интеграции двух методов – PROMETHEE [25] и SAPEVO-M [26]. Предложенный методический подход позволяет проводить детальную количественную и качественную оценку массивов исходных данных, структурировать формат для расчета весовых коэффициентов предпочтительности показателей, критериев и альтернатив.

Наиболее ценной ее стороной является возможность оптимизации количества критериев с помощью их классификации на базе факторного анализа.

Данные модели и методики имеют программную реализацию [27], разработанную на языке Python, что обеспечивает информационно-аналитическую поддержку принимающему решения должностному лицу в процессе анализа и оценки объекта относительно требуемых критериев.

Применение указанных методов позволит провести первичный расчет весов событий ИБ для ввода их в НБМ.

Для обучения рассматриваемой в работе НБМ может быть применен предложенный в исследовании [28] вариант алгоритма обучения искусственного интеллекта семейства AutoAI. Данный алгоритм существенно снижает существующие недостатки самообучающихся систем искусственного интеллекта и обладает следующими преимуществами:

– реализует количественный «причинно-сравнительный анализ» на основе синтезированных обучающих данных о событиях ИБ, которые уже произошли;

– реализует количественное «корреляционное исследование», где оценивается статистическая взаимосвязь между уже свершившимися и еще не свершившимися событиями ИБ и определяются их взаимное влияние и фактические риски;

– алгоритм AutoAI может прогнозировать фактические потери, включая свершившиеся и возможные риски потерь от деструктивных событий ИБ;

– в конструкциях сценариев обучения используется стандартная аналитика с открытым исходным кодом (OSINT) для сбора общедоступных данных, включая общедоступные хранилища (базы данных);

– рассматриваемый алгоритм AutoAI и метод FAIR (метод справедливого распределения ресурсов из теории игр) интегрированы с использованием байесовской оптимизации в качестве вероятностного итеративного алгоритма, основанного на гауссовском процессе или графовой модели и функции сбора обучающих данных по направлениям «разведка» и «функционирование».

Таким образом, рассматриваемый алгоритм обучения искусственного интеллекта по своим структурным и функциональным характеристикам может быть адаптирован для обеспечения безопасности РИС.

Далее исследуем практическое применение выбранных методов моделирования для определения структурно-функциональных связей событий ИБ в РИС и их вероятностных значений.

Результаты и обсуждение

Структурно РИС можно представить совокупностью определенного количества ТИМ различного назначения. В работе определены следующие их виды. Первый из них представляют локальные информационно-вычислительные сети (ЛИВС). ТИМ второго вида – центры обработки данных (ЦОД), а третьего вида – удаленные пользователи (УП). Структура РИС определяется количеством видов ТИМ, количеством и составом элементов, что обеспечивает достижение свойства универсальности и масштабируемости моделирования.

Для определения в составе ТИМ РИС потенциальных объектов ДВ, были выделены концепты восьми уровней, соответствующих уровням модели MBOC/ISO: физического, канального, сетевого, транспортного, сеансового, представительского и прикладного, а также дополнительно включенного пользовательского уровня. Такой подход позволил идентифицировать функциональные процессы между концептами ТИМ РИС на различных уровнях. На рис. 1 представлена структура функциональных связей ТИМ РИС вида ЛИВС на сетевом и аппаратном уровнях.

В ходе построения онтологии ЛИВС можно определить функциональные связи между концептами различных уровней, а также через какие физические и логические интерфейсы на какие объекты может быть осуществлено ДВ, т.е. определить маршруты реализации сценариев УБИ.

Это позволило разработать ОСФМ объектов ДВ на каждом из уровней ТИМ РИС. В качестве примера (рис. 2) приведен фрагмент ОСФМ объектов ДВ на представительском уровне ТИМ РИС. Их уязвимости можно определить из соответствующих баз данных (БДУ).

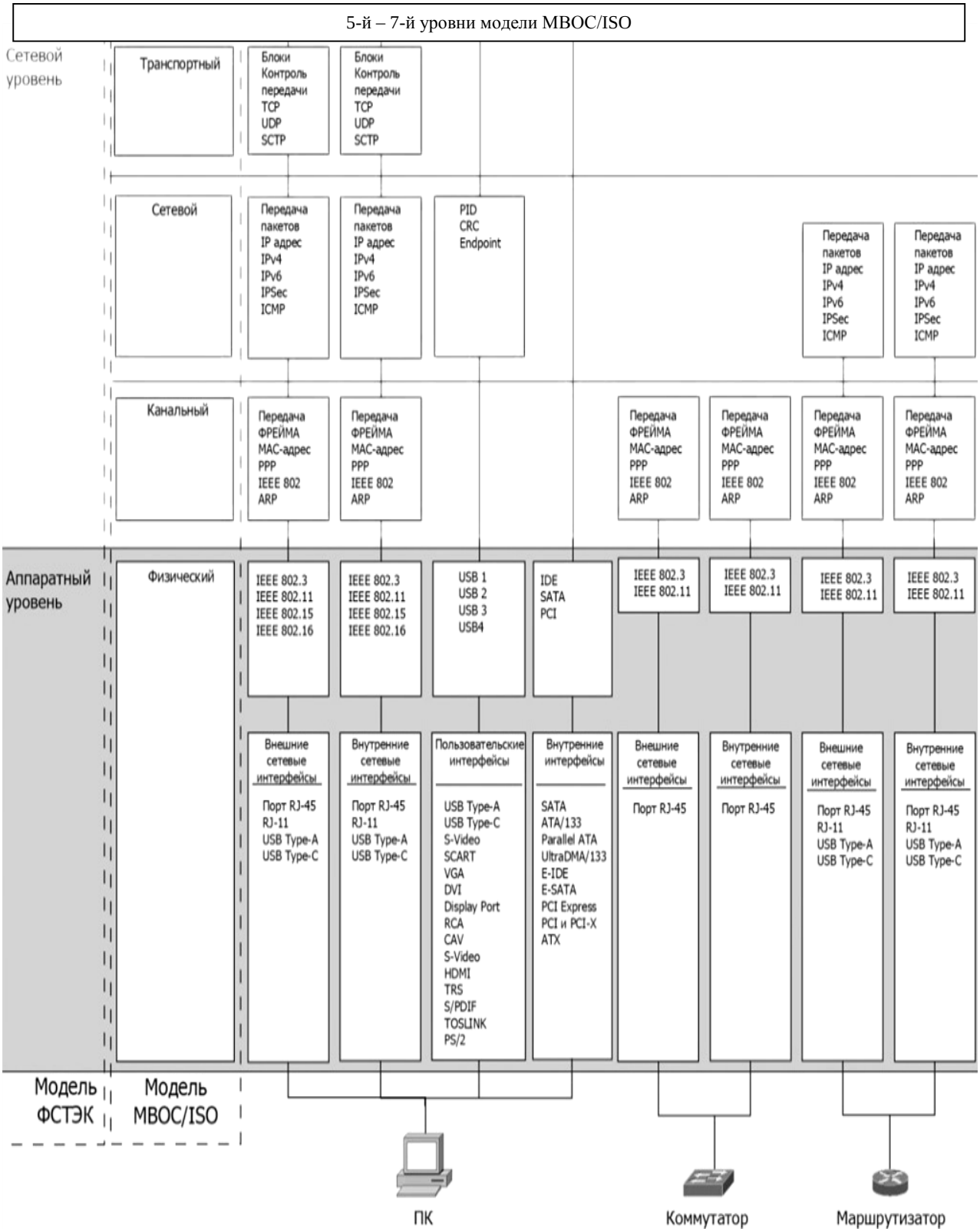


Рис. 1. Концепты и их функциональные связи на сетевом и аппаратном уровнях модели MBOC/ISO для ТИМ вида ЛИВС

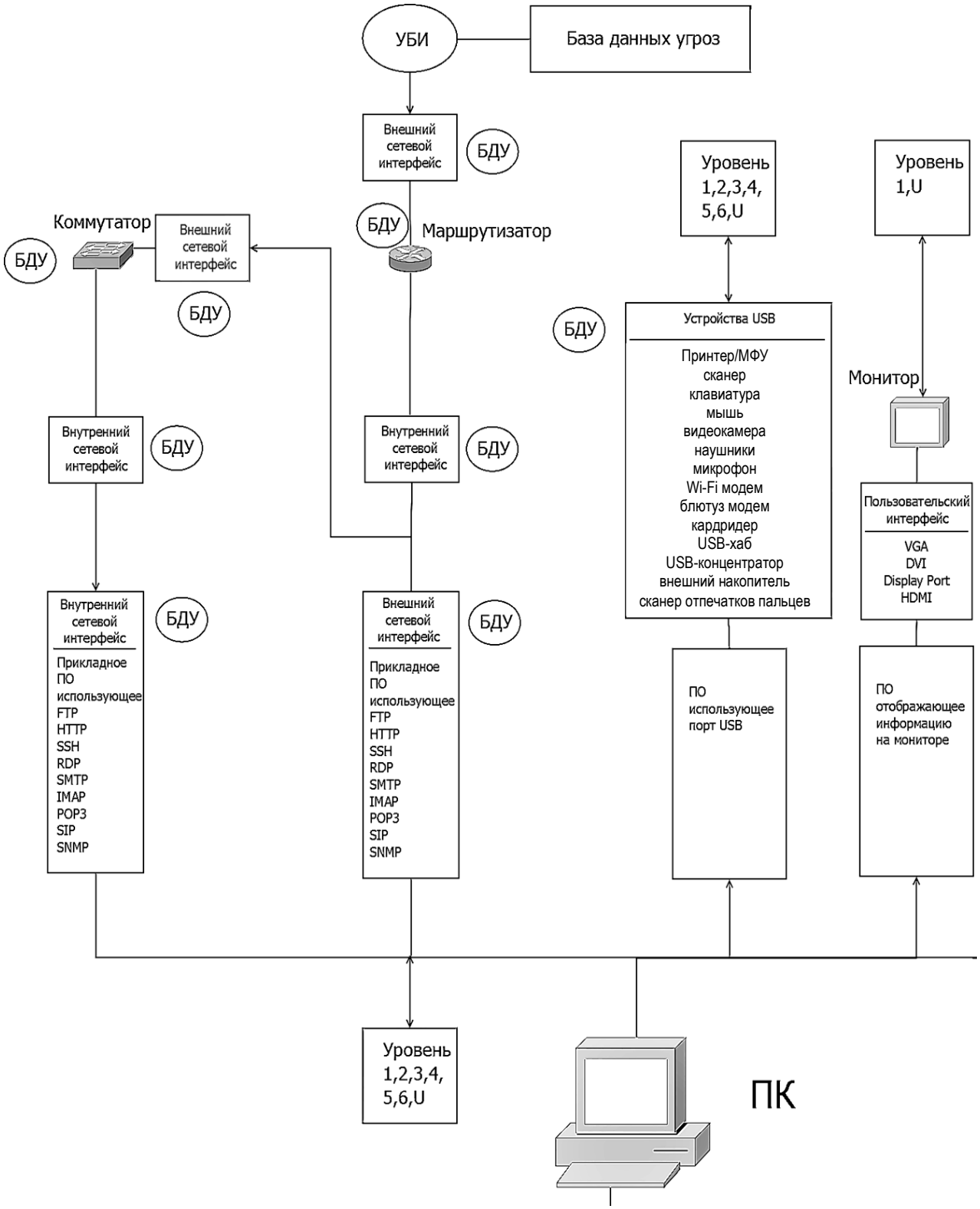


Рис. 2. Онтологическая структурно-функциональная модель объектов ДВ на представительском уровне ТИМ РИС (фрагмент)

Данные модели взаимно интегрированы и предназначены для проведения ситуационного анализа и выявления параметров, определяющих характеристики вектора ДВ на объекты восьми уровней ТИМ РИС, точки и маршруты воздействия применяемых защитных мер, взаимосвязи событий ИБ и степени их взаимовлияния. В таблице концептуально сведены объекты ДВ на уровнях модели.

Онтологические модели алгоритмично связаны с нейро-байесовскими. Основу НБМ составляют типовые кластеры, отражающие вероятностные характеристики процесса функционирования защищаемой РИС в условиях ДВ (рис. 3).

Объекты ДВ на уровнях модели

Уровни модели	Объекты деструктивного воздействия
Пользовательский	Данные пользователя (идентификационные, аутентификационные, персональные, корпоративные), информационные ресурсы
Прикладной	Прикладное программное обеспечение (ПО) (офисное, систем электронного документооборота, браузеров, моделирования, расчетное и др.)
Представительский	Операционные системы, системное ПО, системные библиотеки, платформы виртуализации. ПО поддержки протоколов
Сеансовый	Операционные системы, системное ПО, системные библиотеки, платформы виртуализации. ПО поддержки протоколов
Транспортный	Операционные системы, системное ПО, системные библиотеки, платформы виртуализации. ПО поддержки протоколов
Сетевой	Передаваемые данные (информационные, служебные и технические). Пакеты сообщений
Канальный	Передаваемые данные (информационные, служебные и технические)
Физический	Аппаратное обеспечение ПК, серверов, систем хранения данных, коммутационного и маршрутизирующего оборудования, периферийных и сетевых устройств, элементов ТКС. Каналы связи и среда передачи данных

Каждый типовой кластер НБМ представлен направленным ациклическим графом. Узлы данного графа являются событиями ИБ, выраженными отдельными вероятностными величинами, а его ребра являются условными зависимостями, подчиняющимися Гаусовскому распределению условных вероятностей.

Применив свойство симметричности байесовских и онтологических моделей, примем, что узлы байесовской сети будут соответствовать концептам онтологических моделей, а ребра – их функциональным связям. Данное свойство позволит НБМ выполнить задачу по расчету условных вероятностей событий ИБ, структурно отраженных ОСФМ. Рассмотрим более подробно данный процесс.

Каждый типовой кластер НБМ отражает события ИБ, связанные с риском реализации одной УБИ, посредством эксплуатации множества уязвимостей объекта воздействия (концепта ОСФМ) каким-либо способом и ее локализацией посредством применения ОМ и ТМ. Рассматриваются два исхода: УБИ локализована и УБИ реализована и привела к инциденту ИБ.

В составе типового кластера НБМ выделены четыре зоны событий ИБ.

1. Зона формирования рисков УБИ.
2. Зона ликвидации рисков УБИ.
3. Зона формирования рисков инцидента.
4. Зона ликвидации последствий инцидента.

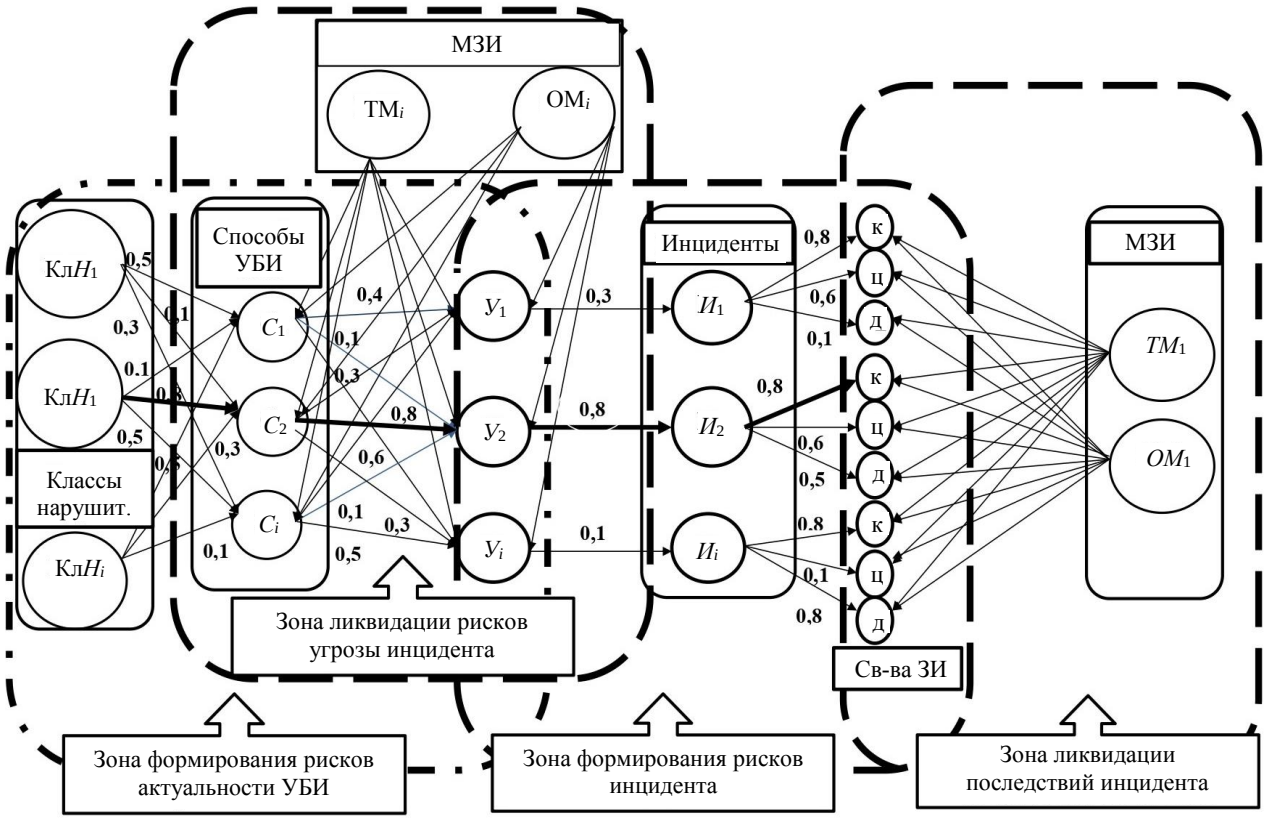


Рис. 3. Типовой кластер НБМ построения защиты элемента РИС

На сформированные ОСФМ симметрично накладывается структура типовых кластеров НБМ. Исходные данные для НБМ получаем из разработанных ОСФМ по направлению событий ИБ деструктивного и защитного характера. Весовые коэффициенты событий ИБ рассчитываются с помощью применения программного продукта PROMETHEE-SAPEVO-M1.

Зона рисков УБИ формируется на основе ОСФМ ТИМ РИС, взаимосвязей сценариев их реализации и уязвимостей объектов воздействия.

Численные значения вероятности выбора нарушителем способа реализации УБИ $P(C_i)$ будут зависеть от его возможностей, затрачиваемых ресурсов, ценности защищаемых активов, структуры ТИМ РИС, применяемых МЗИ, а также актуальных уязвимостей [29].

Применение алгоритма обучения НБМ AutoAI позволяет произвести расчет вероятностных характеристик актуальности УБИ, способов и сценариев их реализации с учетом взаимного влияния свершившихся и прогнозируемых событий ИБ, а также выбрать необходимые для их локализации ОМ и ТМ. Фрагмент данного процесса отражен на рис. 4.

Оценка защищенности ТИМ РИС осуществляется в соответствии с регулятивными документами. Эффективность способов защиты имеет вероятностные характеристики, зависящие от вектора показателей защитных мероприятий и вектора показателей способов и сценариев ДВ, а также выявленных новых актуальных уязвимостей.

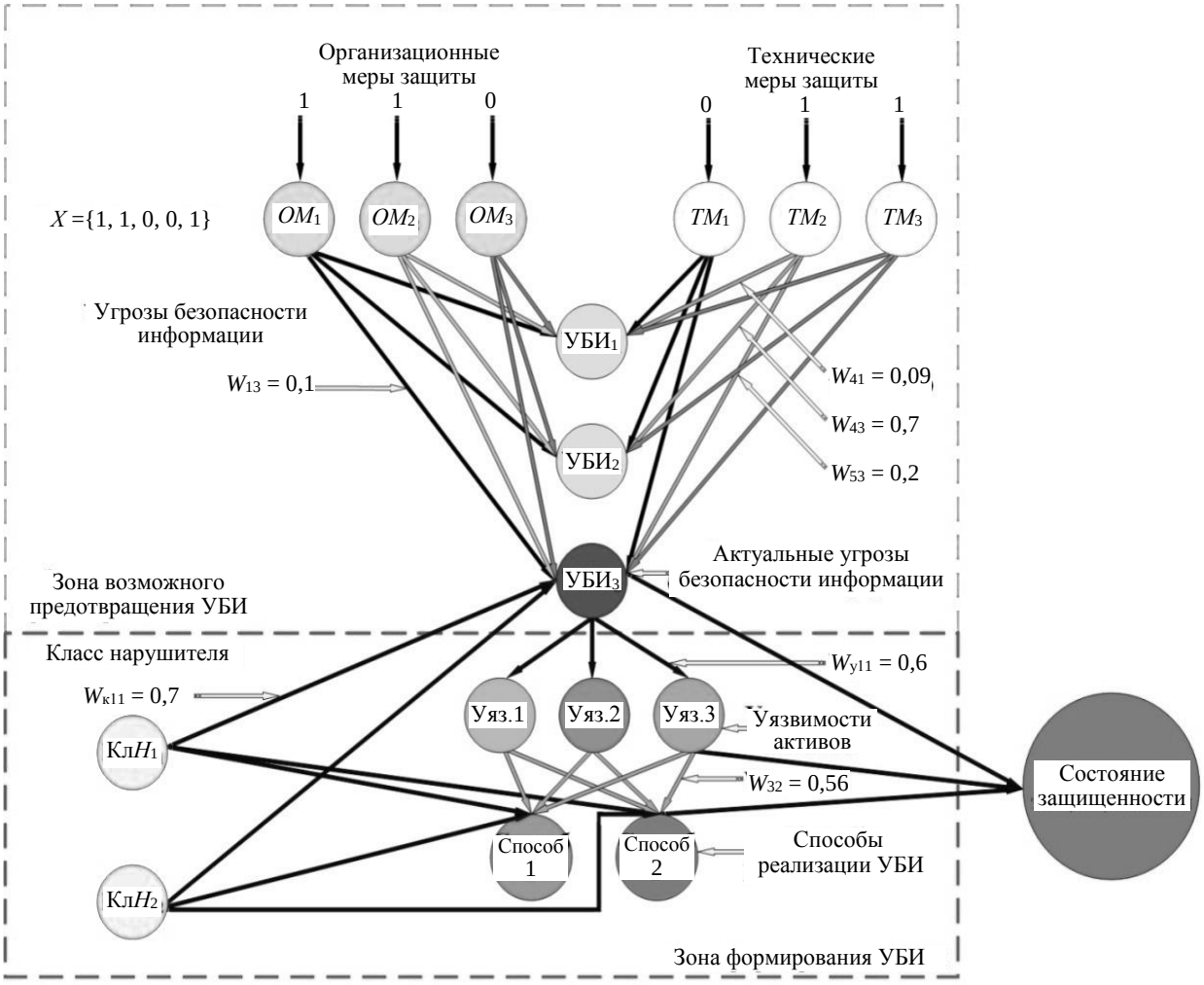


Рис. 4. Работа НБМ по определению вероятностных характеристик защищенности

Рассмотрим содержание методики и алгоритмов для расчета численных показателей оценки защищенности объектов ДВ.

Представленная в работе методика позволяет осуществлять универсальную оценку событий ИБ различного генеза по численным значениям показателей защитных и деструктивных воздействий. Такой подход минимизирует вероятность принятия неэффективного решения.

Рассмотрим алгоритм ее применения для ранее разработанной ОСФ-НБМ.

Каждая РИС состоит из ТИМ различного типа и структуры. Обозначим их через множество $\{G_1 \ldots G_i\}$. В каждом ТИМ выделены восемь уровней его структуры для определения объектов деструктивного воздействия. То есть

$$G_i \in \{F_i, K_i, L_i, T_i, S_i, A_i, P_i, H_i\}, \quad (2)$$

где F_i – физический, K_i – канальный, L_i – сетевой, T_i – транспортный, S_i – сеансовый, A_i – представительский, P_i – прикладной, H_i – пользовательский уровни i-го ТИМ.

В модели потенциальные объекты ДВ на данных уровнях представлены концептами, соединенными между собой функциональными связями.

$$K_i \in \left\{ \sum_1^m K_{F_i}, \sum_1^m K_{k_i}, \sum_1^m K_{L_i}, \sum_1^m K_{T_i}, \sum_1^m K_{S_i}, \sum_1^m K_{A_i}, \sum_1^m K_{P_i}, \sum_1^m K_{H_i} \right\}. \quad (3)$$

Каждый из данных концептов имеет определенный набор уязвимостей $\{Y_1 \ldots Y_n\}$. Уязвимости определяются в ходе проведения пентестинга и (или) мероприятий мониторинга и аудита ИБ. Обозначим эти мероприятия через индекс T_i, где i – вид тестирования на каждом из уровней. Для каждого информационного модуля введем понятие кортежа его уязвимостей, выявленных в ходе тестирования на каждом из уровней:

$$\mathbf{y}_{T_i} \in \left\{ \sum_1^n Y_{F_i}, \sum_1^n Y_{k_i}, \sum_1^n Y_{L_i}, \sum_1^n Y_{T_i}, \sum_1^n Y_{S_i}, \sum_1^n Y_{A_i}, \sum_1^n Y_{P_i}, \sum_1^n Y_{H_i} \right\}. \quad (4)$$

Для обеспечения привязки данного вектора к онтологической модели составим следующие матрицы уязвимостей концептов каждого уровня. В столбцах матрицы отображаются концепты соответствующего уровня, а в строках – обнаруженные уязвимости каждого из концептов:

$$\mathbf{G}_{iF_i} = \begin{bmatrix} K_{1F_i}Y_1 & K_{1F_i}Y_2 & \ldots & K_{1F_i}Y_n \\ K_{2F_i}Y_1 & K_{2F_i}Y_2 & \ldots & K_{2F_i}Y_n \\ K_{3F_i}Y_1 & K_{3F_i}Y_2 & \ldots & K_{3F_i}Y_n \\ K_{mF_i}Y_1 & K_{mF_i}Y_2 & \ldots & K_{mF_i}Y_n \end{bmatrix}, \quad (5а)$$

$$\mathbf{G}_{iK_i} = \begin{bmatrix} K_{1K_i}Y_1 & K_{1K_i}Y_2 & \ldots & K_{1K_i}Y_n \\ K_{2K_i}Y_1 & K_{2K_i}Y_2 & \ldots & K_{2K_i}Y_n \\ K_{3K_i}Y_1 & K_{3K_i}Y_2 & \ldots & K_{3K_i}Y_n \\ K_{mK_i}Y_1 & K_{mK_i}Y_2 & \ldots & K_{mK_i}Y_n \end{bmatrix}, \quad (5б)$$

$$\mathbf{G}_{iL_i} = \begin{bmatrix} K_{1L_i}Y_1 & K_{1L_i}Y_2 & \ldots & K_{1L_i}Y_n \\ K_{2L_i}Y_1 & K_{2L_i}Y_2 & \ldots & K_{2L_i}Y_n \\ K_{3L_i}Y_1 & K_{3L_i}Y_2 & \ldots & K_{3L_i}Y_n \\ K_{mL_i}Y_1 & K_{mL_i}Y_2 & \ldots & K_{mL_i}Y_n \end{bmatrix}, \quad (5в)$$

$$\mathbf{G}_{iT_i} = \begin{bmatrix} K_{1T_i}Y_1 & K_{1T_i}Y_2 & \ldots & K_{1T_i}Y_n \\ K_{2T_i}Y_1 & K_{2T_i}Y_2 & \ldots & K_{2T_i}Y_n \\ K_{3T_i}Y_1 & K_{3T_i}Y_2 & \ldots & K_{3T_i}Y_n \\ K_{mT_i}Y_1 & K_{mT_i}Y_2 & \ldots & K_{mT_i}Y_n \end{bmatrix}, \quad (5г)$$

$$\mathbf{G}_{iS_i} = \begin{bmatrix} K_{1S_i}Y_1 & K_{1S_i}Y_2 & \ldots & K_{1S_i}Y_n \\ K_{2S_i}Y_1 & K_{2S_i}Y_2 & \ldots & K_{2S_i}Y_n \\ K_{3S_i}Y_1 & K_{3S_i}Y_2 & \ldots & K_{3S_i}Y_n \\ K_{mS_i}Y_1 & K_{mS_i}Y_2 & \ldots & K_{mS_i}Y_n \end{bmatrix}, \quad (5д)$$

$$\mathbf{G}_{iA_i} = \begin{bmatrix} K_{1A_i}Y_1 & K_{1A_i}Y_2 & \ldots & K_{1A_i}Y_n \\ K_{2A_i}Y_1 & K_{2A_i}Y_2 & \ldots & K_{2A_i}Y_n \\ K_{3A_i}Y_1 & K_{3A_i}Y_2 & \ldots & K_{3A_i}Y_n \\ K_{mA_i}Y_1 & K_{mA_i}Y_2 & \ldots & K_{mA_i}Y_n \end{bmatrix}, \quad (5е)$$

$$\mathbf{G}_{iP_i} = \begin{bmatrix} K_{1P_i}Y_1 & K_{1P_i}Y_2 & \ldots & K_{1P_i}Y_n \\ K_{2P_i}Y_1 & K_{2P_i}Y_2 & \ldots & K_{2P_i}Y_n \\ K_{3P_i}Y_1 & K_{3P_i}Y_2 & \ldots & K_{3P_i}Y_n \\ K_{mP_i}Y_1 & K_{mP_i}Y_2 & \ldots & K_{mP_i}Y_n \end{bmatrix}, \quad (5ж)$$

$$\mathbf{G}_{iH_i} = \begin{bmatrix} K_{1H_i}Y_1 & K_{1H_i}Y_2 & \ldots & K_{1H_i}Y_n \\ K_{2H_i}Y_1 & K_{2H_i}Y_2 & \ldots & K_{2H_i}Y_n \\ K_{3H_i}Y_1 & K_{3H_i}Y_2 & \ldots & K_{3H_i}Y_n \\ K_{mH_i}Y_1 & K_{mH_i}Y_2 & \ldots & K_{mH}Y_n \end{bmatrix} \quad (5з)$$

где матрицы – уязвимости концептов соответствующих уровней: (5а) – физического; (5б) – канального; (5в) – сетевого; (5г) – транспортного; (5д) – сеансового; (5е) – представительского; (5ж) – прикладного; (5з) – пользовательского. Таким образом, мы получаем множество распределенных по уровням модели ТИМ РИС объектов ДВ и их уязвимостей, которые будут являться точками доступа для реализации УБИ каким-либо способом.

Далее предлагается провести ранжирование концептов путем присвоения им весов влияния на живучесть ТИМ РИС. В частности, вводим матрицу векторов критической значимости концептов каждого уровня ТИМ РИС следующего вида:

$$\mathbf{W}_{\mathbf{G}_i} = \begin{bmatrix} \mathbf{w}_{1K_{F_i}} & \mathbf{w}_{2K_{F_i}} & \mathbf{w}_{3K_{F_i}} & \ldots & \mathbf{w}_{mK_{F_i}} \\ \mathbf{w}_{1K_{K_i}} & \mathbf{w}_{2K_{K_i}} & \mathbf{w}_{3K_{K_i}} & \ldots & \mathbf{w}_{mK_{K_i}} \\ \mathbf{w}_{1K_{L_i}} & \mathbf{w}_{2K_{L_i}} & \mathbf{w}_{3K_{L_i}} & \ldots & \mathbf{w}_{mK_{L_i}} \\ \mathbf{w}_{1K_{T_i}} & \mathbf{w}_{2K_{T_i}} & \mathbf{w}_{3K_{T_i}} & \ldots & \mathbf{w}_{mK_{T_i}} \\ \mathbf{w}_{1K_{S_i}} & \mathbf{w}_{2K_{S_i}} & \mathbf{w}_{3K_{S_i}} & \ldots & \mathbf{w}_{mK_{S_i}} \\ \mathbf{w}_{1K_{A_i}} & \mathbf{w}_{2K_{A_i}} & \mathbf{w}_{3K_{A_i}} & \ldots & \mathbf{w}_{mK_{A_i}} \\ \mathbf{w}_{1K_{P_i}} & \mathbf{w}_{2K_{P_i}} & \mathbf{w}_{3K_{P_i}} & \ldots & \mathbf{w}_{mK_{P_i}} \\ \mathbf{w}_{1K_{H_i}} & \mathbf{w}_{2K_{H_i}} & \mathbf{w}_{3K_{H_i}} & \ldots & \mathbf{w}_{mK_{H_i}} \end{bmatrix}. \quad (6)$$

Вес (значимость) i-го концепта определяется для живучести ТИМ РИС в целом. Весовые коэффициенты определяются экспертным методом из анализа ОСФМ.

Значения весов могут изменяться в пределах от 0 до 1. Критическую значимость весов определим в интервале от 0,8 до 1.

Введем правило: «Если уязвимость в ходе тестирования вскрыта, то она должна быть защищена применением технических средств или организационных мероприятий». Для этого мы формируем матрицу векторов защитных мероприятий.

В этих целях необходимо проделать следующее.

1. Актуализировать угрозы УБИ и сценарии их реализации с применением кластера НБМ.

2. Актуализировать перечень доступных для ДВ концептов и их уязвимостей (5а)–(5з). Данные связи прописаны в базах данных.

3. Составить матрицу распределения СЗИ и проводимых режимных мероприятий. Данные связи прописаны в базах данных и базах знаний.

4. Подключить кластер НБМ, ввести данные по проведенным защитным мероприятиям.

5. Вывести отчет и убедиться, что все уязвимости закрыты и (или) риски реализации сценариев УБИ локализованы.

Однако опыт подсказывает, что абсолютно защищенных РИС нет. Это объясняется следующими причинами:

- не все уязвимости вскрыты в ходе тестирования;
- компьютерная разведка противника применила новый способ вскрытия объектов воздействия;
- противник разработал новый сценарий атаки, позволяющий обойти применяемые СЗИ;
- противник уничтожил (заблокировал) применяемые СЗИ;
- СЗИ вышли из строя в ходе эксплуатации или параметры их были настроены неправильно;
- противник получил физический доступ к элементам ИС и (или) к системе защиты информации.

В данном ракурсе весьма актуальной будет методика определения потенциальной возможности ДВ на концепты ТИМ РИС.

Для определения потенциальной возможности ДВ на концепты необходимо провести следующие действия:

1. Для каждого ТИМ РИС введем понятие вектора вероятностей обнаружения его уязвимостей компьютерной разведкой противника (7):

$$\mathbf{G}_{P_i} \in \{P_{У_1}, P_{У_2}, \ldots, P_{У_n}\}. \quad (7)$$

2. Составим матрицы вероятностей вскрытия уязвимостей ($\mathbf{P}_{\text{вск.}У_i}$), вскрытия элементов системы защиты ($\mathbf{P}_{\text{вск.СЗ}_i}$).

3. Составим матрицы вероятностей выживания i-го информационного модуля ($\mathbf{P}_{\text{выж.ТИМ}_i}$) при физическом, программном воздействии и при эксплуатации уязвимостей концептов.

4. Составим матрицы вероятностей выживания элементов системы защиты ($\mathbf{P}_{\text{выж.СЗ}_i}$) при физическом и (или) программном воздействии.

5. Составим матрицы вероятностей сохранения работоспособности при воздействии преднамеренных или непреднамеренных радиоэлектронных помех на средства защиты ($\mathbf{P}_{\text{сп.СЗ}_i}$) и элементы ТИМ ($\mathbf{P}_{\text{сп.ЭТИМ}_i}$).

6. Составим матрицы вероятностей исправного функционирования средств защиты ($\mathbf{P}_{\text{над.СЗИ}_i}$) и элементов ТИМ ($\mathbf{P}_{\text{над.ЭТМИ}_i}$) в ходе эксплуатации в условиях критического изменения параметров, в том числе и при ошибочных действиях персонала.

Расчет вероятностных характеристик пп. 3–6 должен производиться с учетом весов критичности концептов ТИМ на всех его уровнях [30].

Отмеченное ранее в исследовании свойство интегративности байесовских и онтологических моделей позволило разработать методику расчета указанных выше вероятностных характеристик деструктивного воздействия с помощью НБМ.

Порядок расчета изменения численных значений показателей защищенности ТИМ РИС в ходе функционирования представлен в следующей методике.

Суть его заключается в возможности получать обновленные значения вероятностных характеристик новых событий ИБ по мере получения информации о них.

В математической модели Байеса узлы графа, являющиеся событиями ИБ типа «Объект ДВ – уязвимость», будут получать информацию от кластеров ДВ и кластеров защитных мероприятий по мере ее поступления. При этом возможен одновременный ввод информации о событиях ИБ различного генеза в несколько узлов.

В ТИМ РИС взаимное влияние ДВ и защитных мер представлено в виде различных по структуре цепочек событий: последовательных, сходимых и расходимых.

При этом в цепочках последовательных событий могут быть однородные – (рис. 5 *а*, *б*) и разнородные – (деструктивные и защитные) события ИБ (рис. 5, *в*–*е*).

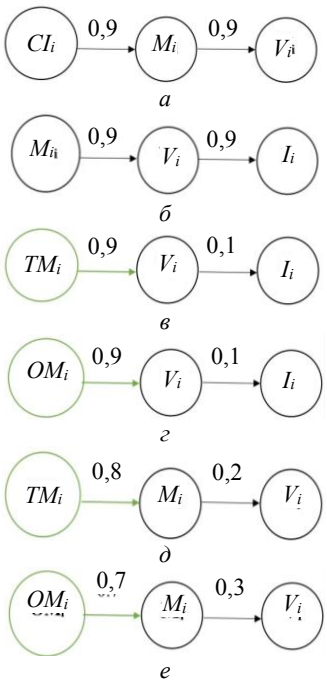


Рис. 5. Виды цепочек последовательных событий:
а, *б* – цепочки однородных (деструктивных) событий;
в–*е* – разнородные последовательности событий

Для любого набора событий расчет совместного распределения их вероятностей осуществляется по формулам (8) и (9).

Для варианта рис. 5, *а* – цепочки однородных событий – расчет производится по формуле (8):

$$P(\text{Кл}H_i У_i \mid S_i) = \frac{P(\text{Кл}H_i, S_i, У_i)}{P(S_i)} =$$

$$= \frac{P(\text{Кл}H_i)(S_i \mid \text{Кл}H_i)P(У_i \mid S_i)}{P(S_i)} =$$

$$= P(\text{Кл}H_i У_i \mid S_i)P(У_i \mid S_i). \quad (8)$$

Прочтение формулы позволяет вывести утверждение, что вероятность того, что нарушитель КлН_i сможет реализовать УБИ способом S_i, зависит от вероятности наличия актуальной для S_i уязвимости $У_i$.

Для варианта рис. 5, *в* – цепочки разнородных событий – расчет производится по формуле (9):

$$P(TM_i И_i \mid У_i) = \frac{P(TM_i, У_i, И_i,)}{P(У_i)} =$$

$$= \frac{P(TM_i)(У_i \mid TM_i)P(И_i \mid У_i)}{P(У_i)} = P(TM_i \mid У_i)P(И_i \mid У_i). \quad (9)$$

Утверждение для цепочки событий ИБ на рис. 5, *в*: вероятная эффективность *ТМ* будет зависеть от вероятности наличия незакрытой уязвимости объекта ДВ.

Для цепочек последовательных событий на рис. 5, *б–е* формулы и утверждения о вероятностных зависимостях событий ИБ составляются аналогично приведенным выше примерам.

Рассмотрим взаимное влияние событий ИБ деструктивного и защитного характера представленных в виде сходимых цепочек (рис. 6).

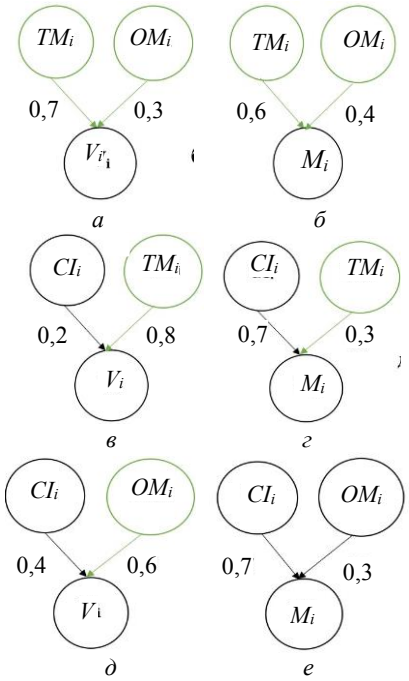


Рис. 6. Виды сходимых цепочек событий

Расчет их совместного распределения вероятностей для варианта рис. 6, *а* может быть произведен по формуле (10):

$$P(TM_i, OM_i, У_i) = \sum_{У_i} P(TM_i)P(OM_i)P(У_i \mid OM_i, TM_i) =$$

$$= P(OM_i \mid У_i)P(TM_i \mid У_i). \quad (10)$$

Утверждение для цепочки расходимых событий ИБ на рис. *б, а*: вероятность актуальности уязвимости $У_i$ будет зависеть от вероятностей ее ликвидации с помощью ОМ_i и (или) ТМ_i.

Для цепочек последовательных событий на рис. 5, *е* и рис. 6, *а*, *б* формулы и утверждения о вероятностных зависимостях событий ИБ составляются в соответствии с приведенным примером (10).

Взаимное влияние деструктивных воздействий и МЗИ в виде цепочек расходимых событий представлено на рис. 7.

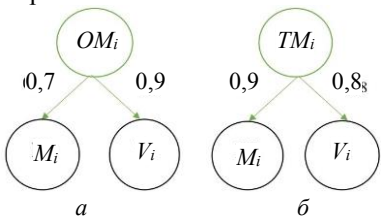


Рис. 7. Виды расходимых цепочек событий

Совместное распределение вероятностей для сходимой последовательности событий ИБ рассчитывается по формуле (11):

$$P(S_i, У_i \mid TM_i) = \frac{P(TM_i, S_i, У_i)}{P(TM_i)} = P(S_i \mid TM_i)\, P(У_i \mid TM_i). \quad (11)$$

Утверждение для цепочки сходимых событий ИБ: вероятность актуальности уязвимости $У_i$ и возможности ее эксплуатации способом S_i будет зависеть от вероятностей их нейтрализации защитными мерами (рис. 7, *а* – OM_i и (или) рис. 7, *б* – TM_i).

Разработанная методика позволяет рассчитать изменения численных значений вероятности событий при возможном наступлении (свершении) других событий, т.е. в динамике рассчитывать вероятностные зависимости деструктивных и защитных.

Выводы и заключение

В представленной работе выполнена научная задача и получены следующие результаты.

Первым научным вкладом стал предложенный подход, связанный с декомпозицией элементов распределенной информационной системы по уровням модели MBOC/ISO и определением объектов (концептов) ДВ на каждом из этих уровней. Это позволяет выявить уязвимости каждого концепта, определить точки входа и пути распространения УБИ и, следовательно, сформировать векторы тактик и сценариев их реализации.

Следующим научным вкладом стала разработка онтологической структурно-функциональной модели ТИМ РИС, интегрированной с вероятностной нейро-байесовской моделью. Такая интеграция двух разнотипных моделей стала возможной благодаря выявленным в ходе исследования свойствам симметричности структуры элементов РИС, реализуемых ими процессов и событий ИБ различного генеза. Это позволило получить новое качество интегрированной модели – возможность оценивать зависимости вероятностей исправного функционирования процессов в ТИМ РИС от реализации событий ИБ.

Разработанные и примененные в модели типовые информационные модули и типовые кластеры вероятностей событий информационной безопасности обеспечивают свойства универсальности и масштабируемости модели.

Предложенные методики позволяют определять степень критичности для РИС объектов ДВ, их уязвимостей, векторы атак и векторы защитных мер. В результате мы получаем технологическую карту состояния безопасности РИС или ее элемента.

Первичный расчет вероятностей событий ИБ деструктивного и защитного характера (их весов) может быть произведен с применением метода и программного продукта PROMETHEE-SAPEVO-M1.

В динамике оперативного управления их перерасчет осуществляется с применением формул Байеса для последовательных, сходящихся и расходящихся цепочек событий. Предлагаемый для использования алгоритм обучения НБМ позволяет проводить расчеты взаимных вероятностей событий ИБ.

Направлением дальнейших исследований в данной области будут разработка методик, реализующих формализованные алгоритмы определения сценариев, тактик и техник реализации УБИ и определения их предпочтительности для складывающейся ситуации. Также интересной будет разработка баз данных и баз знаний для обучения НБМ с применением предлагаемого варианта алгоритма AutoAI и расширение области применения методики и программного продукта PROMETHEE-SAPEVO-M1 в разработанной СППР.

Практическая значимость результатов исследования заключается в их использовании в деятельности организаций, осуществляющих проведение аттестаций РИС. Применение результатов исследования позволяет значительно сократить сроки проведения работ по формированию модели УБИ и повысить показатели обоснованности принятых решений и достоверности результатов оценки защищенности ТИМ РИС.

Работа выполнена в рамках реализации программы ЛИЦ «Доверенные сенсорные системы» (договор № 009/20 от 10.04.2020) при финансовой поддержке Минкомсвязи России и АО «РВК». Идентификатор соглашения о предоставлении субсидии – 0000000007119P190002.

Литература

1. A multi-criteria and statistical approach to sup–port the analysis of the superiority of OECD countries / D.A. De Moura Pereira, M. Dos Santos, I.P. De Araujo Costa, M.A.L. Moreira, A.V. Terra, S. De Souza Rocha, K. F. S. Gomez // IEEE Access: Interdisciplinary Open Access, VOLUME 10, 2022 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/9810236, свободный (дата обращения: 20.06.2022).

2. Gomez L. Multicriteria ranking with ordinal data / L. Gomez, A.-R. Muri, K.F.S. Gomez // Syst. Anal. – 1997. – Vol. 27, No. 2. – P. 139–146.

3. Multi-criteria analysis applied to the selection of aircraft by the Brazilian Navy / S.M.N. Maeda, I.P.A. Costa, M.A.P. Castro Junior, L.P. Favero, A.P.A. Costa, H.V.P. Corrisa, K.F.S. Gomez, M. Santos. – Prodution [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/353776847, свободный (дата обращения: 20.06.2022).

4. Баранов В.В. Св-во о гос. регистрации программы для ЭВМ № 2022665542 «Информационная система поддержки принятия решений при разработке системы защиты информации» (ИС ППР РСЗИ). Дата поступления: 12 августа 2022 г. Дата государственной регистрации в Реестре программ для ЭВМ: 17 августа 2022 г.

5. Международный стандарт ISO/IEC 15408-3:2022. Информационная безопасность, кибербезопасность и защита конфиденциальности – Критерии оценки ИТ-безопасности. – Ч. 3: Компоненты обеспечения безопасности [Электронный ресурс]. – Режим доступа: https://www.iso.org/home.html, свободный (дата обращения: 08.06.2022).

6. Международный стандарт ISO/IEC 27000. Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Обзор и словарь [Электронный ресурс]. – Режим доступа: https://pqm–online.com/assets/files/pubs/translations/std/iso-mek-27000-2016.pdf, свободный (дата обращения: 08.06.2022).

7. Методический документ. Утвержденная ФСТЭК России 5 февраля 2021 г. «Методика оценки угроз информационной безопасности» [Электронный рессурс]. – Режим доступа: https://fstec.ru/ tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g, свободный (дата обращения: 08.06.2022).

8. Key concepts of a systemological approach to adaptive monitoring of information security CPS / M. Poltavtseva, A. Shelupanov, D. Bragin, D. Zegda, E. Alexandrova // Symmetry. – 2021. – Vol. 13 (12). – P. 2425.

9. Industrial cyber-physical systems: risks assessment and attacks modeling / A.G. Kravets, N. Salnikova, K. Dmitrenko, M. Lempert. – 2020. – Vol. 260. – P. 197–210.

10. Стандарт ISO/IEC. 7498-1. Информационные технологии. Базовая эталонная модель: Базовая модель [Электронный рессурс]. – Режим доступа: https://www.ecma-international.org/wp-content/uploads/ s020269e.pdf, свободный (дата обращения: 12.06 2022).

11. Рассел С. Искусственный интеллект: современный подход: пер. с англ. / С. Рассел, П. Норвиг. – 2-е изд. – М.: ИД «Вильямс», 2016. – 1408 с.

12. Джиарратано Д. Экспертные системы: принципы разработки и программирования. – 4-е изд.; пер. с англ. – М.: ИД «Вильямс», 2007. – 1147 с.

13. Maksimova E. Prediction of destructive harmful effects on the object of critical information infrastructure / E. Maksimova, V. Baranov // Communications in Computer and Information Science book series (CCIS). – 2021. – Vol. 1395. – P. 88–99. DOI: 10.1007/978-981-16-1480-4_8.

14. Массель Л. Интеллектуальные инструменты поддержки для принятия стратегических решений по развитию интеллектуальных сетей / Л. Массель, А. Массель. – Вебсайт конференций E3S. – 2018 [Электронный рессурс]. – Режим доступа: https://doi.org/10.1051 /e3sconf/20186902009, свободный (дата обращения: 08.06 2022).

15. Скворцов Н.А. Вопросы согласования разнородных онтологических моделей и онтологических контекстов. Онтологическое моделирование / под ред. Л.А. Калиниченко: матер. семинара. – М.: ИПИ РАН, 2008. – С. 149–166.

16. Перл Д. Лаборатория когнитивных систем Калифорнийского университета. – Лос-Анджелес, Байесовские сети. – М.: Мир, 2000. – 102 с.

17. Azar A.T. Adaptive neuro-fuzzy systems. Fuzzy systems. – IN-TECH, Austria, 2010. – P. 85–110.

18. Ficilis P. Software project management technologies: an overview / P. Ficilis, V. Gerogiannis, L. Anthopoulos // Jour-

nal of Software and Application Development. – 2014. – P. 1096–1110.

19. Herzog A. Ontology of Information Security. International Journal of Information Security and Con-fidentiality. – 2007. – Vol. 1 (4). – P. 1–23.

20. Jaxen F. Bayesian networks and decision-making graphs. – M.: Sprinnger, 2001. – P. 54–120.

21. Singhal A. Security risk analysis of corporate networks using probabilistic attack graphs. Network security indicators. – Cham, 2017. – P. 53–73.

22. Egoshin N.S. Model of threats to the confidentiality of information processed in cyberspace, based on the model of information flows / N.S. Egoshin, A.N. Konev, A.N. Shelupanov // Symmetry. – 2020. – Vol. 12, iss. 11. – P. 1–18.

23. Катасёв А.С. Нейронечеткая модель формирования правил классификации как эффективный аппроксиматор объектов с дискретным выходом // Кибернетика и программирование. – 2018. – № 6. – С. 110–122.

24. PROMETHEUS-SAPEVO-M1 Hybrid approach based on ordinal and cardinal input data: multi-criteria evaluation of helicopters to support operations of the Brazilian Navy / M.A.L. Moreira, I.P. de Araujo Costa, M.T. Pereira, M. dos Santos, K.F.S. Gomez, F.M. Muradas // Algorithms. – 2021. – Vol. 14, No. 140 [Электронный ресурс]. – Режим доступа: https:// doi.org/10.3390/a14050140, свободный (дата обращения: 22.06.2022).

25. Brans J.-P. The method of ranking the preferences of an organization: The PROMETHEE method for making decisions based on several criteria / J.-P. Brans, P. Vinke // Management. Science. – 1985. – Vol. 31, No. 6. – P. 647–656.

26. SAPEVO-M: a method of group multicriteria ordinal ranking / K.F.S. Gomez, M. dos Santos, L.F.H. de Souza de Barros Teixeira, A.M. Sanseverino, M.R.S. dos Barcelos // Pesquisa Operacional. – 2020. – Vol. 40, No. 40. – P. 1–23. DOI: 10.1590/0101–7438.2020.040.00226524.

27. PROMETHE-SAPEVO-M1 hybrid modeling proposal: Multi-criteria evaluation of unmanned aerial vehicles for use in naval warfare / M.L. Moreira, K.F.S. Gomez, M. dos Santos, M.S. dos Carmo, J.V.G.A. Araujo // Proc. Int. Joint Conference on Industrial Engineering and Operations Management. – 2020. – Vol. 337. – P. 381–393. DOI: 10.1007/978-3-030-56920-4_31.

28. Radanliev P. Improving the cybersecurity of the healthcare system with the help of self-optimizing and self-adapting artificial intelligence (Part 2) / P. Radanliev, D. De Ruhr // Healthcare technology. – 2022. – Vol. 12. – P. 923–929 [Электронный ресурс]. – Режим доступа: https://doi.org/ 10.1007/s12553-022-00691-6, свободный (дата обращения: 22.08.2022).

29. Robotic system for analyzing information systems and communication networks in the field of cybersecurity / V.V. Baranov, Yu.Yu. Gromov, O.S. Lauta, E.A. Maksimova, N.P. Sadovnikova, L.V. Tretyakova // Journal of Physics: Conference Series. International Conference on Information Technologies in Business and Industry, ITBI–2020. – Bristol, England, 2020. – P. 12–19.

30. Koryshev N. Building a fuzzy classifier based on the whale optimization algorithm for detecting network intrusions / N. Koryshev, I. Khodashinsky, A. Shelupanов // Symmetry. – 2021. – No. 13 (7). – P. 1211.

Баранов Владимир Витальевич
Канд. военных наук, доцент, зав. каф. информационной безопасности Южно-Российского государственного политехнического университета (НПИ) им. М.И. Платова
Просвещения ул., 132, г. Новочеркасск, Россия, 346428
Тел.: +7-928-100-05-98
Эл. почта: baranov.vv.2015@yandex.ru

Шелупанов Александр Александрович
Д-р техн- наук, профессор,
президент Томского государственного университета систем управления и радиоэлектроники
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-813-929-40-80
Эл. почта: saa@tusur.ru

Baranov V.V., Shelupanov A.A

Cognitive model for assessing the security of information systems for various purposes

The paper substantiates the relevance of the development of a cognitive model for assessing the security of information systems for various purposes, designed to support decision-making by officials of information security management bodies, analyzes scientific papers and research in this area, formulates requirements for the functional capabilities of the model, investigates and identifies the most appropriate modeling tools, develops integrated ontological and neuro-Bayesian models typical clusters of information systems, tactics and techniques for the implementation of UBI through the vulnerabilities of objects of various levels of the ISO/OSI model, protective and attacking influences, allowing to identify such objects of influence, their current vulnerabilities and scenarios for the implementation of information security threats, to calculate the joint probability distribution of information security events of various genesis, as well as to simulate the process of operational management of information security

Keywords: ontological model; neuro-Bayesian model, impact objects, vulnerabilities, structural survivability, functional survivability, information security measures.
DOI: 10.21293/1818-0442-2022-25-4-88-100

References

1. De Moura Pereira D.A., Dos Santos M., De Araujo Costa I.P., Moreira M.A.L., Terra A.V., De Souza Rocha S., Gomez K.F.S. A multi-criteria and statistical approach to support the analysis of the superiority of OECD countries. IEEE Access: Interdisciplinary Open Access, Vol. 10, 2022. Available at: https://ieeexplore.ieee.org/document/9810236, free (Accessed: June 20, 2022).

2. Gomez L., Muri A.-R., Gomez K.F.S. Multicriteria ranking with ordinal data. *System Analysis*, 1997, vol. 27, no. 2, pp. 139–146.

3. Maeda S.M.N., Costa I.P.A., Castro Junior M.A.P., Favero L.P., Costa A.P.A., Corrisa H.V.P., Gomez K.F.S., Santos M. Multi-criteria analysis applied to the selection of aircraft by the Brazilian Navy. Prodution, Available at: https://www.researchgate.net/publication/ 353776847, free (Accessed: June 20, 2022).

4. Certificate of state registration of the computer program № 2022665542 «Information system for decision making support in the development of an information security system» (IS PPR RSSI). V.V. Baranov, Received date August 12, 2022. Date of state registration in the Register of computer programs on August 17, 2022.

5. International standard ISO/IEC 15408-3:2022. Information Security, Cybersecurity and Privacy Protection – IT Security Assessment Criteria. Part 3: Security Components. Available at: https://www.iso.org/ home.html, free *(*Accessed: June 20, 2022) (in Russ.)

6. International Standard ISO/IEC 27000 Information Technology – Security methods – Information security management systems – Overview and dictionary. Available at: https://pqm-online.com/assets/files/pubs/translation/STD/ISO-

IEC-27000-2016.PDF format, free (Accessed: June 20, 2022) (in Russ.)

7. Methodological document. Approved by the FSTEC of Russia on February 5, 2021, Methodology for assessing threats to information security. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/doku-menty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g, free. (Accessed: June 20, 2022). (In Russ.)

8. Poltavtseva M., Shelupanov A., Bragin D., Zegda D., Alexandrova E. Key concepts of a systemological approach to adaptive monitoring of information security CPS. *Symmetry*, 2021, vol. 13 (12), p. 2425.

9. Kravets A., N. Salnikova, K.Dmitrenko, M. Lempert. Industrial cyber-physical systems: risk assessment and attack modeling. *Research in the field of systems, decision-making and control*. 2020, vol. 260, pp. 197–210 (in Russ.)

10. ISO/IEC. 7498-1 STANDARD Information technologies. Basic Reference Model: Basic model [Electronic resource]. Available at: https://www.ecma-international.org/wp-content/uploads/s020269e.pdf, free (Accessed: June 12, 2022) (in Russ.)

11. Russell S., Norvig P. Artificial intelligence: a modern approach. Second Edition. USA, New Jersey, Pirson Education, 1995. 1043 p. (in Russ.).

12. Giarratano D. Expert Systems: Principles and Programming. 3rd Edition. USA, MA, Boston, PWS Publishing, 1998, 288 p.

13. Baranov V., Maksimova E. Prediction of destructive harmful effects on the object of critical information infrastructure. *Communications in Computer and Information Science Book Series (CCIS*), 2021, vol. 1395, p. 88–99. DOI: 10.1007/978-981-16-1480-4_8.

14. Massel L., Massel A. Intelligent support tools for making strategic decisions on the development of intelligent networks. *E3S Conference website successfully 2018.* Available at: https://doi.org/10.1051 /e3sconf/20186902009, free (Accessed: June 08, 2022) (in Russ.)

15. Skvortsov N.A. Issues of coordination of different ontological models and ontological contexts. Ontological modeling. *Edited by L.A. Kalinichenko: Materials of the seminar. M.: IPI RAS*. 2008, pp. 149–166 (in Russ.)

16. Pearl D. Laboratory of Cognitive Systems, University of California, Los Angeles. Bayesian Networks. *Moscow: Mir*, 2000, 102 p. (in Russ.)

17. Azar A.T. Adaptive neuro-fuzzy systems. Fuzzy systems. *IN-TECH, Austria*, 2010, pp. 85–110.

18. Ficilis P., Gerogiannis V., Anthopoulos L. Software project management technologies: an overview. *Journal of Software and Application Development*, 2014, pp. 1096–1110.

19. Herzog A. Ontology of Information Security. *International Journal of Information Security and Confidentiality*. 2007, no. 1 (4). p. 1–23.

20. Jaxen F. Bayesian networks and decision-making graphs. *M.: Springer*, 2001, pp. 54–120.

21. Singhal A. Security risk analysis of corporate networks using probabilistic attack graphs. *Network Security Indicators. Cham*, 2017, pp. 53–73.

22. Egoshin N.S., Konev A.N., Shelupanov A.A. Model of threats to the confidentiality of information processed in cyberspace, based on the model of information flows. *Symmetry*, 2020, vol. 12, Issue 11, 1840, pp. 1–18.

23. Katasev A.S. A neuro-fuzzy model for the formation of classification rules as an effective approximator of objects with a discrete output. *Cybernetics and Programming*, 2018, no. 6, pp. 110–122 (in Russ.)

24. Moreira M.A.L., de Araujo Costa I.P., Pereira M.T., dos Santos M., Gomez K.F.S., Muradas F.M. PROMETHEUS-SAPEVO-M1 Hybrid approach based on ordinal and cardinal input data: multi-criteria evaluation of helicopters to support operations of the Brazilian Navy. *Algorithms*, 2021, vol. 14, no. 140. Available at: https:// doi.org/10.3390/a14050140, free (Accessed: June 20, 2022).

25. Brans J.-P., Vinke P. The method of ranking the preferences of an organization: The PROMETHEE method for making decisions based on several criteria. *Management. Science*, 1985 vol. 31, no. 6, pp. 647–656.

26. Gomez K.F.S., dos Santos M., de Souza de Barros Teixeira L.F.H., Sanseverino A.M., dos Barcelos M. R. S. SAPEVO-M: a method of group multicriteria ordinal ranking. *Pesquisa Operacional*, 2020, vol. 40, no. 40, pp. 1–23, DOI: 10.1590/0101-7438.2020.040.00226524.

27. Moreira M.L., Gomez K.F.S., dos Santos M., dos Carmo M.S., Araujo J.V.G.A. PROMETHE-SAPEVO-M1 hybrid modeling proposal: Multi-criteria evaluation of unmanned aerial vehicles for use in naval warfare. *Proceedings of International. Joint Conference on Industrial Engineering and Operations Management*, 2020, vol. 337, pp. 381–393, DOI: 10.1007/978-3-030-56920-4_31.

28. Radanliev P., De Ruhr D. Improving the cybersecurity of the healthcare system with the help of self-optimizing and self-adapting artificial intelligence (Part 2). *Healthcare Technology*, 2022, vol. 12, pp. 923–929. Available at: https://doi.org/10.1007/s12553-022-00691-6, free (Accessed: August 22, 2022).

29. Baranov V.V., Gromov Yu.Yu., Lauta O.S., Maksimova E.A., Sadovnikova N.P., Tretyakova L.V. Robotic system for analyzing information systems and communication networks in the field of cybersecurity. *Journal of Physics: Conference Series. International Conference on Information Technologies in Business and Industry, ITBI-2020. Bristol, England*, 2020, pp. 12–19.

30. Koryshev N., Khodashinsky I., Shelupanov A. Building a fuzzy classifier based on the whale optimization algorithm for detecting network intrusions. *Symmetry*, 2021, vol. 13 (7), p. 1211.

Vladimir V. Baranov
Candidate of Military Sciences, Associate Professor,
Head of the Department of «Information Security»,
South Russian State Polytechnic University (NPI)
named after M.I. Platov
132, Prosveshcheniya str., Novocherkassk, Russia, 346428
Phone: +7-928-100-0-598
Email: kaf-ib@npi-tu.ru

Aleksandr A. Shelupanov
Doctor of Science in Engineering, Professor,
President of Tomsk State University of Control Systems
and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-813-929-40-80
Email: saa@tusur.ru

УДК 004.056.52

Е.А. Кушко, Д.А. Грачёв, Н.Ю. Паротькин, В.В. Золотарёв

О вопросах безопасности киберфизических систем

Киберфизические системы находят все более широкое применение во всех отраслях. С ростом распространения этих систем увеличивается и число атак на них. Рассмотрены основные технологии, используемые для построения киберфизических систем, меры безопасности, реализуемые в них, их преимущества, недостатки и уязвимости. Также авторами приведен общий подход к обеспечению безопасности киберфизических систем.
Ключевые слова: киберфизические системы, сенсорные сети, интернет вещей, уязвимость.
DOI: 10.21293/1818-0442-2022-25-4-101-109

Киберфизическая система – это комплексная система, состоящая из вычислительных и физических элементов, которая постоянно получает данные из окружающей среды и использует их для дальнейшей оптимизации процессов управления [1]. Примерами такой системы могут являться: «умный» дом, «умный» город и другие «умные» автоматизированные системы управления. Ключевой особенностью киберфизических систем является связывание физических процессов производства или других процессов, которые требуют непрерывного управления в реальном времени с программно-аппаратными системами [2].

Интернет вещей (Internet of things, IoT) – это динамичная распределенная среда, которая связывает множество интеллектуальных устройств, способных воспринимать окружающую среду и выполнять соответствующие действия [3]. Такие устройства позволяют отслеживать состояние внешней среды, собирать информацию о реальном мире и создавать системы повсеместных вычислений, в которых каждое устройство может взаимодействовать с любым другим устройством в мире, где бы оно ни находилось. IoT-технологии обеспечивают совместную работу устройств – как отдельных датчиков или как совокупности различных датчиков, образующих конечную макросистему и действующих как единое целое.

Понятие киберфизических систем часто рассматривают совместно с понятием интернета вещей. Оба типа систем имеют схожие элементы, однако киберфизические системы являются более широким понятием и имеют более сложную архитектуру. Главная схожесть архитектур заключается в том, что на нижнем уровне киберфизических систем и систем интернета вещей лежит сенсорная сеть. Сенсорная сеть представляет собой динамическую, самоорганизующуюся и распределенную сеть датчиков и исполнительных устройств. Она предназначена для решения задач автоматизации, диагностики, телеметрии и межмашинного взаимодействия. Сенсорная сеть должна быть проста в создании и эксплуатации, нетребовательна к частому техническому обслуживанию, обладать высокой отказоустойчивостью и надежностью, а также быть легко масштабируемой [4].

Технологии передачи данных

Технология передачи данных сенсорной сети выбирается в зависимости от требований по дальности и энергопотреблению, уровня шума и производительности устройств. На первый взгляд, многие беспроводные стандарты, применяющиеся в сенсорных сетях, имеют схожие свойства, однако эти стандарты разработаны для решения разных задач и, соответственно, функционируют по-разному. В табл. 1 приведена сравнительная таблица популярных стандартов.

Таблица 1

Сравнительная характеристика стандартов беспроводной связи сенсорных сетей

Технология беспроводной передачи данных (стандарт)	Bluetooth (IEEE 802.15.1)	Wi-Fi (IEEE 802.11b)	ZigBee (IEEE 802.15.4)	LoRa	Z-Wave
Частотный диапазон, ГГц	2,4–2,483	2,4–2,483	2,4–2,483	2,4–2,483	0,8–0,9
Пропускная способность, кбит/с	723,1	11 000	250	до 50	до 100
Размер стека протокола, Кбайт	Более 250	Более 1000	32–64	64	64
Время непрерывной автономной работы от батареи, дни	1–100	0,5–5	100–1000	365–1000	90–700
Максимальное количество узлов в сети	7	10	65 536	1000	232
Диапазон действия, м (усредненные значения)	10–100	20–300	10–100	500	40–100
Область применения	Создание персональных сетей	Создание локальных сетей	Удаленный мониторинг и управление	Удаленная передача информации	Удаленный мониторинг и управление

Из-за того, что устройства сенсорной сети должны функционировать достаточно длительное время в сложных условиях, это накладывает ограничения на их размер, дальность передачи данных, энергопотребление. Кроме того, устройств требуется вплоть до несколько тысяч в зависимости от решаемых за-

дач. Поэтому такие устройства имеют низкую стоимость, низкую производительность и функционируют в условиях низкой пропускной способности [4].

На безопасности сенсорных сетей сказывается отсутствие механизмов обнаружения вторжений, аутентификации и шифрования. В силу низкой производительности и стоимости устройств средства и механизмы защиты, как правило, сильно упрощены, что делает эти устройства уязвимыми. Все вышеперечисленные факторы влияют на то, что злоумышленник может с минимальными затратами проникнуть в сенсорную сеть [5].

Задачи, которые решает сенсорная сеть, требуют от неё соответствия следующим характеристикам: автономность, надежность, отказоустойчивость и масштабируемость. В некоторых случаях может стоять задача сбора и анализа данных в режиме реального времени, что дополнительно накладывает требования к задержкам. Поэтому и меры защиты, реализуемые в сенсорных сетях, направлены на обеспечение высокой доступности: обеспечения устойчивых каналов связи, построение оптимальных маршрутов, защита от внешних воздействий и т.д.

Bluetooth

Сеть Bluetooth имеет топологию типа «звезда» или ячеистой сети и использует высоконагруженный диапазон 2,4 ГГц, что вносит помехи при организации связи. Поддержка стандартом Bluetooth небольшого числа узлов в сети ограничивает разработчиков систем в построении систем со сложной структурой. Сенсорная сеть на базе Bluetooth не является надежным решением. Однако широкая распространенность данного стандарта позволяет достаточно легко взаимодействовать с конечными устройствами сенсорной сети при помощи персональных мобильных устройств. Стандарт Bluetooth охватывает все уровни модели OSI. Данный стандарт поддерживает механизмы аутентификации и шифрования сообщений как на уровне сети, так и на прикладном уровне, однако имеет ряд существенных уязвимостей [6].

Wi-Fi

Сеть Wi-Fi имеет централизованную структуру, а соответственно единую точку отказа, так как типичная топология сети Wi-Fi – это «звезда» или «дерево». Выход из строя одного маршрутизатора нарушает нормальное функционирование всей сети. Механизм добавления новых узлов не позволяет гибко наращивать масштаб сенсорной сети. Высокая пропускная способность сети Wi-Fi связана с высоким энергопотреблением. Скорости, предлагаемые стандартом Wi-Fi, избыточны для сенсорной сети, для неё гораздо важнее низкое энергопотребление. Несмотря на широкую распространённость данного беспроводного стандарта, существуют более дешевые решения, которые лишены указанных недостатков. Но у сети Wi-Fi есть значительное преимущество – это возможность применения средств защиты информации, которые используются для защиты обычных локальных сетей. Wi-Fi охватывает только физический и канальный уровни модели OSI, соответственно, у разработчиков системы есть возможность гибкого конфигурирования и использования протоколов других уровней. Однако это и снижает совместимость устройств разных производителей между собой.

ZigBee

Сеть ZigBee имеет ячеистую топологию. В сети ZigBee существует две модели безопасности: распределенная модель и централизованная модель [7]. В обоих моделях безопасности используется шифрование AES-128 как на сетевом уровне, так и на уровне приложений. ZigBee также предусматривает проверку целостности при помощи механизма Message Integrity Check (MIC). Однако для подключения к сети ZigBee используется глобальный заранее сгенерированный ключ для подключения к сети (pre-configured global link key), который имеет значение по умолчанию. Этот ключ используется для обеспечения совместимости устройств ZigBee от различных производителей. Для повышения уровня защищенности необходимо прописывать во все устройства в сети ZigBee нестандартный ключ, иначе сеть будет уязвима для проникновения злоумышленником. Также злоумышленник может перехватить ключ сетевого уровня [8] или физически извлечь его из прошивки устройства [9]. Шифрование на уровне приложений также является уязвимым, так как этот ключ тоже может быть скомпрометирован [10].

LoRa

LoRa образует сеть с топологией «звезда из звезд» и охватывает все уровни модели OSI. LoRa обеспечивает конфиденциальность передаваемых данных средствами шифрования AES на нескольких уровнях: на сетевом уровне с использованием уникального ключа сети (Unique Network key, EUI64); сквозную безопасность на уровне приложений с помощью уникального ключа приложения (Unique Application key, EUI64); специального ключа устройства (Device specific key, EUI128). Однако технология LoRa также имеет уязвимости [11].

Z-Wave

Сеть Z-Wave реализует тополгию ячеистой сети. Данный факт в совокупности с использованием гораздо менее нагруженного диапазона 0,8–0,9 ГГц, наличия механизмов самовосстановления (процедура Explorer Frame) и построения оптимальных маршрутов доставки делает Z-Wave одним из самых надежных решений для сенсорной сети. Z-Wave также охватывает все уровни модели OSI. Z-Wave использует собственный стандарт безопасности Security 2 [12], который также поддерживает шифрование AES-128 и использует механизмы подключения новых устройств в сети при помощи PIN-кодов и QR-кодов для того, чтобы злоумышленник не мог осуществить перехват подключения и проникнуть в сеть. Использование протокола Диффи–Хеллмана на эллиптических кривых для обмена ключами также значительно повышает уровень защищенности сети Z-Wave. Однако, как и любая другая технология, она имеет уязвимости [13].

Протоколы прикладного уровня

Наиболее широко распространенными протоколами прикладного уровня, используемыми в киберфизических системах, являются MQTT, CoAP, AMQP, DDS и XMPP (рис. 1). MQTT и CoAP особенно подходят для сервисов, требующих сбора данных (например, обновления датчиков) в условиях систем с ограниченными возможностями. Напротив, AMQP, DDS и XMPP отвечают специфическим требованиям к услугам, а именно: обмен деловыми сообщениями, обмен мгновенными сообщениями и обнаружение присутствия в сети и обмен сообщениями в реальном времени соответственно.

Прикладной уровень	MQTT	CoAP	AMQP	DDS	XMPP
Транспортный уровень	TCP			UDP	
Интернет-уровень	IPv4 и IPv6 + 6LoWPAN				
Уровень сетевых интерфейсов	IEEE 802.3	IEEE 802.11	IEEE 802.15	IEEE 802.16	Другие

Рис. 1. Протоколы прикладного уровня

Что касается служб безопасности, то решения, обеспечивающие целостность и конфиденциальность обмена данными и предоставляющие механизмы аутентификации и авторизации, весьма разнообразны. Протоколы обмена сообщениями обычно поддерживают как стандартные, так и собственные службы безопасности. Исходя из этого, реализация соответствующих решений по обеспечению безопасности возлагается на разработчиков. Ниже приведена табл. 2, в которой отражены возможности рассмотренных ранее протоколов в области шифрования, авторизации и обеспечения конфиденциальности [14].

Таблица 2

Сводка служб безопасности, поддерживаемых протоколами обмена сообщениями

Протокол	Аутентификация		Авторизация	Конфиденциальность	
	SASL	Sp*	Sp*	TLS	DTLS
MQTT		+		+	
CoAP					+
AMQP	+			+	
DDS		+	+	+	
XMPP	+		+	+	

* Sp (special) – специфичная реализация.

Из приведенных данных видно, что механизмы шифрования имеются во всех протоколах обмена сообщениями. Например, конфиденциальность обеспечивается стандартными службами, такими как TLS и DTLS, а механизмы аутентификации и авторизации основаны на стандартных (т.е. SASL) или пользовательских решениях.

Важно отметить отсутствие некоторых механизмов обеспечения безопасности при разработке протокола. Более того, использование служб обеспечения безопасности носит рекомендательный характер, и в целях снижения нагрузки на вычислительные мощности IoT-сетей разработчики склонны пренебрегать этими службами при разработке, настройке и использовании своих приложений. В связи с этим, устройства часто подвергаются рискам безопасности, характерным для рассматриваемых протоколов.

Уязвимости протокола MQTT

На основе анализа возможных угроз безопасности устройств с поддержкой MQTT были определены следующие потенциально уязвимые процессы:

• аутентификация: брокер MQTT не проверяет должным образом личность издателя/подписчика и не блокирует повторные попытки аутентификации. Эти уязвимости могут предоставить злоумышленнику доступ к MQTT-устройствам или, что еще хуже, к брокеру, что может иметь плачевные последствия для функционирования всей сети;

• авторизация: брокер MQTT неправильно устанавливает разрешения на публикацию/подписку. Эта уязвимость может предоставить злоумышленнику контроль над данными или функциями MQTT-устройств;

• доставка сообщений: издатель отправляет сообщения, которые не могут быть доставлены из-за отсутствия подписчиков. Эта уязвимость может привести к значительному снижению производительности брокера;

• проверка сообщений: издатель отправляет сообщения, содержащие запрещенные символы, которые неправильно интерпретируются брокерами и подписчиками. не исключено, что эта уязвимость может быть использована для осуществления различных вредоносных атак;

• шифрование сообщений: клиенты и серверы обмениваются сообщениями в открытом виде, что позволяет злоумышленнику подслушивать и подменять сообщения во время их передачи. Эта уязвимость может быть использована для проведения атак типа «человек посередине» (MITM).

Анализ CVE, затрагивающих продукты и услуги на базе MQTT, показал, что существует около 60 уязвимостей CVE. В частности, поддельные MQTT-сообщения могут легко заставить брокеров не реагировать на запросы. Например, вредоносный MQTT-клиент может вызвать переполнение стека, просто отправив пакет SUBSCRIBE, содержащий не менее 65 400 символов «/» (CVE-2019-11779). Аналогично пакет CONNECT в сочетании с неправильно сформированным пакетом запроса UNSUBSCRIBE может быть использован для атаки типа «отказ в обслуживании» (DoS) на брокера (CVE-2019-6241).

Другие проблемы безопасности относятся к категориям аутентификации и авторизации, как в случае с клиентами, которые устанавливают свое имя пользователя на «#», тем самым обходя механизмы контроля доступа и подписываясь на все темы MQTT (CVE-2017-7650).

Помимо этого, актуальная атака «отказ в обслуживании», направленная на то, чтобы сделать брокер невосприимчивым или даже аварийным, может быть осуществлена путем отправки больших сообщений или сообщений с высоким уровнем QoS. Кроме того, несанкционированная публикация, направленная на физическое повреждение или отключение IoT-устройств, может быть осуществлена с помощью привилегированных сообщений, которые предоставляют злоумышленнику удаленный контроль над этими устройствами. Таким образом, рассмотренные угрозы безопасности могут серьезно повлиять на сеть на базе протокола MQTT и поставить под угрозу доступность и конфиденциальность циркулирующих в ней данных.

В качестве ответных мер угрозам безопасности в стандарте MQTT перечислены механизмы, которые должны быть включены в реализацию MQTT, а именно:

• аутентификация пользователей и устройств;

• авторизация доступа к ресурсам сервера;

• целостность управляющих пакетов MQTT и данных приложения;

• конфиденциальность управляющих пакетов MQTT и данных приложения.

Для каждого из этих механизмов стандарт дает некоторые общие рекомендации (например, повторная аутентификация длительных сессий, предотвращение подписки на все темы, использование VPN). Однако данные контрмеры относятся к простым сценариям, т.е. в отношении более сложных атак эти меры могут быть недостаточными или попросту бесполезными.

Несмотря на то, что использование протокола TLS настоятельно рекомендуется стандартом MQTT для обеспечения безопасной связи, TLS не решает всех проблем безопасности. Как известно, старые версии TLS, его неправильная конфигурация и использование слабых наборов шифров делают протоколы подверженными атакам безопасности. Кроме того, для реализации TLS требуется значительная вычислительная мощность и пропускная способность сети, которые могут быть попросту недоступны в сетях IoT с ограниченными вычислительными возможностями.

Уязвимости протокола CoAP

CoAP поддерживает использование протокола Datagram Transport Layer Security (DTLS), UDP-реализации протокола TLS, который обеспечивает эквивалентные гарантии безопасности. Привязка DTLS для протокола CoAP определена в терминах четырех режимов безопасности, которые отличаются механизмами аутентификации и согласования ключей и варьируются от отсутствия безопасности до безопасности на основе сертификатов. То есть при их использовании стоит задача найти оптимальный компромисс между ограничениями производительности/энергии и требованиями безопасности. Конечно, отсутствие соответствующих служб безопасности может позволить злоумышленнику легко скомпрометировать среды CoAP.

На основе анализа возможных угроз безопасности устройств с поддержкой CoAP были определены следующие потенциально уязвимые процессы:

• разбор сообщений: использование парсеров, т.е. программ (сервисов или скриптов), собирающих данные с определенных источников информации и выдающих в нужном формате, может послужить источником угроз из-за некорректной обработки. Эта уязвимость может повлиять на доступность узла CoAP и даже открыть возможность удаленного выполнения произвольного кода на атакуемом узле;

• проксирование и кэширование: механизмы контроля доступа к прокси и кэшам не реализованы должным образом. Эта уязвимость может скомпрометировать их содержимое, тем самым нарушив конфиденциальность и целостность сообщений CoAP;

• bootstrapping: установка новых узлов CoAP реализована неправильно. Эта уязвимость может предоставить неавторизованным узлам доступ к среде CoAP;

• генерация ключей: генерация криптографических ключей недостаточно надежна. Использование этих ключей может скомпрометировать узлы CoAP;

• подделка IP-адресов: подделывая IP-адреса узлов CoAP, злоумышленник может осуществлять атаки, связанные с генерацией поддельных сообщений и подтверждений, а также повлиять на межпротокольные обмены: сообщение с поддельным IP-адресом и фальшивым номером порта источника, отправленное на CoAP-узел, может заставить его интерпретировать полученное сообщение в соответствии с правилами целевого протокола.

Анализ нескольких CVE, затрагивающих продукты и услуги на базе CoAP, показывает, что наиболее распространенная проблема безопасности связана с неправильным разбором сообщений. Например, некоторые библиотеки CoAP неправильно обрабатывают недопустимые параметры или определенные исключения при получении специально созданных сообщений (например, CVE-2018-12679, CVE-2018-12680). Другие библиотеки подвержены уязвимостям переполнения при обработке входящего сообщения (например, CVE-2019-17212). Эксплуатация этих уязвимостей может иметь различные последствия, такие как утечка памяти, отказ в обслуживании, а также удаленное выполнение кода, что приводит к серьезным последствиям для всей системы, функционирующей на базе протокола CoAP.

Протокол UDP также является вектором, используемым для атаки на узлы с поддержкой CoAP. Например, определенные интерфейсы сервера CoAP могут быть использованы для атаки распределенного отказа в обслуживании с использованием подмены IP-адреса источника и усиления трафика. Эта уязвимость является следствием неправильной обработки определенного сообщения ответа (например, CVE-2019-9750).

Стандарт CoAP предусматривает некоторые общие меры по смягчению последствий, чтобы справиться с типами угроз и атак, рассмотренных в

предыдущем разделе. В частности, стандарт настоятельно рекомендует использовать DTLS для защиты узлов CoAP.

В рамках механизма контроля доступа существует угроза, связанная с возможностями узла по сбору информации, необходимой для внедрения в сеть с поддержкой CoAP в качестве аутентифицированного узла. В данном вопросе был предложен трехэтапный процесс загрузки нового узла. Процесс начинается с фазы обнаружения, на которой обнаруживается новый узел. Затем этому узлу предоставляются ключи для установления безопасного канала связи. Наконец, эти ключи используются для выполнения фактической конфигурации самого узла [15].

Улучшения протокола DTLS также изучались с точки зрения криптографического алгоритма. В частности, интеграция DTLS в CoAP на основе криптографии эллиптических кривых помогает минимизировать вычислительные затраты и использование ПЗУ [16].

Уязвимости протокола AMQP

Что касается безопасности, AMQP поддерживает фреймворк Simple Authentication and Security Layer (SASL) для аутентификации клиента и TLS для обеспечения целостности и конфиденциальности связи. Отметим, что в отличие от MQTT и CoAP, эти службы безопасности обычно включены по умолчанию, что снижает потенциальные риски безопасности. Тем не менее, согласно базе данных NVD, за последние шесть лет в продуктах и сервисах на базе AMQP было обнаружено множество уязвимостей. Эти уязвимости в основном затрагивают центральный компонент сети – брокер. Они влияют на такие процессы, как управление доступом, проверка сообщений и идентификации, управление очередью сообщений.

Последствия этих уязвимостей включают повышение привилегий, раскрытие информации, атаки типа «отказ в обслуживании», обход аутентификации и авторизации, удаленное выполнение кода, перехват трафика. Более конкретно, несколько уязвимостей связаны с отсутствием проверки имен хостов и сертификатов, эксплуатация которых позволяет злоумышленникам подделывать идентификаторы и перехватывать трафик для MiTM-атак (например, CVE-2018-11087, CVE-2018-8119, CVE-2016-4467). Аналогично отсутствие контроля доступа в очередях сообщений позволяет злоумышленникам выполнять привилегированные команды (CVE-2019-3845). Кроме того, несколько CVE указывают на то, что использование специально созданных сообщений AMQP и открытых команд отключения позволяет осуществить атаку типа «отказ в обслуживании» (CVE-2015-7559, CVE-2017-15699, CVE-2015-0224, CVE-2015-1499).

Другие риски безопасности, влияющие на AMQP-среды, связаны с конфигурацией брокеров. Несмотря на наличие веб-интерфейса пользователя, их настройка может быть очень сложной. Неправильный выбор при настройке очередей сообщений, обменов, производителей и потребителей может привести к серьезным уязвимостям. Кроме того, пользовательские интерфейсы могут быть подвержены уязвимостям, обычно встречающимся в вебсфере (например, CVE-2015-0862, CVE-2016-0734, CVE-2017-4965).

Одна из наиболее распространенных ошибок конфигурации связана с применением стандартных учетных данных для входа в систему, которые могут быть использованы злоумышленником для получения контроля над интерфейсом администратора брокера и, следовательно, над всей средой AMQP.

Уязвимости протокола DDS

Что касается безопасности, протокол DDS предлагает богатое разнообразие механизмов. Как и другие протоколы обмена сообщениями, DDS поддерживает TLS и DTLS. Более того, для обеспечения конфиденциальности, целостности и подлинности обменов новейшая спецификация безопасности OMG DDS определяет архитектуру, основанную на наборе встроенных плагинов. Например, плагины предлагают механизмы аутентификации и авторизации DataWriters и DataReaders, что позволяет избежать несанкционированной публикации и подписки. Тем не менее, и спецификация, и плагины подвержены уязвимостям. В частности, протокол рукопожатия, используемый для подтверждения разрешений, передает открытым текстом информацию о возможностях участников, что позволяет злоумышленникам обнаружить потенциально важную информацию о достижимости в сети DDS (CVE-2019-15135).

Продолжая тему уязвимостей предлагаемых плагинов, стоит отметить две уязвимости, обнаруженные для плагина Access Control, способные привести к несанкционированным или непреднамеренным соединениям между участниками (CVE-2019-15136, CVE-2019-15137).

Уязвимости протокола XMPP

Протокол XMPP предоставляет надежные услуги безопасности, поддерживая SASL для процесса аутентификации и TLS для обеспечения конфиденциальности и целостности данных. Эти службы встроены в основные спецификации протокола, поэтому они включены по умолчанию. Тем не менее отсутствие поддержки сквозного шифрования делает протокол уязвимым для различных типов угроз. Например, злоумышленник может изменить, удалить или воспроизвести строфы или получить несанкционированный вход на сервер. В дополнение к проблемам безопасности протокола стоит отметить, что частые проблемы связаны с недостаточным контролем операций с памятью и ненадлежащей проверкой сертификатов (CVE-2019-1845, CVE-2019-12855, CVE-2014-3451, CVE-2018-15720, CVE-2016-1307).

Эти уязвимости позволяют осуществлять широкий спектр атак с различными последствиями, например, сделать сервисы недоступными, получить конфиденциальную информацию или получить доступ к XMPP-серверам.

Несколько методов снижения угроз безопасности были разработаны в качестве расширений XMPP в серии XEP. В частности, в XEP-0205 представлены меры, направленные на предотвращение DoS-атак, а XEP-0178 посвящен правильному использованию сертификатов для аутентификации SASL. Тем не менее несколько XEP содержат уязвимости, связанные с неправильной реализацией самих XEP (например, CVE-2016-10376, CVE-2017-5602, CVE-2019-1000021). Используя эти уязвимости, злоумышленники могут получить доступ к частным данным или выдать себя за пользователя и осуществить атаки социальной инженерии.

Атаки на протоколы прикладного уровня

Частые источники рисков связаны с отсутствием соответствующих служб безопасности или их неправильной конфигурацией. Хотя протоколы обмена сообщениями и предлагают различные службы безопасности, они уязвимы с точки зрения неправильной конфигурации этих служб. Кроме того, отсутствие встроенных механизмов аутентификации / авторизации или использование слабых механизмов делает устройства уязвимыми для несанкционированного доступа. Аналогично неправильная настройка TLS или использование слабых наборов шифров делают устройства уязвимыми к раскрытию данных, циркулирующих в киберфизической системе.

Эти выводы были подтверждены анализом CVE продуктов и услуг, основанных на рассмотренных протоколах. Более точно, многие уязвимости связаны с неправильной проверкой/разбором сообщений (например, переполнение буфера, проверка опций/исключений) и слабыми механизмами аутентификации/авторизации (например, проверка имени пользователя/имени хоста, проверка сертификата).

Важно также отметить, что риски и уязвимости безопасности подвергают устройства широкому спектру угроз и атак, представленных в табл. 3, которые могут иметь очень серьезные последствия.

Таблица 3

Подверженность прикладных протоколов типам атак

Протокол	Атаки типа «IP-спуфинг»	Атаки типа DoS/DDoS	Атаки типа MITM
MQTT		+	+
CoAP	+	+	+
AMQP		+	
DDS		+	
XMPP		+	+

Обеспечение безопасности киберфизических систем

Доступность, надежность и целостность приоритетнее конфиденциальности из-за потенциального воздействия на физический мир. Надежные системы шифрования и аутентификации могут привести к недопустимым задержкам. Необходимо реализовывать меры безопасности не на отдельных устройствах, а на всей инфраструктуре системы.

Традиционные средства защиты, такие как межсетевые экраны, средства антивирусной защиты, средства обнаружения и предотвращения вторжений и др., очень часто неэффективны для защиты IoT-инфраструктуры из-за того, что трафик генерируемый системой специфичен и сложен в анализе и устройства взаимодействуют напрямую друг с другом по беспроводному соединению [17].

При этом киберфизическая система должна быть устойчива к помехам, иметь резервные пути доставки информации, иметь механизмы обнаружения и противодействия действиям злоумышленников: проникновение в сеть, искажение кадров, подмена узлов и т.д.

Устойчивость к помехам реализуется использованием помехозащищенной передачи. Ячеистая топология сети предполагает несколько путей доставки, однако необходимо строить топологию таким образом, при котором существуют резервные пути доставки для каждого узла.

В общем виде система обнаружения вторжений для киберфизических систем осуществляет сбор трафика или его статистики и сравнение собранных данных с эталоном. Любое отклонение от эталона может свидетельствовать об атаке:

• Изменение количества узлов в сети. Это напрямую указывает на наличие нелегитимного узла.

• Изменение уровня мощности сигнала узла. Резкое изменение уровня принимаемого сигнала может свидетельствовать о подмене передающего узла.

• Изменение маршрутов доставки данных. Большинство киберфизических систем имеют ячеистую топологию, а одним из критериев выбора маршрута доставки является качество сигнала. Поэтому изменение маршрута может быть вызвано добавлением нового узла или подменой существующего, а соответственно, и влиянием на качество передачи.

• Увеличение или уменьшение числа кадров, изменение типа трафика. В киберфизических системах узлы генерируют, как правило, однотипный трафик, поэтому изменение количества трафика и его типа, например рост числа служебных пакетов, может указывать на присутствие злоумышленника.

• Ухудшение характеристик производительности сети. Снижение пропускной способности, увеличение задержек также может указывать на присутствие злоумышленника в системе.

• Уменьшение или увеличение времени реакции на запросы. Данный факт может указывать на подмену легитимного узла, например, более производительным устройством, в случае более быстрой реакции на запросы.

• Изменение временных периодов отправки данных. Узлы в киберфизических системах функционируют, как правило, по определенным временным циклам, большинство времени находясь в режиме низкого энергопотребления. Соответственно, и активность в периоды, не свойственные узлу, является аномальной.

Очевидно, что каждый параметр отклонения в отдельности может давать ложный результат, поэтому их следует использовать в совокупности.

Для обеспечения конфиденциальности сообщений и их подлинности необходимо использовать

такие алгоритмы шифрования (например, блочные: CLEFIA, PRESENT [18] и потоковые: MICKEY 2.0, Trivium [19]) и схемы аутентификации (например, μTESLA [20], схема Wenbo [21]), которые будут учитывать требования к задержкам в системе, а также требования к энергоэффективности и низкую производительность конечных устройств.

Разработка таких решений является одним из востребованных направлений исследований на текущий момент.

Защита от исследования

При применении такой схемы построения системы защиты вынуждены постоянно собирать, анализировать трафик и состояние киберфизической системы в целом. Поэтому существует другой подход к повышению защищенности – это технология защиты движущейся цели. Данный подход предполагает, что без собранной информации о системе злоумышленник не может эффективно осуществить свою атаку.

Киберфизические системы, как правило, статичны: данные передаются самыми эффективными маршрутами между конкретными узлами по заданным протоколам. Злоумышленник, в случае проникновения в систему, имеет неограниченные временные ресурсы для сбора информации для планирования своей атаки. Технология защиты движущейся цели предполагает реконфигурирование защищаемой системы через интервалы времени таким образом, при котором злоумышленник не может обладать долгосрочной информацией о системе. Злоумышленник при этом никак не ограничивается в своих действиях.

Авторами предложено новое решение [22, 23], которое основано на принципах технологии движущейся цели и децентрализованных анонимных сетей. Узлы в сенсорной сети передают данные таким образом, при котором защищены шифрованием передаваемые данные и скрыты стороны взаимодействия, т.е. скрыт сам факт передачи информации. Протокол передачи данных не использует явную адресацию, а информационный поток скрыт среди множества идентичных потоков. Передача данных предусмотрена таким образом, чтобы затруднить анализ данных.

Заключение

По причине того, что киберфизические системы функционируют на базе устройств низкой производительности в условиях низкой пропускной способности, такие системы имеют недостаточный уровень защищенности. В силу особенности задач, решаемых системами такого рода, реализуемые меры защиты в них направлены прежде всего на обеспечение высокой доступности и надежности.

Беспроводная связь, ячеистая топология, низкая производительность, высокие требования к энергопотреблению – все это приводит к тому, что традиционные средства защиты невозможно применить в киберфизических системах. Однако использование помехозащищенных технологий передачи, резервирование путей доставки данных, анализ системы на предмет аномалий, использование алгоритмов шифрования из класса «легковесной» криптографии, а также использование схем аутентификаций для слабопроизводительных систем позволяют значительно повысить уровень защищенности киберфизической системы.

Также существует и другой подход к защите – технология защиты движущейся цели. Данная технология не ограничивает в действиях злоумышленника, а лишь не позволяет ему обладать долгосрочной информацией о системе, на основе которой он может эффективно планировать свою атаку.

Исследование выполнено при финансовой поддержке Минцифры РФ (грант ИБ). Проект № 40469-07/2021-К.

Литература

1. Киберфизические системы в современном мире. Блог компании Toshiba [Электронный ресурс]. – Режим доступа: http://habr.com/ru/company/toshibarus/blog/438262, свободный (дата обращения: 15.08.2022).

2. Куприяновский В.П. Киберфизические системы как основа цифровой экономики / В.П. Куприяновский, Д.Е. Намиот, С.А. Синягов // International Journal of Open Information Technologies. – 2016. – Т. 4, № 2. – С. 18–25.

3. Чеклецов В.В. Чувство планеты. Интернет вещей и следующая технологическая революция. – М.: Изд-во Российского исследовательского центра по интернету вещей, 2013. – 130 с.

4. Русанов П.И. Особенности работы беспроводных сенсорных сетей / П.И. Русанов, А.Г. Юрочкин // Вестник Воронежского института высоких технологий. – 2019. – № 4 (31). – С. 79–81.

5. Десницкий В.А. Анализ защищенности программно-аппаратных компонентов в беспроводных сенсорных сетях / В.А. Десницкий, А.В. Мелешко // Информационные технологии и телекоммуникации. – 2019. – Т. 7, № 1. – С. 75–83.

6. Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey / A. Barua, A. Al Alamin, S. Hossain, E. Hossain // IEEE Open Journal of the Communications Society. – 2022. – Vol. 3. – P. 251–281.

7. Security analysis of ZigBee / X. Fan, F. Susan, W. Long, S. Li // MWR InfoSecurity. – 2017. – P. 1–18.

8. ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys / P. Radmand, M. Domingo, J. Singh, J. Arnedo, A. Talevski, S. Petersen, S. Carlsen // 2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. – 2010. – P. 465–470.

9. Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned / O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, P. Toivanen // 2014 14th International Conference on Hybrid Intelligent Systems. – 2014. – P. 199–206.

10. Ďurech J. Security attacks to ZigBee technology and their practical realization / J. Ďurech, M. Franeková // 2014 IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI). – 2014. – P. 345–349.

11. Chacko S. Security mechanisms and Vulnerabilities in LPWAN / S. Chacko, M.D. Job // IOP conference series: materials science and engineering. – IOP Publishing, 2018. – Vol. 396, No. 1. – P. 012027.

12. Lilli M. Formal Proof of a Vulnerability in Z-Wave IoT Protocol / M. Lilli, C. Braghin, E. Riccobene // SECRYPT. – 2021. – P. 198–209.

13. Crushing the Wave--new Z-Wave vulnerabilities exposed / N. Boucif, F. Golchert, A. Siemer, P. Felke, F. Gosewehr // arXiv preprint arXiv:2001.08497. – 2020.

14. Nebbione G. Security of IoT application layer protocols: Challenges and findings / G. Nebbione, M.C. Calzarossa // Future Internet. – 2020. – Vol. 12, No. 3. – P. 55–75.

15. Secure bootstrapping of nodes in a CoAP network / O. Bergmann, S. Gerdes, S. Schafer, F. Junge, C. Bormann // 2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). – 2012. – P. 220–225.

16. Security-aware CoAP application layer protocol for the internet of things using elliptic-curve cryptography / F. Albalas, M. Al-Soud, O. Almomani, A. Almomani // Power (mw). – 2018. – Vol. 1333. – P. 550–558.

17. NTT Security - GTIR 2017 [Электронный ресурс]. – Режим доступа: https://www.nttsecurity.com/en-us/gtir-2017, свободный (дата обращения: 15.08.2022).

18. Jangra M. Performance analysis of CLEFIA and PRESENT lightweight block ciphers / M. Jangra, B. Singh // Journal of Discrete Mathematical Sciences and Cryptography. – 2019. – Vol. 22, No. 8. – P. 1489–1499.

19. Ertaul L. IoT security: Performance evaluation of grain, mickey, and trivium-lightweight stream ciphers / L. Ertaul, A. Woodall // Proceedings of the International Conference on Security and Management (SAM). – 2017. – P. 32–38.

20. Efficient and enhanced broadcast authentication protocols based on multilevel μTESLA / X. Li, N. Ruan, F. Wu, J. Li, M. Li // 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC). – 2014. – P. 1–8.

21. A secure user authentication protocol for sensor network in data capturing / Z. Quan, T. Chunming, Z. Xianghan, R. Chunming // Journal of Cloud Computing. – 2015. – Vol. 4, No. 1. – P. 1–12.

22. Кушко Е.А. Метод реализации защищенного обмена данными на основе динамической топологии сети // Вестник СибГУТИ. – 2020. – № 4. – С. 39–52.

23. Kushko E.A. Concealment of sensor network node interaction / E.A. Kushko, N.Y. Parotkin // IOP Conference Series: Materials Science and Engineering. – 2021. – Vol. 1155, No. 1. – P. 012058.

Кушко Евгений Александрович
Аспирант каф. безопасности информационных технологий (БИТ) Сибирского государственного ун-та науки и технологий (СибГУ) им. акад. М.Ф. Решетнёва
Имени газеты «Красноярский рабочий» пр-т, д. 31,
г. Красноярск, Россия, 660037
Тел.: +7 (391-2) 22-76-39
Эл. почта: evgeny.kushko@gmail.com

Грачёв Дмитрий Александрович
Студент каф. БИТ СибГУ им. акад. М.Ф. Решетнёва
Имени газеты «Красноярский рабочий» пр-т, 31,
г. Красноярск, Россия, 660037
Тел.: +7 (391-2) 22-76-39
Эл. почта: ostromir28@gmail.com

Паротькин Николай Юрьевич
Канд. техн. наук, доцент каф. БИТ СибГУ им. акад. М.Ф. Решетнёва
Имени газеты «Красноярский рабочий» пр-т, 31,
г. Красноярск, Россия, 660037
Тел.: +7 (391-2) 22-76-39
Эл. почта: nyparotkin@yandex.ru

Золотарёв Вячеслав Владимирович
Канд. техн. наук, доцент, зав. каф. БИТ СибГУ им. акад. М.Ф. Решетнёва
Имени газеты «Красноярский рабочий» пр-т, 31,
г. Красноярск, Россия, 660037
Тел.: +7 (391-2) 22-76-39
Эл. почта: amida.2@yandex.ru

Kushko E.A., Grachyov D.A., Parotkin N.Y., Zolotaryov V.V.

Security issues of cyber-physical systems

Cyber-physical systems are increasingly being used in all industries. However, as the distribution of these systems grows, the number of attacks on them increases. The paper covers main cyber-physical systems building technologies, implemented security measures, advantages, disadvantages and vulnerabilities of such systems. The authors also provide a general approach to ensuring cyber-physical systems security.

Keywords: cyber-physical systems, sensor networks, internet of things, vulnerability.
DOI: 10.21293/1818-0442-2022-25-4-101-109

References

1. *Kiber-fizicheskie sistemy v sovremennom mire. Blog kompanii Toshiba* [Cyber-physical systems in the modern world. Toshiba Blog]. Available at: http://habr.com/ru/company/toshibarus/blog/438262, free (Accessed: August 15, 2022) (in Russ.).

2. Kupriyanovsky V.P., Namiot D.E., Sinyagov S.A. [Cyber-physical systems as a base for digital economy]. *International Journal of Open Information Technologies*, 2016, vol. 4, no. 2, pp. 18–25 (in Russ.).

3. Cheklecov V.V. *Chuvstvo planety. Internet veshchej i sleduyushchaya tekhnologicheskaya revolyuciya* [Feeling the planet. Internet of Things and the next technological revolution]. Moscow: Russian Research Center Internet of Things Publ., 2013. 130 p. (in Russ.).

4. Rusanov P.I. Yurochin A.G. [Wireless features touch networks]. *Bulletin of Voronezh Institute of High Technologies*, 2019, no. 4 (31), pp. 79–81 (in Russ.).

5. Desnitsky V.A., Meleshko A.V. [Security analysis of software and hardware components in wireless sensor networks]. *Telecom IT*, 2019, vol. 7, no. 1, pp. 75–83 (in Russ.).

6. Barua A., Al Alamin A., Hossain S., Hossain E. Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey. *IEEE Open Journal of the Communications Society*, 2022, vol. 3, pp. 251–281.

7. Fan X., Susan F., Long W., Li S. Security analysis of ZigBee. *MWR InfoSecurity*, 2017, pp. 1–18.

8. Radmand P., Domingo M., Singh J., Arnedo J., Talevski A., Petersen S., Carlsen S. ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys. *Proceedings of 2010 International Conference on P2P*, Parallel, Grid, Cloud and Internet Computing. IEEE Publ., 2010, pp. 465–470.

9. Olawumi O., Haataja K., Asikainen M., Vidgren N., Toivanen P. Three practical attacks against ZigBee security:

Attack scenario definitions, practical experiments, countermeasures, and lessons learned. *Proceedings of 14th International Conference on Hybrid Intelligent Systems*. IEEE Publ., 2014, pp. 199–206.

10. Ďurech J., Franeková M. Security attacks to ZigBee technology and their practical realization. *Proceedings of 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*. IEEE, 2014, pp. 345–349.

11. Chacko S., Job M.D. Security mechanisms and Vulnerabilities in LPWAN. *IOP Conference Series: Materials Science and Engineering*, 2018, vol. 396, no. 1, p. 012027.

12. Lilli M., Braghin C., Riccobene E. Formal Proof of a Vulnerability in Z-Wave IoT Protocol. *SECRYPT*, 2021, pp. 198–209.

13. Boucif N., Golchert F., Siemer A., Felke P., Gosewehr F. Crushing the Wave--new Z-Wave vulnerabilities exposed. *arXiv preprint arXiv:2001.08497*, 2020. Available at: https://arxiv.org/abs/2001.08497 (Accessed: August 15, 2022).

14. Nebbione G., Calzarossa M.C. Security of IoT application layer protocols: Challenges and findings. *Future Internet*, 2020, vol. 12, no. 3, pp. 55–75.

15. Bergmann O., Gerdes S., Schafer S., Junge F., Bormann C. Secure bootstrapping of nodes in a CoAP network. *Proceedings of Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE Publ., 2012, pp. 220–225.

16. Albalas F., Al-Soud M., Almomani O., Almomani A. Security-aware CoAP application layer protocol for the internet of things using elliptic-curve cryptography. *Power (mw)*, 2018, vol. 1333, pp. 550–558.

17. NTT Security - GTIR 2017. Available at: https://nttsecurity.com/en-us/gtir-2017, free (Accessed: August 15, 2022).

18. Jangra M., Singh B. Performance analysis of CLEFIA and PRESENT lightweight block ciphers. *Journal of Discrete Mathematical Sciences and Cryptography*, 2019, vol. 22, no. 8, pp. 1489–1499.

19. Ertaul L., Woodall A. IoT security: Performance evaluation of grain, mickey, and trivium-lightweight stream ciphers. *Proceeding of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science Computer Engineering and Applied Computing WorldComp Publ., 2017, pp. 32–38.

20. Li X., Ruan N., Wu F., Li J., Li M. Efficient and enhanced broadcast authentication protocols based on multilevel μTESLA. *Proceedings of 33rd International Performance Computing and Communications Conference (IPCCC)*. IEEE Publ., 2014, pp. 1–8.

21. Quan Z., Chunming T., Xianghan Z., Chunming R. A secure user authentication protocol for sensor network in data capturing. *Journal of Cloud Computing*, 2015, vol. 4, no. 1, pp. 1–12.

22. Kushko E.A. [Secure data communication implementing method based on dynamic network topology]. *Herald of the Siberian State University of Telecommunications and Informatics*, 2020, no. 4, pp. 39–52 (in Russ.).

23. Kushko E.A., Parotkin N.Y. Concealment of sensor network node interaction. *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1155, no. 1, p. 012058.

Evgenij A. Kushko
Postgraduate student, Department of Information Technologies Security, Reshetnev Siberian State University of Science and Technology (SibSU)
31, Imeni gazety «Krasnoyarskiy rabochiy» pr., Krasnoyarsk, Russia, 660037
Phone: +7 (391-2) 22-76-39
Email: evgeny.kushko@gmail.com

Dmitrij A. Grachyov
Student, Department of Information Technologies Security, SibSU
31, Imeni gazety «Krasnoyarskiy rabochiy» pr., Krasnoyarsk, Russia, 660037
Phone: +7 (391-2) 22-76-39
Email: ostromir28@gmail.com

Nikolaj Y. Parotkin
Candidate of Science in Engineering, Assistant Professor, Department of Information Technologies Security, SibSU
31, Imeni gazety «Krasnoyarskiy rabochiy» pr., Krasnoyarsk, Russia, 660037
Phone: +7 (391-2) 22-76-39
Email: nyparotkin@yandex.ru

Vyacheslav V. Zolotaryov
Candidate of Science in Engineering, Head of Department of Information Technologies Security, SibSU
31, Imeni gazety «Krasnoyarskiy rabochiy» pr., Krasnoyarsk, Russia, 660037
Phone: +7 (391-2) 22-76-39
Email: amida.2@yandex.ru

УДК 621.317/619

М.А. Назаров, Э.В. Семенов

Анализ нелинейно-инерционных свойств устройств оцифровки с использованием их модели в виде нелинейного рекурсивного фильтра

Рассмотрен метод анализа нелинейно-инерционных свойств устройств регистрации (аналого-цифрового преобразования) сигналов. Метод включает построение модели устройства оцифровки в виде нелинейного рекурсивного фильтра ограниченного порядка (второго-третьего). Две-четыре нелинейные функции в такой модели предлагается рассматривать как характеристики нелинейности устройства. Указано на влияние этих характеристик на разные части переходной характеристики устройства. Для выбранного примера (цифрового осциллографа) показано, что нелинейность собственно квантующего узла осциллографа имеет бессистемный характер, но мала на фоне относительно гладких искажений в аналоговом тракте осциллографа.

Ключевые слова: нелинейный фильтр, сверхширокополосный импульсный сигнал, нелинейные искажения, поведенческая модель, безынерционная нелинейность, реактивная нелинейность.
DOI: 10.21293/1818-0442-2022-25-4-110-114

Устройства оцифровки сигналов являются одним из ключевых компонентов многих радиосистем. В ряде случаев важными являются нелинейные искажения в таких устройствах (для систем связи со сложными сигналами или для систем диагностики и зондирования с анализом нелинейного отклика объектов [1, 2]). Например, при обнаружении нелинейных объектов в задачах сверхкороткоимпульсной сверхширокополосной нелинейной локации [3] необходимо учитывать нелинейные искажения сигналов приемником (устройством оцифровки). Характеризации нелинейно-инерционных свойств систем для произвольных воздействий посвящен ряд работ, например [4–6], однако до сих пор ни одно из решений не воспринято инженерами для практического использования [7].

В работе [8] предложен метод анализа нелинейных искажений произвольных сигналов устройством с разделением этих искажений на составляющие за счет применения простой поведенческой нелинейной модели системы. Показано, что каждая из вневременных характеристических функций этой модели определяет нелинейные искажения в отдельных частях переходного процесса системы. Мы полагаем, что далее семейство характеристических функций модели [8] можно использовать непосредственно для исчерпывающей характеризации нелинейных искажений различных устройств.

В настоящей статье демонстрируется возможность использования семейства характеристик нелинейного рекурсивного фильтра, используемого в качестве поведенческой модели устройства, для исчерпывающей характеризации нелинейности устройства оцифровки (аналого-цифрового преобразования) сигнала.

Пример анализируемого устройства оцифровки

На практике в различных задачах широко используются устройства оцифровки с полосой 100…150 МГц, разрядностью 8 бит и чувствительностью около 10 мВ. В качестве примера выберем типичное устройство со схожими параметрами: осциллограф National Instruments PXI-5114 [9]. По заявлениям производителя данное регистрирующее устройство имеет полосу пропускания 125 МГц, длительность фронта переходной характеристики не более 2,8 нс, коэффициент нелинейных искажений −58 дБ (0,13%).

Построение параметризованной модели устройства

Нелинейная модель устройства показана на рис. 1. Модель представляет собой нелинейный рекурсивный фильтр второго порядка. Расчет выходного напряжения по заданному входному току определяется выражениями (2)–(7) в [7].

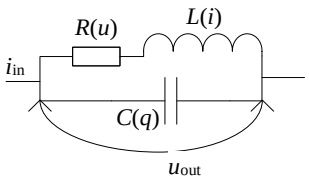


Рис. 1. Нелинейная модель регистрирующего устройства National Instruments PXI-5114

В данной модели нелинейная ампер-вольтовая характеристика $u(i)$ соответствует амплитудной характеристике устройства и оказывает влияние после окончания переходного процесса (на плоской вершине переходной характеристики). Нелинейная кулон-вольтовая характеристика $u(q)$ определяет крутизну фронта переходной характеристики устройства и оказывает влияние в начале переходного процесса, а нелинейная вебер-амперная характеристика $i(\psi)$ влияет на величину и форму выброса перерегулирования переходной характеристики.

Определим нелинейные функции $u(i)$, $u(q)$, $i(\psi)$ данной цепи для семейства переходных характеристик моделируемого устройства. Семейство переходных характеристик было измерено (рис. 2) при подаче сигнала с генератора PicoSourse PG 911 [10] с

длительностью фронта не более 60 пс, что значительно меньше времени нарастания напряжения канала регистрирующего устройства (около 2,8 нс).

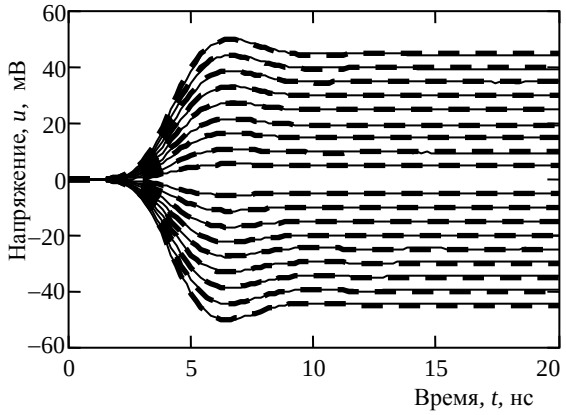


Рис. 2. Семейство переходных характеристик NI PXI-5114: измеренные (сплошные кривые), рассчитанные по нелинейной модели (пунктирные кривые)

Для определения искажений на плоской вершине переходной характеристики (безынерционные искажения) измерим ампер-вольтовую характеристику $u(i)$ канала регистрирующего устройства. Поскольку коэффициент нелинейных искажений канала регистрирующего устройства мал и составляет около 0,13% [9], то для измерения амплитудной характеристики необходимо использовать цифроаналоговый преобразователь (ЦАП) с нелинейностью, на порядок меньшей нелинейности канала регистрирующего устройства. В качестве ЦАП был выбран чип Asahi Kasei AK4490. Нелинейность ЦАП с буферными усилителями составляет не более 0,0015% [11], что на два порядка меньше нелинейности канала регистрирующего устройства. ЦАП выдавал ступенчатый сигнал с длительностью ступеньки 62,5 мкс, что значительно больше времени переходных процессов для генератора и в канале регистрирующего устройства. Ступеньки генерировались для 20 значений напряжений в диапазоне напряжений от −50 до +50 мВ (для диапазона 0,1 В канала регистрирующего устройства National Instruments PXI-5114), а значение точки стробирования выбиралось в момент времени 60 мкс от начала каждой ступеньки.

Результат измерения $u(i)$ представлен на рис. 3. Ожидаемая нелинейность моделируемого устройства мала, поэтому нелинейность функций $u(i)$, $u(q)$, $i(\psi)$ будет неразличима глазом. Для целей графического отображения на рисунках усилим нелинейность характеристических функций (в K раз) согласно выражению

$$y^*(x) = y_0(x) + K[y(x) - y_0(x)], \qquad (1)$$

где $y(x)$ – одна из функций $u(i)$, $u(q)$, $i(\psi)$; $y_0(x)$ – линеаризация соответствующей характеристической функции; $y^*(x)$ – функция с усиленной нелинейностью. Для всех характеристик примем $K = 15$.

Из рис. 3 видно, что нелинейность ампер-вольтовой характеристики (статическая нелинейность) незначительна даже с усиленной на графике нелинейностью (далее будет показано, что нелинейность функций $u(q)$, $i(\psi)$ в несколько раз превышает нелинейность функции $u(i)$). Поэтому далее функцию $u(i)$ будем считать линейной. Линейность функции $u(i)$ означает, что резистор в рекурсивном фильтре (см. рис. 1) также линеен.

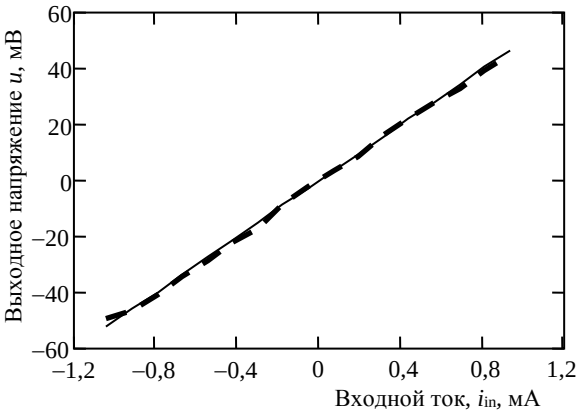


Рис. 3. Линеаризованная ампер-вольтовая характеристика канала NI PXI-5114 (сплошная кривая) и измеренная кривая с усиленной нелинейностью (пунктирная кривая)

Нелинейно-инерционные искажения определяются экстрагированными функциями $u(q)$ и $i(\psi)$. Определим данные функции из семейства измеренных переходных характеристик (см. рис. 2).

Из рис. 2 видно, что фронт переходной характеристики в начальный момент времени имеет экспоненциальный характер. Для уменьшения невязки измеренного и смоделированного сигналов будем подавать на вход модели единичный скачок, сглаженный фильтром Гаусса с постоянной времени 1,2 нс.

Определение характеристик $u(q)$ и $i(\psi)$ проводится в соответствии с рекурсивным алгоритмом, изложенным в [7]. Переходная характеристика с минимальной амплитудой (около 5 мВ) считается малосигнальной. Линейная емкость и индуктивность $C_0 = q/u$ и $L_0 = \psi/i$ для этой кривой определяются вариационным методом для достижения наилучшего соответствия измеренной и смоделированной переходных характеристик. Для следующей переходной характеристики C_1 и L_1 определяются также погрешностью ее моделирования, но в таблице значений C и L остаются также и предыдущие значения, определяющие нелинейность кривых $u(q)$ и $i(\psi)$. Интерполяция между значениями в таблицах выполняется кубическим сплайном.

Экстрагированные функции $u(q)$ и $i(\psi)$ показаны на рис. 4 и 5 (с усилением нелинейности в 15 раз по выражению (1)).

Сопротивление этого резистора равно входному сопротивлению регистрирующего устройства (50 Ом), поскольку он определяет преобразование входного напряжения устройства во входной ток модели.

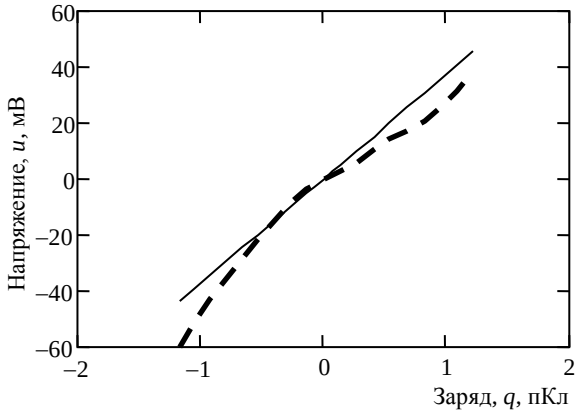


Рис. 4. Линеаризованная кулон-вольтовая характеристика канала NI PXI-5114 (сплошная кривая) и измеренная кривая с усиленной нелинейностью (пунктирная кривая)

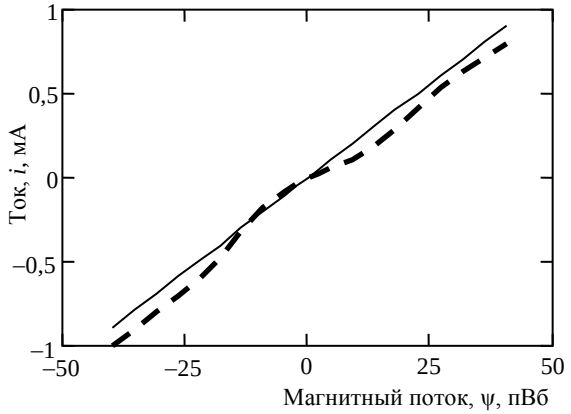


Рис. 5. Линеаризованная вебер-амперная характеристика канала NI PXI-5114 (сплошная кривая) и измеренная кривая с усиленной нелинейностью (пунктирная кривая)

Оценка качества моделирования нелинейных искажений сигналов

Особую важность для нелинейно-инерционных моделей имеет качество отображения ими нелинейных искажений сигналов. В качестве метода оценки нелинейных искажений будем использовать метод сравнения реального отклика объекта на тестовый сигнал и отклика линеаризованной модели объекта на этот же сигнал [12–16]. Характеристика нелинейности по данному методу для измеренных переходных характеристик определяется выражением в [12]

$$\varepsilon(t) = u_{\text{out}}(t) - F^{-1}\left(\frac{F\left[u_{\text{out }0}(t)\right]}{F\left[i_{\text{in }0}(t)\right]}\right) * i_{\text{in}}(t)\,, \qquad (2)$$

где F^{-1} и F – обратное и прямое преобразование Фурье соответственно; $i_{\text{in }0}(t)$ и $u_{\text{out }0}(t)$ – тестовый сигнал (ток) малой амплитуды и отклик объекта малой амплитуды (напряжение) на него соответственно (0,1 мА и 5 мВ в нашем случае); $*$ – символ свертки; $\varepsilon(t)$ – характеристика нелинейности при тестовом токе $i_{\text{in}}(t)$ и отклике напряжения $u_{\text{out}}(t)$ на этот ток.

Вычислим характеристику нелинейности для каждой измеренной переходной характеристики, используя выражение (2). На рис. 6, *а* приведено семейство характеристик нелинейности, нормированных к верхнему пределу измерения регистрирующего устройства (50 мВ). На рис. 6, *б* приведены характеристики нелинейности, вычисленные аналогичным образом по смоделированным переходным характеристикам.

Из сопоставления рис. 6, *а* и *б* видно, что характеристики нелинейности по результатам измерения и моделирования имеют одинаковые минимальные и максимальные величины (в пределах −2…1%), а отображающие их поверхности близки по форме. Таким образом, можно утверждать, что полученная модель адекватно отражает нелинейные искажения регистрирующего устройства National Instruments PXI-5114.

Анализ характеристик нелинейности устройства оцифровки

Анализ кривых на рис. 3–5 показывает следующее. Статическая нелинейность устройства носит бессистемный характер и мала (0,34%) относительно искажений внутри переходного процесса. Если устройство оцифровки используется для регистрации импульсных сигналов, то этой нелинейностью можно пренебречь без заметного ухудшения качества характеризации общей нелинейности.

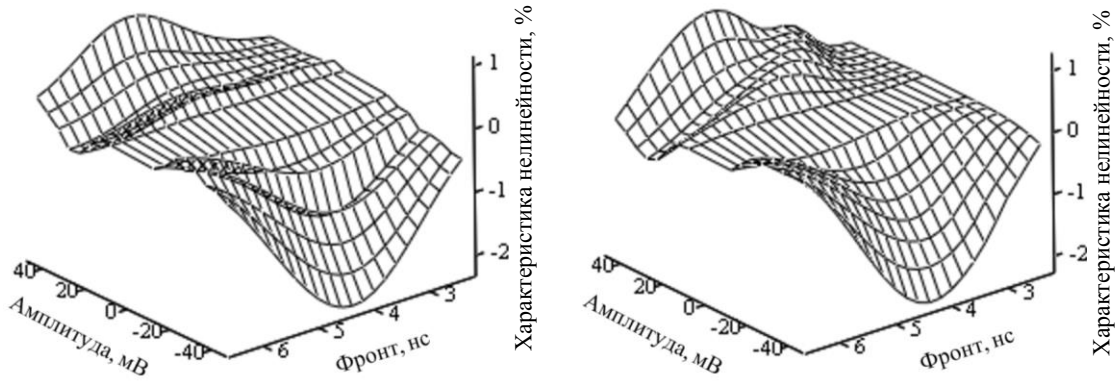


Рис. 6. Поверхности распределения характеристики нелинейности ε для фронта (в %) в зависимости от амплитуды переходной характеристики (−50...50 мВ) на фронте (2,3...6,5 нс) по модели – *а*, по измеренным переходным характеристикам – *б*

Наибольший вклад (до 2,2%) в общую нелинейность вносят нелинейности емкостей входного буфера (усилителя) устройства оцифровки (кулон-вольтовая характеристика на рис. 4). Эта нелинейность относительно гладкая (не связана с матрицей аналого-цифрового преобразователя) и имеет четные составляющие нелинейности (несимметричная схема буфера).

Нелинейность обратных связей (вебер-амперная характеристика на рис. 5) имеет уровень до 0,8% и сказывается в окрестности выброса на переходной характеристике устройства.

Заключение

В работе проанализированы нелинейно-инерционные свойства типичного устройства регистрации сигналов с полосой 125 МГц. Для этого синтезирована его модель в виде нелинейного рекурсивного фильтра. Исходя из измеренной переходной характеристики (единственный выброс на плоской вершине без провала), оказалось достаточно модели второго порядка.

Три вневременные характеристики полученной модели исчерпывающим образом характеризуют нелинейно-инерционные свойства устройства: ампер-вольтовая характеристика отражает нелинейность на плоской вершине, кулон-вольтовая – на фронте сигнала, а вебер-амперная – нелинейность выброса на плоской вершине.

Установлено, что указанная производителем нелинейность может быть ассоциирована только со статической нелинейностью устройства (нелинейность матрицы АЦП, десятые доли процента). Нелинейность на фронтах сигналов оказывается на порядок больше и обусловлена искажениями в аналоговом входном буфере.

Работа выполнена при финансовой поддержке Российского научного фонда, проект № 22-29-00605.

Литература

1. Байкалова А.Е. Увеличение динамического диапазона приемной системы нелинейного видеоимпульсного локатора / А.Е. Байкалова, Э.В. Семенов // Прикладные аспекты СВЧ-техники: матер. 32-й Междунар. конф. «СВЧ-техника и телекоммуникационные технологии». – Севастополь: СевГУ, 2022. – Вып. 4. – С. 241 – 242.

2. Семенов Э.В. Программно-аппаратный комплекс для исследования нелинейности преобразования видеоимпульсных сигналов сверхширокополосными приемниками / Э.В. Семенов, Н.Д. Малютин, А.Г. Лощилов // Обмен опытом в области создания сверхширокополосных РЭС: матер. II науч.-техн. конф. «Центральное конструкторское бюро автоматики». – Омск, 2008. – С. 174–177.

3. Авдеев В.Б. Сверхкороткоимпульсная сверхширокополосная нелинейная радиолокация / В.Б. Авдеев, А.В. Бердышев, С.Н. Панычев // Телекоммуникации. – 2006. – № 8. – С. 23–27.

4. Лабутин С.А. Оценивание и коррекция динамических искажений сигналов на основе нелинейных моделей средств измерений // Измерительная техника. Метрология. – 1986. – № 12. – С. 22–29.

5. Ланнэ А.А. Синтез нелинейных систем. Нерекурсивные системы, детерминированный случай // Электронное моделирование. – 1980. – № 1. – С. 60–68.

6. Лабутин С.А. Коррекция нелинейно-инерционных искажений импульсных сигналов в измерительных преобразователях // Техника средств связи. Сер.: Радиоизмерительная техника. – 1989. – Вып. 1. – С. 9–15.

7. Semyonov E.V. Simple Behavioral Model of Baseband Pulse Devices in the Form of a Second-Order Nonlinear Recursive Filter // IEEE Transactions on circuits and systems-ii: express briefs. – 2021. – Vol. 68, No. 6. – P. 2192–2196.

8. Семенов Э.В. Анализ состава нелинейных искажений при видеоимпульсных воздействиях с применением поведенческих нелинейных моделей электрических цепей // Изв. вузов России. Радиоэлектроника. – 2022. – Т. 25, № 2. – С. 29–39.

9. PXI-5114 Specification [Электронный ресурс]. – Режим доступа: https://www.ni.com/docs/en-US/bundle/pxi-5114-specs/page/specs.html#, свободный (дата обращения: 01.11.2022).

10. PicoSource® PG900 Series [Электронный ресурс]. – Режим доступа: https://www.picotech.com/download/datasheets/picosource-pg900-series-data-sheet.pdf, свободный (дата обращения: 01.11.2022).

11. TEAC NT-503 Owner's manual. [Электронный ресурс]. – Режим доступа: https://teac.jp/downloads/products/teac/NT-503/NT-503_OM_EFS_vE.pdf, свободный (дата обращения: 01.11.2022).

12. Semyonov E.V. Using the difference between convolutions of test signals and responses of the object to study the nonlinearity of the conversion of ultra-wideband signals / E.V. Semyonov, A.V. Semyonov // Radio engineering and electronics. – 2007. – Vol. 52, No. 4. – P. 480–485 (in Russ.).

13. Semyonov E. Measurements of the nonlinearity of the ultra wideband signals transformation / E. Semyonov, A. Loschilov // Ultra Wideband Communications: Novel Trends – System, Architecture and Implementation. – Rijeka, Croatia: InTech, 2011. – P. 3–16. DOI: 10.5772/16867.

14. Иванов И.Ф. О едином методе измерения нелинейности импульсных устройств / И.Ф. Иванов, В.С. Трофимов // Радиотехника. – 1963. – Т. 18, № 2. – С. 52–60.

15. The IM microscope: a new approach to nonlinear analysis of signals in satellite communications system / D.S. Arnstein, X.T. Vuong, C.B. Cotner , H.M. Daryanani // COMSAT Technical Review. – 1992. – Vol. 22, No 1. – P. 93–123 [Электронный ресурс]. – Режим доступа: https://www.artelllc.com/wp-content/uploads/T3-3-White Paper-XTV-Spring-1992-IM-Microscope.pdf, свободный (дата обращения: 09.11.2022).

16. Calculating passive intermodulation products with IM Microscope method / W. Haining, L. Jiangang, W. Jiqin, Z Chenxin // J. of Air Force Engineering University: Natural Science Edition. – 2005. – Vol. 6, No 3. – P. 47–49 [Электронный ресурс]. – Режим доступа: http://kjgcdx.ijournal.cn/ch/reader/create_pdf.aspx?file_no=20050314, свободный (дата обращения: 09.11.2022).

Назаров Максим Андреевич
М.н.с. каф. радиоэлектроники и систем связи (РСС)
Томского государственного университета
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: (382-2) 41-33-65
Эл. почта: mnaz90@mail.ru

Семенов Эдуард Валерьевич
Д-р техн. наук, профессор каф. РСС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0001-5470-1185
Тел.: (382-2) 41-33-65
Эл. почта: edwardsemyonov@narod.ru

Nazarov M.A., Semyonov E.V.

Simple behavioral model of a recording device using a second-order non-linear recursive filter

A method to analyze the non-linear-inertial properties of devices for recording (analog-to-digital conversion) of signals is considered. The method includes a building of a model of a digitizing device in the form of a nonlinear recursive filter of a limited order (second or third). Two or four non-linear functions in such a model are proposed to be considered as characteristics of the non-linearity of the device. The influence of these characteristics on different parts of the transient response of the device is indicated. For the selected example (digital oscilloscope), it is shown that the nonlinearity of the oscilloscope quantizing unit itself has an unsystematic character, but is small against the background of relatively smooth distortions in the analog path of the oscilloscope.

Keywords: non-linear filter, ultra-wideband pulse signal, nonlinear distortions, behavioral model, inertial non-linearity, reactive non-linearity.
DOI: 10.21293/1818-0442-2022-25-4-110-114

References

1. Baikalova E.V. Semyonov E.V. Uvelichenie dinamicheskogo diapazona priemnoj sistemy nelinejnogo videoimpul'snogo lokatora [Increasing the dynamic range of the receiving system of a nonlinear video pulse locator]. Prikladnye aspekty SVCH-tekhniki. Materialy 32 Mezhdunarodnoj konferencii «SVCH tekhnika i telekommunikacionnye tekhnologii» [Applied Aspects of Microwave Engineering: Proceedings of the 32nd International Conference]. Sevastopol, SevGU Publ., 2022, vol. 4, pp. 241–242 (in Russ.).

2. Semyonov E.V., Malyutin N.D., Loschilov A.G. *Programmno-apparatnyj kompleks dlya issledovaniya nelinejnosti preobrazovaniya videoimpul'snyh signalov sverhshirokopolosnymi priemnikami* [Hardware-software complex for studying the nonlinearity of video-pulse signal conversion by ultra-wideband receivers]. Obmen opytom v oblasti sozdaniya sverhshirokopolosnyh RES. Materialy II nauch.-tekhn. konferencii [Exchange of experience in the field of creation of ultra-wideband radio-electronic means. Proceedings of the II science and engineering conferences]. Omsk, 2008, pp. 174–177 (in Russ.).

3. Avdeev V.B. [Ultra-short-pulse ultra-wideband nonlinear radar] / V.B. Avdeev, A.V. Berdyshev, S.N. Panychev. *Telecommunications*, 2006, no. 8, pp. 23–27 (in Russ.).

4. Labutin S.A. [Estimation and correction of dynamic signal distortions based on nonlinear models of measuring instruments]. *Measuring technology. Metrology*, 1986, no. 12, pp. 22–29 (in Russ.).

5. Lanne A.A. [Synthesis of nonlinear systems. Nonrecursive systems, deterministic case]. *Electronic Modeling*, 1980, no. 1, pp. 60–68 (in Russ.).

6. Labutin S.A.. [Correction of non-linear-inertial distortions of pulse signals in measuring transducers]. *Communication Technology. Series Radio Measuring |Equipment*, 1989, vol. 1, pp. 9–15 (in Russ.).

7. Semyonov E.V. Simple Behavioral Model of Baseband Pulse Devices in the Form of a Second-Order Nonlinear Recursive Filter. *IEEE Transactions on Circuits and Systems-II: Express Brief*s, 2021, vol. 68, no. 6, pp. 2192–2196.

8. Semyonov E.V. [Analysis of the Composition of Nonlinear Distortions under Video Impulse Effects Using Behavioral Nonlinear Models of Electrical Circuits]. *Izvestia Universities of Russia. Radioelectronics*, 2022, no. 1, pp. 29–39 (in Russ.).

9. PXI-5114 Specification. Available at: https://www.ni.com/docs/en-US/bundle/pxi-5114-specs/page/specs.html# (Accessed: November 01, 2022).

10. PicoSource® PG900 Series. Available at: https://www.picotech.com/download/datasheets/picosource-pg900-series-data-sheet.pdf (Accessed: November 01, 2022).

11. TEAC NT-503 Owner's manual. Available at: https://teac.jp/downloads/products/teac/NT-503/NT-503_OM_EFS_vE.pdf (Accessed: November 01, 2022).

12. Semyonov E.V. Using the difference between convolutions of test signals and responses of the object to study the nonlinearity of the conversion of ultra-wideband signals / E.V. Semyonov, A.V. Semyonov // *Radio Engineering and Electronics*, 2007, vol. 52, no. 4, pp. 480–485 (in Russ.).

13. Semyonov E., Loschilov A. Measurements of the nonlinearity of the ultra wideband signals transformation / E. Semyonov, A. Loschilov // *Ultra Wideband Communications: Novel Trends – System, Architecture and Implementation. Rijeka, Croatia: InTech*, 2011, pp. 3–16. doi: 10.5772/16867.

14. Ivanov I.F., Trofimov V.S. On a Unified Method for Measuring the Nonlinearity of Pulsed Devices. *Radiotekhnika* [Radio engineering], 1963, vol. 18, no. 2, pp. 52–60. (in Russ.).

15. The IM microscope: a new approach to nonlinear analysis of signals in satellite communications systems / D.S. Arnstein, X.T. Vuong, C.B. Cotner, H.M. Daryanani // *COMSAT Technical Review*, 1992, vol. 22, no 1, pp. 93–123. Available at: https://www.artelllc.com/wp-content/uploads/T3-3-WhitePaper-XTV-Spring-1992-IM-Microscope.pdf (Accessed: November 09, 2022).

16. Calculating passive intermodulation products with IM Microscope method / W. Haining, L. Jiangang, W. Jiqin, Z. Chenxin // J. of Air Force Engineering University: Natural Science Edition, 2005, vol. 6, no. 3, pp. 47–49. Available at: http://kjgcdx.ijournal.cn/ch/reader/create_pdf.aspx?file_no=20050314 (Accessed: November 09, 2022).

Maxim A. Nazarov
Junior researcher,
Department of Radioelectronics and Communication Systems,
Tomsk State University of Control Systems and Radioelectronics
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 41-33-65
Email: mnaz90@mail.ru

Edward V. Semyonov
Doctor of Science in Engineering, Professor,
Department of Radioelectronics and Communication Systems,
Tomsk State University of Control Systems and Radioelectronics
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0001-5470-1185
Phone: +7 (382-2) 41-33-65
Email: edwardsemyonov@narod.ru

УДК 65.011.56

Э.И. Гаврильев, Т.В. Авдеенко

Многофакторная регрессионная модель оценки квалификации тестировщика программного обеспечения

Компетентность тестировщиков и их профессиональное развитие являются важными аспектами успеха ИТ-проекта. Руководство компаний периодически проводит оценку квалификации сотрудников для выявления потенциальных направлений карьерного роста. Однако такая оценка зачастую основывается на субъективном мнении руководителей, что может негативно сказаться на дальнейшем профессиональном развитии работника. Целью данной работы является разработка регрессионной модели для оценки квалификации тестировщиков программного обеспечения (ПО). Предлагаемая модель использует данные из информационных систем, которыми пользуются тестировщики в своей ежедневной работе. Для сбора информации и проведения расчетов разработана система поддержки принятия решений (СППР), которая была внедрена в компании, занимающейся разработкой ПО для банковской отрасли. Построение регрессионной модели позволило выявить основные факторы, оказывающие влияние на профессиональные знания и навыки тестировщика.

Ключевые слова: тестирование ПО, повышение квалификации, оценка персонала, профессиональное развитие, многомерный регрессионный анализ, система управления задачами, система управления тестированием, управление знаниями.

DOI: 10.21293/1818-0442-2022-25-4-115-121

Результаты ИТ-проекта во многом зависят от уровня квалификации ИТ-специалистов, так как выполняемые задачи требуют наличия у сотрудников продвинутых профессиональных, коммуникативных и управленческих навыков. ИТ-организациям выгоднее развивать профессиональную компетентность сотрудников, чем проводить поиск и найм специалистов на рынке труда, потому что ввод нового сотрудника в компанию требует большего количества временных и материальных ресурсов. Наличие условий для профессионального роста также может уменьшить уровень текучести кадров и повысить степень мотивированности сотрудников [1].

В связи с вышесказанным особую актуальность на ИТ-предприятиях приобретает система профессионального развития сотрудников. Важным элементом этой системы является подсистема оценки квалификации работников, на которой основано большое количество управленческих решений в области работы с персоналом: управление развитием карьеры, кадровые перестановки и мотивация труда [2]. Однако при оценке сотрудника в настоящее время чаще всего используется субъективное мнение руководителей, что может привести к некорректным результатам оценки и негативно повлиять на его дальнейшее профессиональное развитие.

В настоящей работе была поставлена цель: уменьшить субъективность при оценке квалификации тестировщика за счет использования объективных показателей его работы совместно с субъективной оценкой руководителя. Для достижения поставленной цели была построена регрессионная модель, использующая данные из систем, в которых тестировщики работают ежедневно: система управления задачами, система управления знаниями и система управления тестированием. Начальный набор предикторов включал в себя показатели из систем управления знаниями и задачами из предыдущей работы, в рамках которой была построена регрессионная модель оценки профессиональных навыков и знаний разработчиков [3]. Дополнительно было проведено сравнение предикторов построенных моделей для выявления сходств и различий при оценке квалификации ИТ-специалистов.

Обзор литературы

Подходы к оценке квалификации тестировщиков ПО рассматривались в литературе довольно фрагментарно в отличие от подходов к оценке квалификации разработчиков ПО. Имеющиеся публикации исследуют только навыки и знания, необходимые тестировщикам для трудоустройства, в то время как согласно поставленной цели исследования интерес для нас представляют методы и способы оценки квалификации тестировщиков [4].

В работе [5] исследования сосредоточены на поиске характеристик «эффективных» тестировщиков на основе результатов интервью с менеджерами продуктов и самими тестировщиками из трех ИТ-компаний. В результате были выделены 4 группы характеристик:

1. Опыт: наличие опыта работы с различными информационными системами, базовых знаний о предметной области и программировании, а также навыки составления понятных отчетов о дефектах в работе системы.

2. Самоанализ: понимание «полной картины» проекта, приоритета дефекта программного продукта.

3. Мотивы: осознание важности тестирования, (нравится находить ошибки в функционале информационной системы).

4. Личные характеристики: тщательность, терпение, самостоятельность и добросовестность.

Также в [5] было выявлено, что знания о предметной области и специфические технические навыки являются более важными, чем навыки, связанные с тестированием, например планирование тестирования и написание тест-кейсов.

Другое исследование [6] посвящено поиску и анализу наиболее важных характеристик «хороших» тестировщиков. Авторы провели ряд интервью со специалистами в области тестирования ПО из нескольких крупных ИТ-компаний и выявили 4 группы навыков и знаний:

1. Навыки, связанные с тестированием: планирование тестирования, написание тест-кейсов, знание и опыт применения разных методов тестирования, управление процессом тестирования.

2. Технические навыки: программирование, администрирование операционных систем, управление жизненным циклом ИС и фреймворки разработки, специфические инструменты для тестирования и диагностики.

3. Коммуникативные и управленческие навыки.

4. Знания о предметной области.

Из этих 4 групп наиболее важными характеристиками «хорошего» тестировщика являются: коммуникативные навыки, наличие образования в области ИТ, умение выполнять разнообразные задачи, внимательность, аккуратность, любознательность и желание обеспечить соответствующий уровень качества разрабатываемой информационной системы.

Также в литературе предлагаются другие подходы для повышения качества разрабатываемых ИС в ИТ-компаниях. Например, в работах предлагается эффективный метод интеллектуального управления разработкой в команде при применении гибкого подхода на основе онтологической модели (ontology-based approach) к управлению знаниями [7, 8].

Для определения списка необходимых навыков, которыми должны обладать тестировщики, исследователи провели анализ 400 вакансий на должность тестировщика из 33 стран [9]. В результате анализа вакансий было выявлено, что тестировщики должны обладать навыками, связанными с планированием и управлением тестирования, разработкой тест-кейсов и автотестов. Также работодателей интересуют такие технические навыки, как программирование и работа с реляционными базами данных.

Хотя вышеприведенные исследования выделяют ряд навыков и знаний, необходимых тестировщику на этапе найма на работу, однако отсутствуют убедительные свидетельства, что эти характеристики можно использовать при оценке квалификации сотрудника после его трудоустройства. В рассмотренных работах также не изучены методы, которые можно применить для оценки навыков и знаний тестировщика. Метод, основанный на субъективном мнении непосредственного руководителя, может предоставить некорректные результаты ввиду следующих факторов: наличие особенностей во взаимоотношениях между руководителем и подчиненным; высокая требовательность руководителя; эффект края, при котором учитывается только последняя неделя работы, и т.д.

Необходимо отметить, что в отдельных исследованиях для оценки результатов деятельности ИТ-специалистов используются данные из репозиториев проектов, над которыми они работали. Так, в исследовании [10] авторы рассматривали вклад разработчика в Open Source Software в виде коммитов исходного кода, написанных страниц документации и составленных отчетов о дефектах. В другой работе было установлено, что разработчик с большим уровнем вклада в проект, вероятно, будет иметь более высокий уровень «качества» [11]. Основное внимание уделялось выявлению корреляции между «качеством» разработчиков и их вкладом в проект, измеряемым с помощью таких показателей, как количество коммитов и отсутствие дефектов в коде.

Таким образом, метод оценки сотрудника, основанный на использовании данных из систем, в которых он работает, отличается более высоким уровнем объективности, чем мнение непосредственного руководителя работника, так как в основе этого метода лежат количественно измеряемые показатели и данные, соответствующие действительности. В настоящей работе мы используем такой подход для оценки технических знаний и умений тестировщика ПО.

Метод исследования

В своей ежедневной работе тестировщики в ИТ-индустрии используют систему управления тестированием, систему управления задачами и систему управления знаниями [12].

Система управления задачами используется для организации работы проектной команды [13]. В этой системе каждая задача представляет собой задание, которое необходимо выполнить в рамках разработки или сопровождения ИС, например, исправление дефекта, разработка экранной формы и т.д. Примерами такого рода систем являются Atlassian Jira, Redmine, Trello.

Система управления знаниями применяется для организации процессов создания, хранения и передачи знаний [14]. Например, в этой системе фиксируется документация для разработчиков, которая необходима при поддержке системы: API-документация, данные для авторизации, функциональные требования и т.д. Чаще всего в компаниях используют Atlassian Confluence, Notion и Microsoft Sharepoint.

Система управления тестированием используется для управления планами тестирования, составления и хранения тест-кейсов, а также формирования отчетов о результатах проведения тестирования [15]. Примерами таких систем являются TestLink, TestRail и PractiTest.

На основе литературного обзора и предыдущих работ для оценки квалификации разработчика были выделены первичные показатели для оценки квалификации тестировщика. Информация из системы управления задачами используется для расчета следующих показателей, связанных с тестированием и сроками решения задач:

– среднее количество решенных задач в день;

– среднее количество переоткрытий решенных дефектов в день;

– среднее время решения задачи в минутах;

– количество созданных задач с типом «Ошибка» с приоритетами «Blocker», «Critical», «Major», «Minor»;

– среднее время проверки задачи в минутах;

– среднее количество успешно проверенных задач в день;

– состав проектной команды сотрудника, в которой он работает: количество разработчиков, менеджеров проекта и т.д.

Данные из системы управления знаниями используются для расчета следующих показателей активности сотрудника:

– количество созданных страниц;

– количество обновлений содержимого страниц;

– среднее количество отметок «Нравится» на страницах, созданных сотрудником.

Данные из системы управления тестированием используются для расчета следующих показателей разработки тест-кейсов:

– количество созданных тест-кейсов;

– среднее количество шагов в тест-кейсах;

– количество выполненных тестов в статусах «Пройден», «Заблокирован», «Провален» и «Не запускался».

В рамках одной из предыдущих работ для проведения расчетов был разработан прототип системы поддержки принятия решений (СППР) на основе программной платформы Node.js [16]. На данный момент прототип СППР был декомпозирован на 2 подсистемы: подсистемы загрузки данных из внешних систем и подсистемы оценки сотрудника.

На рис. 1 представлена структурно-функциональная модель подсистемы загрузки данных. Подсистема проводит миграцию информации из списка указанных внешних систем в конце календарного дня.

На рис. 2 представлена структурно-функциональная модель оценки квалификации сотрудника. Подсистема проводит последовательную четырехшаговую процедуру оценки: выбор сотрудника, загрузка дополнительной информации о работнике, расчет показателей и формирование отчета. В настоящее время вместо запуска импорта данных из внешних систем на втором шаге выполняется запрос из базы данных прототипа СППР.

Доработанная система используется в компании среднего размера, которая выступает вендором ПО в банковской отрасли. Основным инструментом разработки её программных продуктов является собственный low-code конструктор приложений [3]. В компании в качестве системы управления задачами используется Atlassian Jira, в качестве системы управления знаниями выступает Atlassian Confluence, а TestLink применяют в качестве системы управления тестированием.

Сама оценка ИТ-специалистов проводится непосредственными руководителями по 3 факторам на основе 8-балльной шкалы, где 1 – минимальное значение, а 8 – максимальное [3]:

– профессиональные знания и навыки;

– ответственность;

– навыки взаимодействия.

На начальном этапе был проведен ряд интервью с ведущими специалистами контроля качества и менеджерами проектных команд, чтобы узнать, каким образом они проводят оценку квалификации тестировщиков. В результате были добавлены следующие показатели для оценки квалификации:

– показатели оценки качества отчета о дефекте: наличие обязательных составных частей отчета (описание фактического и ожидаемого результата работы системы, шаги для воспроизведения дефекта), наличие нескольких кейсов по воспроизведению ошибки в одном дефекте, показатели читаемости отчета: автоматический индекс удобочитаемости, индекс Колман–Лиау, индекс Флеша [17];

– показатели, связанные с результатом решения зарегистрированного дефекта в системе управления задачами (резолюцией): процент задач, решенных с резолюцией «Решено», «Не могу воспроизвести», «Дубликат», «Не может быть решен»;

– показатели оценки производительности тестирования: среднее количество заведенных отчетов об ошибках; среднее время обнаружения ошибки в минутах; среднее время тестирования задачи в минутах; среднее количество проверенных задач в день;

– показатели частоты использования инструментов для тестирования и обновления программных продуктов компании: количество вложений с запросами и ответами интеграционных веб-сервисов в отчетах о дефектах; количество вложений с журналами сервера и консоли; количество задач на обновление программной платформы тестируемого продукта; количество выполненных задач, содержащих упоминание инструментов для тестирования (Soap UI, JMeter, Postman);

– показатели, относящиеся к менторству новых сотрудников: количество обученных стажеров; количество подключений к менторству; количество успешно закрытых стажировок и количество неуспешно закрытых стажировок.

В итоге для оценки профессиональных знаний и навыков тестировщика было выделено 50 показателей. Для изучения влияния выделенных показателей на уровень квалификации работника был проведен многомерный регрессионный анализ, в котором зависимой переменной выступала оценка профессиональных навыков и знаний сотрудника от непосредственного руководителя, а предикторами выступали эти показатели.

Выборка включает в себя результаты 39 оценок квалификации 28 тестировщиков в период 2017–2021 гг. Для каждой оценки был определен интервал дат, за который необходимо провести выгрузку данных из систем и расчет показателей. В итоге была загружена информация по 148 414 задачам, 3 513 страницам из системы управления знаниями и 75 576 тест-кейсам из системы управления тестированием.

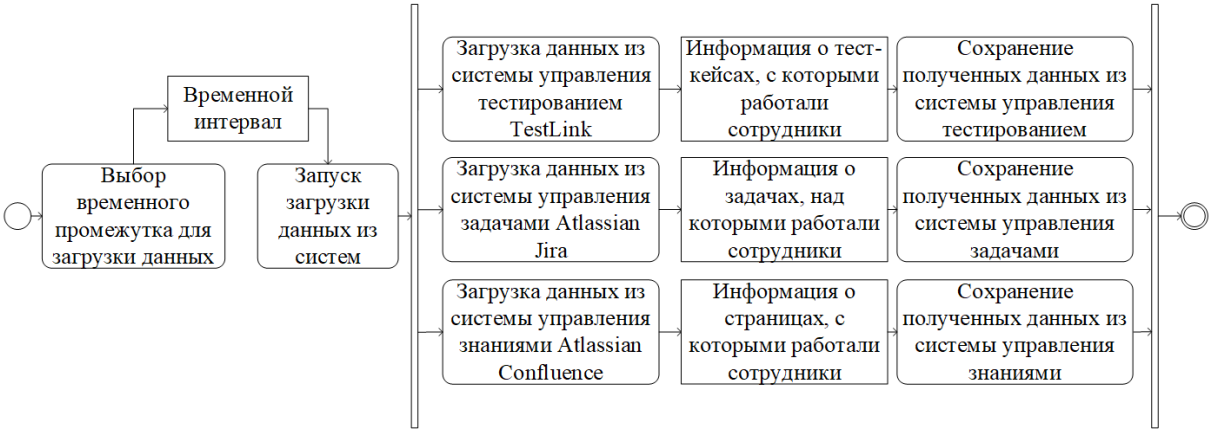


Рис. 1. Структурно-функциональная модель подсистемы загрузки данных

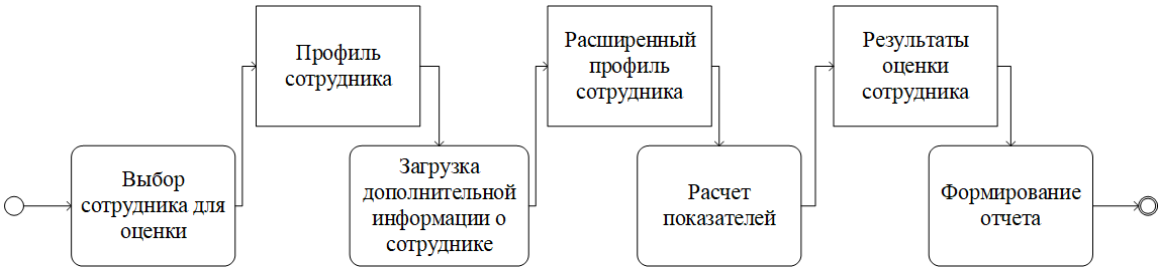


Рис. 2. Структурно-функциональная модель подсистемы оценки сотрудника

Результаты исследования

Основной целью проведения регрессионного анализа является построение линейной модели вида (1):

$$y = \beta_0 + \beta_1 x_1 + ... + \beta_k x_k + \varepsilon, \quad (1)$$

где y – зависимая переменная модели, т.е. оценка профессиональных навыков и знаний тестировщика; x_i – объясняющие переменные (предикторы), представляющие собой результаты деятельности тестировщиков; β_i – неизвестные параметры модели, подлежащие оцениванию на основе собранных данных; ε – случайная неизвестная ошибка, удовлетворяющая необходимым требованиям.

Линейная модель была построена в *R* с помощью пакета lm. После этого была проанализирована независимость переменных модели. Для обнаружения мультиколлинеарности был рассчитан коэффициент инфляции дисперсии (VIF). Предикторы со значением VIF больше 3 удалялись из модели.

Для анализа построенной модели использовались *F*-критерий Фишера и *t*-критерий Стьюдента. Первоначальные версии модели имели p-значение больше 0,05, что указывает на избыточность предикторов, и поэтому итеративно исключались незначимые показатели.

Итоговый вариант модели зависимости профессиональных знаний и навыков тестировщиков от показателей имеет p-значение 0,0007121 и $F_{8,29} = 4{,}846$, что также указывает на ее статистическую значимость (таблица). Коэффициент детерминации R2 равен 0,4552. Предикторами этой модели являются:

– среднее значение индекса Колман–Лиау у отчетов о дефектах, зарегистрированных сотрудником (CLMN_LIAU);

– среднее количество зарегистрированных дефектов в день (B_BY_DT);

– количество приложенных сотрудником вложений, связанных с интеграционными веб-сервисами (INT_ATT);

– среднее значение индекса Флеша у отчетов о дефектах, зарегистрированных сотрудником (FLSCH);

– среднее время решения задачи в минутах (ISS_RS_TM);

– количество приложенных сотрудником вложений, относящихся к журналированию работы системы (LOG_FS);

– количество зарегистрированных дефектов с несколькими кейсами воспроизведения ошибок (MLT_CS).

– количество стажеров, успешно прошедших стажировку под менторством сотрудника (TR).

Результаты функции LM для модели профессиональных навыков и знаний тестировщика

Coefficients	Estimate	Std. Error	*t* value	Pr (>|*t*|)
(Intercept)	3,593335	0,417691	8,603	1,78e-09
CLMN_LIAU	0,038604	0,017370	2,222	0,03421
B_BY_DT	-0,283585	0,119879	–2,366	0,02490
INT_ATT	0,005296	0,002066	2,563	0,01583
FLSCH	-0,013566	0,007843	–1,730	0,09430
ISS_RS_TM	-0,002190	0,001569	–1,396	0,17340
LOG_FS	0,024608	0,013642	1,804	0,08165
MLT_CS	0,018453	0,005672	3,254	0,00289
TR	0,476377	0,135983	3,503	0,00151

Функциональный вид модели представлен формулой (2):

$$prof = 3{,}593 + 0{,}039 * CLMN\_LIAU -$$

$$- 0{,}284 * \text{B\_BY\_DT} + 0{,}005 * \text{INT\_ATT} - $$
$$- 0{,}014 * \text{FLSCH} - 0{,}002 * \text{ISS\_RS\_TM} +$$
$$+ 0{,}025 * \text{LOG\_FS} + 0{,}018 * \text{MLT\_CS} + 0{,}476 * \text{TR}. \quad (2)$$

На профессиональные знания и навыки тестировщика положительно влияют количество стажеров, успешно прошедших стажировку; количество вложений, относящихся к интеграциям и журналированию работы системы, негативно влияют индексы удобочитаемости, среднее количество зарегистрированных дефектов в день и среднее время решения задачи.

Анализ результатов и выводы

По результатам можно отметить, что при оценке квалификации тестировщика непосредственные руководители опираются на среднее время решения задач (ISS_RS_TM), как и при оценке квалификации разработчика. Этот показатель тесно связан с бюджетом и сроком проекта: чем дольше решается задача, тем выше становится уровень операционных расходов и риск срыва установленных сроков.

Положительно на оценку влияют количество прикрепленных к дефектам вложений, связанных с журналированием работы системы (LOG_FS) и интеграционными веб-сервисами (INT_ATT). При помощи этих собранных файлов разработчик может оперативнее определить первопричину ошибки и способ её дальнейшего решения. Получить эти вложения тестировщик может при наличии знаний и опыта работы со специфическими инструментами тестирования. Например, для сбора файлов, связанных с журналированием, сотрудник должен уметь работать с консолью веб-браузера и операционной системы, а для вложений, относящихся к интеграционным веб-сервисам, работник должен уметь проводить тестирование при помощи специального программного обеспечения: Soap UI, Postman и JMeter. Эти программные продукты позволяют провести более комплексное и тщательное тестирование веб-сервисов.

В области ИТ менторство является одним из важных механизмов обучения и развития новых сотрудников [18]. Тестировщики, выступающие в роли ментора, систематизируют и валидируют собственные знания и опыт, накопленные в процессе работы. Также в ходе обучения новые сотрудники задают вопросы, которые позволяют менторам по-другому взглянуть на свои профессиональные навыки и знания. Кроме того, стажеры могут привнести в компанию современные инструменты и технологии, способные повысить уровень качества разрабатываемого программного продукта. В связи с этим на уровень профессиональных навыков положительно влияет количество стажеров, успешно прошедших стажировку (TR).

Однако показатели удобочитаемости и сложности составленных отчетов о дефектах (CLMN_LIAU, FLSCH) обратно пропорциональны оценке уровня профессиональных навыков. Возможно, это связано с уровнем комплексности проверяемого функционала информационной системы, описание дефектов которого требует применения сложных синтаксических конструкций.

В ИТ-индустрии не рекомендуется в отчетах о дефектах указывать несколько кейсов для воспроизведения ошибки [19]. Однако результаты указывают на то, что наличие нескольких кейсов в одном дефекте положительно влияет на оценку профессиональных знаний тестировщика (MLT_CS). Возможно, в рамках исследуемой компании сотрудникам требуется несколько способов для воспроизведения дефекта, чтобы исправить все возможные его проявления в рамках одной задачи.

Негативно на уровень профессиональных навыков влияет среднее количество зарегистрированных дефектов в день (B_BY_DT). Возможно, это связано с уровнем важности влияния ошибки на общую функциональность системы, так как на поиск и обнаружение дефектов с высоким уровнем влияния может уйти больше времени, в то время как дефекты с более низким уровнем влияния, например дефекты графического интерфейса, легче обнаружить и зафиксировать в системе управления задачами.

Оказалось, что показатели из системы управления тестированием оказались избыточными, так как в исследуемой компании небольшая часть сотрудников работает в этой системе. Основная часть работников фиксирует составленные тест-кейсы при помощи других инструментов, например Microsoft Excel и Google-таблицы, а результаты их исполнения регистрируются в системе управления задачами.

Показатели частоты фиксаций информации в системе управления знаниями оказались неактуальными при оценке профессиональных знаний и навыков тестировщиков, так как в исследуемой компании они чаще выступают в роли потребителей информации, в то время как разработчики более активно создают и обновляют страницы в системе.

Заключение

В рамках данной работы была построена регрессионная модель для оценки профессиональных знаний и навыков тестировщиков. Было выявлено, что при оценке менеджеры учитывают среднее количество зарегистрированных дефектов в день и показатели качества отчетов о дефектах: удобочитаемость текста, вложения и несколько кейсов для воспроизведения ошибки. Также на уровень профессиональных знаний и навыков положительно влияет количество трудоустроенных стажеров, которых обучил сотрудник.

При оценке квалификации тестировщиков и разработчиков менеджеры ориентируются на среднее время решения задачи, так как этот показатель тесно связан с бюджетом и сроком проекта, а также он отражает производительность сотрудника. Однако показатели из системы управления знаниями оказались избыточными, так как в исследуемой компании тестировщики в меньшей степени фиксируют знания.

При помощи разработанных модели и системы поддержки принятия решения менеджеры могут проводить оценку квалификации тестировщика. В

дальнейшем планируется подготовить методику для составления индивидуального плана развития ИТ-специалиста в области разработки ПО на основе полученных результатов оценки.

Литература

1. Соловьёв Д.П. Обучение и развитие персонала: учеб. пособие / Д.П. Соловьев, Л.А. Илюхина. – Самара: Изд-во Самар. гос. экон. ун-та, 2019. – 204 с.

2. Носырева И.Г. Анализ эффективности системы оценки персонала / И.Г. Носырева, Н.В. Балашова // Экономика труда. – 2019. – № 1 (6). – С. 440–452.

3. Gavriliev E.I. Model and Procedure for Assessing the Qualification of a Software Developer / E.I. Gavriliev, T.V. Avdeenko // 2022 IEEE 23rd International Conference of Young Professionals in Electron Devices and Materials (EDM). – 2022. – P. 303–307.

4. Juristo N. Guest editors' introduction: Software testing practices in industry / N. Juristo, A.M. Moreno, W. Stigel // IEEE Software. – 2006. – № 4 (23). – P. 19–21.

5. Iivonen J. Characteristics of high performing testers: a case study / J. Iivonen, M.V. Mäntylä, J. Itkonen // ESEM '10: Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement. – 2019. – P. 1–9.

6. Deak A. What Characterizes a Good Software Tester? – A Survey in Four Norwegian Companies // Lecture Notes in Computer Science. – 2014. – № 8763. – P. 162–172.

7. Murtazina M.S. An ontology-based approach to the agile requirements engineering / M.S. Murtazina, T.V. Avdeenko // Perspectives of System Informatics. PSI 2019. Lecture Notes in Computer Science. – 2019. – № 11964. – P. 205–213.

8. Avdeenko T.V. Intelligent support of requirements management in agile environment / T.V. Avdeenko, M.S. Murtazina // Studies in Computational Intelligence: Service orientation in holonic and multi-agent manufacturing. – 2019. – № 803. – P. 97–108.

9. Florea R. The skills that employers look for in software testers / R. Florea, V. Stray // Software Quality Journal. – 2019. – № 27. – P. 1449–1479.

10. Gousios G. Measuring developer contribution from software repository data / G. Gousios, E. Kalliamvakou, D. Spinellis // In Proceedings of the 2008 international working conference on Mining software repositories, MSR '08. – 2008. – P. 129–132.

11. An Empirical Study of Developer Quality / Y. Qiu, W. Zhang, W. Zou, J. Liu, Q. Liu // Software Quality Reliability and Security-Companion (QRS-C) 2015 IEEE International Conference on Software Quality, Reliability and Security. – 2015. – P. 202–209.

12. A Collaboration Tools for Global Software Engineering / F. Lanubile, C. Ebert, R. Prikladnicki, K. Herzig // IEEE Software. – 2010. – № 2 (27) – P. 52–55.

13. Макашов П.А. Сервис-ориентированный подход к управлению ИТ-проектами на примере использования программного продукта «JIRA» / П.А. Макашов, Н.А. Романенко // Современные информационные технологии и ИТ-образование. – 2015. – № 2 (11). – С. 127–132.

14. Apraci I. The impact of knowledge management practices on the acceptance of Massive Open Online Courses (MOOCs) by engineering students: A cross-cultural comparison / I. Apraci, M. Al-Emran, M.A. Al-Sharafi // Telematics and Informatics. – 2020. – № 54. – P. 1–13.

15. Collins E.F. Software Test Automation practices in agile development environment: An industry experience report / E.F. Collins, V.Jr. Lucena // 2012 7th International Workshop on Automation of Software Test (AST). – 2012. – P. 57–65.

16. Гаврильев Э.И. Процедура оценки квалификации разработчика программного обеспечения / Э.И. Гаврильев, Т.В. Авдеенко // Наука. Технологии. Инновации: сб. науч. трудов: в 10 ч. – Новосибирск: Изд-во НГТУ, 2021. – С. 145–148.

17. Иксанов Р.А. Проблема синтаксической сложности текстов нормативно-правовых актов в сфере экономической деятельности / Р.А. Иксанов, А.И. Муратова // Вестник БИСТ (Башкирского института социальных технологий). – 2021. – № 1 (50). – С. 81–85.

18. A Case Study of Onboarding in Software Teams: Tasks and Strategies / A. Ju, H. Sajnani, S. Kelly, K. Herzig // Proceedings of the 43rd International Conference on Software Engineering. – 2021. – P. 613–623.

19. Schuegerl P. Enriching SE ontologies with bug report quality / P. Schuegerl, J. Rilling, P. Charland // Proc. 4th International Workshop on Semantic Web Enabled Software Engineering. – 2008. – P. 1–17.

Гаврильев Эрчимэн Иванович
Аспирант каф. теоретической и прикладной информатики (ТПИ) Новосибирского государственного технического университета (НГТУ)
Карла Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0001-7289-3969
Тел.: +7-923-246-05-82
Эл. почта: erchimen_gavriliev@outlook.com

Авдеенко Татьяна Владимировна
Д-р техн. наук, проф. каф. ТПИ НГТУ
Карла Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0002-8614-5934
Тел.: +7-913-951-60-06
Эл. почта: tavdeenko@mail.ru

Gavriliev E.I., Avdeenko T.V.

Multivariate regression model to assess the qualifications of a software tester

The competence of testers and their professional development are important aspects of IT-project's success. Companies' management evaluates periodically the employees' qualifications in order to identify potential areas for career growth. However, the assessment is frequently based on managers' subjective opinions and may negatively affect employees' further professional development. The purpose of this work is to develop a regression model for assessing the qualifications of software testers. The proposed model uses data from information systems that testers use in their daily work. To collect information and carry out calculations, a decision support system was developed, that was implemented in a company developing software for the banking industry. Building a regression model made it possible to identify the main factors influencing the professional knowledge and skills of a tester.

Keywords: software testing, personnel assessment, professional development, multivariate regression analysis, task management system, testing management system, knowledge management.
DOI: 10.21293/1818-0442-2022-25-4-115-121

References

1. Solovyov D.P., Ilyukhina L.A. *Obuchenie i razvitie personala* [Personnel training and development] study guide, Samara, Samara St. Econ. Univ. Publ., 2019. 204 p. (in Russ.)

2. Nosireva I.G., Balashova N.V. [Analysis of the effectiveness of the personnel assessment system]. *Ekonomika truda*, 2019, vol. 6, no. 6, pp. 440–452 (in Russ.).

3. Gavriliev E.I., Avdeenko T.V. Model and Procedure for Assessing the Qualification of a Software Developer. *2022 IEEE 23rd International Conference of Young Professionals in Electron Devices and Materials (EDM)*, 2022, pp. 303–307.

4. Juristo N., Moreno A.M., Stigel W. Guest editors' introduction: Software testing practices in industry. *IEEE Software*, 2006, vol. 23, no. 4, pp. 19–21.

5. Iivonen J., Mäntylä M.V., Itkonen J. Characteristics of high performing testers: a case study. *ESEM '10: Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*, 2019, pp. 1–9.

6. Deak A. What Characterizes a Good Software Tester? A Survey in Four Norwegian Companies. *Lecture Notes in Computer Science*, 2014, no. 8763, pp. 162–172.

7. Murtazina M.S., Avdeenko T.V. An ontology-based approach to the agile requirements engineering. *Perspectives of System Informatics. PSI 2019. Lecture Notes in Computer Science*, 2019, no. 11964, pp. 205–213.

8. Avdeenko T.V., Murtazina M.S. Intelligent support of requirements management in agile environment. *Studies in Computational Intelligence: Service orientation in holonic and multi-agent manufacturing*, 2019, no. 803, pp. 97–108.

9. Florea R., Stray V. The skills that employers look for in software testers. *Software Quality Journal*, 2019, no. 27, pp. 1449–1479.

10. Gousios G., Kalliamvakou E., Spinellis D. Measuring developer contribution from software repository data. *Proceedings of the 2008 International Working Conference on Mining Software Repositories, MSR '08*, 2008, pp. 129–132.

11. Qiu Y., Zhang W., Zou W., Liu J., Liu Q. An Empirical Study of Developer Quality. *Software Quality Reliability and Security-Companion (QRS-C) 2015 IEEE International Conference on Software Quality, Reliability and Security*, 2015, pp. 202–209.

12. Lanubile F., Ebert C., Prikladnicki R., Vizcaíno A. Collaboration Tools for Global Software Engineering. *IEEE Software*, 2010, vol. 27, no. 2, pp. 52–55.

13. Makashov P.A., Romanenko N.A. [Service-oriented approach to IT project management on the example of using JIRA software product]. *Modern Information Technology and IT-Education*, 2015, vol. 11, no. 2, pp. 127–132.

14. Apraci I., Al-Emran M., Al-Sharafi M.A. The impact of knowledge management practices on the acceptance of Massive Open Online Courses (MOOCs) by engineering students: A cross-cultural comparison. *Telematics and Informatics*, 2020, no. 54, pp. 1–13.

15. Collins E. F., Lucena Jr. V. Software Test Automation practices in agile development environment: An industry experience report. *2012 7th International Workshop on Automation of Software Test (AST)*, 2012, pp. 57–65.

16. Gavriliev E.I., Adveenko T.V. [Procedure for assessing the qualifications of a software developer]. *Science. Technology. Innovations: Collection of Scientific Papers. In 10 parts*, Novosibirsk, NSTU publ., 2021, pp. 145–148.

17. Iksanov R. A., Muratova A.I. [Syntaxic difficulty of problem texts of normative legal acts in the sphere of economic activities]. *Bulletin of BIST (Bashkir Institute of Social Technologies)*, 2021, vol. 50, no. 1, pp. 81–85.

18. Ju A., Sajnani H., Kelly S., Herzig K. A Case Study of Onboarding in Software Teams: Tasks and Strategies. *Proceedings of the 43rd International Conference on Software Engineering*, 2021, pp. 613–623.

19. Schuegerl P., Rilling J., Charland P. Enriching SE ontologies with bug report quality. *Proceedings 4th International Workshop on Semantic Web Enabled Software Engineering*, 2008, pp. 1–17.

Erchimen I. Gavriliev
Postgraduate student, Department of Theoretical and Applied Computer Science (TACS),
Novosibirsk State Technical University (NSTU)
20, Karla Marksa pr., Novosibirsk, Russia, 630073
ORCID: 0000-0001-7289-3969
Phone: +7-923-246-05-82
Email: erchimen_gavriliev@outlook.com

Tatiana V. Avdeenko
Doctor of Science in Engineering, Professor,
Department of TACS NSTU
20, Karla Marksa pr., Novosibrsk, Russia, 630073
ORCID: 0000-0002-8614-5934
Phone: +7-913-951-60-06
Email: tavdeenko@mail.ru

ЭЛЕКТРОТЕХНИКА

УДК 51-74.621

А.И. Андриянов, М.В. Баранчиков

Управление нелинейными динамическими процессами трехфазных рекуперирующих преобразователей с пространственно-векторной модуляцией

Рассматривается система управления нелинейными динамическими процессами трехфазных рекуперирующих преобразователей, построенная на основе метода направления на цель, благодаря чему возможно обеспечить желаемый динамический режим без дополнительного параметрического синтеза. Это позволяет исключить противоречие между требованиями, предъявляемыми к частоте коммутации или параметрам переходного процесса в системе, и требованиями к желаемому динамическому режиму при изменении параметров внешних воздействий в широком диапазоне. Предложена система управления нелинейными динамическими процессами на основе метода направления на цель, позволяющая решить указанную проблему. При реализации рассматриваемой системы предполагается оценка координат неподвижных точек желаемого режима на основе измерений на реальном объекте управления с последующей цифровой обработкой полученных сигналов с целью выделения основных гармоник. Выполнено моделирование рассмотренной системы и показана эффективность предложенной системы управления нелинейными динамическими процессами. Предлагаемый подход может применяться в других системах преобразования электроэнергии с низкочастотными периодическими воздействиями с частотой сети в условиях низкочастотных искажений формы токов или напряжения в результате бифуркаций.
Ключевые слова: трехфазный рекуперирующий преобразователь, нелинейная динамика, бифуркация, система управления, метод направления на цель, желаемый динамический режим, низкочастотные периодические воздействия.
DOI: 10.21293/1818-0442-2022-25-4-125-133

Трехфазные рекуператоры электроэнергии применяются на технических объектах, где возможен возврат энергии при динамическом торможении двигателя или генерации. К таким объектам относятся лифтовое и крановое оборудование, центрифуги, электротранспорт и т.д. [1].

Такие устройства могут выпускаться как в виде отдельных блоков, подключаемых вместо тормозного резистора, так и быть встроенными в состав преобразователей частоты в виде активных выпрямителей на входе и работать в двунаправленном режиме. Также они могут выполняться в виде преобразователей для источников электроэнергии постоянного тока, подающих энергию в сеть переменного тока. Применение таких устройств позволяет во многих случаях экономить электроэнергию, обеспечивая при этом высокую электромагнитную совместимость с сетью.

Как известно, основной задачей при рекуперации является задача формирования трехфазного синусоидального тока, находящегося в противофазе со входным напряжением, что характерно для режима возврата энергии в сеть.

Трехфазные рекуперирующие преобразователи (ТРП) выполняются как системы автоматического управления, содержащие внешний контур напряжения звена постоянного тока и внутренние контуры фазных токов. При этом требуется обеспечить высокую синусоидальность тока, возвращаемого в сеть, с минимумом искажений.

Данные системы относятся к классу нелинейных динамических, и при определенном наборе параметров внешних воздействий возможны бифуркации и переход устройства в нежелательные динамические режимы, сопровождающиеся нелинейными колебаниями напряжения звена постоянного тока с большой амплитудой [3–5]. Это может существенно исказить синусоидальность сетевого тока. В реальных системах в широком диапазоне могут меняться входное напряжение, внешнее воздействие в виде тока звена постоянного тока, задание на напряжение звена постоянного тока, что требуется учитывать при построении систем управления.

Анализ сложных динамических режимов ТРП возможен лишь с применением нелинейных динамических моделей [3–5], которые учитывают динамические нелинейности систем рассматриваемого класса.

Проектирование регуляторов системы управления импульсными преобразователями электроэнергии, как правило, осуществляется на основе малосигнальных линейных динамических моделей с применением теории линейных систем автоматического управления [6–8], но это из-за ряда ограничений не всегда позволяет исключить возможность возникновения нежелательных динамических режимов в условиях меняющихся параметров внешних воздействий на систему [2].

Устранение нежелательных динамических режимов в импульсных преобразователях электроэнергии осуществляется с использованием двух подходов. Первый поход связан с дополнительным параметрическим синтезом, заключающимся в коррекции ранее рассчитанных параметров регулятора на основе малосигнальных моделей параметров регулятора или частоты коммутации ключей [3–5]. Второй подход связан со структурно-алгоритмическим синтезом [2, 9–11], когда строится система

управления, включающая в себя основную систему управления и систему управления нелинейными динамическими процессами (СУНДП), реализующую определенный алгоритм управления и позволяющую исключить нежелательные режимы без проведения дополнительного параметрического синтеза регулятора основной системы управления или повышения частоты коммутации ключей. Данный подход более сложный, но позволяет исключить недостатки параметрического синтеза, связанные со снижением быстродействия из-за коррекции параметров регуляторов или повышением динамических потерь из-за роста частоты коммутации.

Ранее одним из авторов был разработан ряд систем управления для преобразователей электроэнергии широкого класса, базирующихся на запаздывающей обратной связи и методе направления на цель [2]. Основной особенностью предложенных систем является внедрение дополнительной СУНДП, которая вводит корректирующие воздействия в замкнутые контуры основной системы управления. Это позволяет обеспечить желаемый динамический режим в широком диапазоне изменения параметров системы.

В [2] рассматривалась СУНДП для ТРП, базирующаяся на запаздывающей обратной связи, которая показала приемлемые результаты. В то же время метод направления на цель [2, 13], являющийся более эффективным с точки зрения устранения нежелательных режимов, но при этом более сложным с точки зрения технической реализации, для управления нелинейными динамическим процессами ТРП не применялся, что является актуальной задачей.

В данной работе рассмотрен трехфазный рекуператор электроэнергии, построенный на основе трехфазного мостового преобразователя с системой управления на основе пространственно-векторной модуляции [12] с функцией управления нелинейными динамическими процессами на основе метода направления на цель. Предложена СУНДП, позволяющая устранять нежелательные динамические режимы в широком диапазоне изменения параметров внешних воздействий.

Описание системы

Схема замещения ТРП с пропорционально-интегральным регулятором напряжения и пропорциональным регулятором тока представлена на рис. 1. Она является модификацией схемы, ранее рассмотренной в [2], где использовалась скалярная широтно-импульсная модуляция и СУНДП на основе запаздывающей обратной связи.

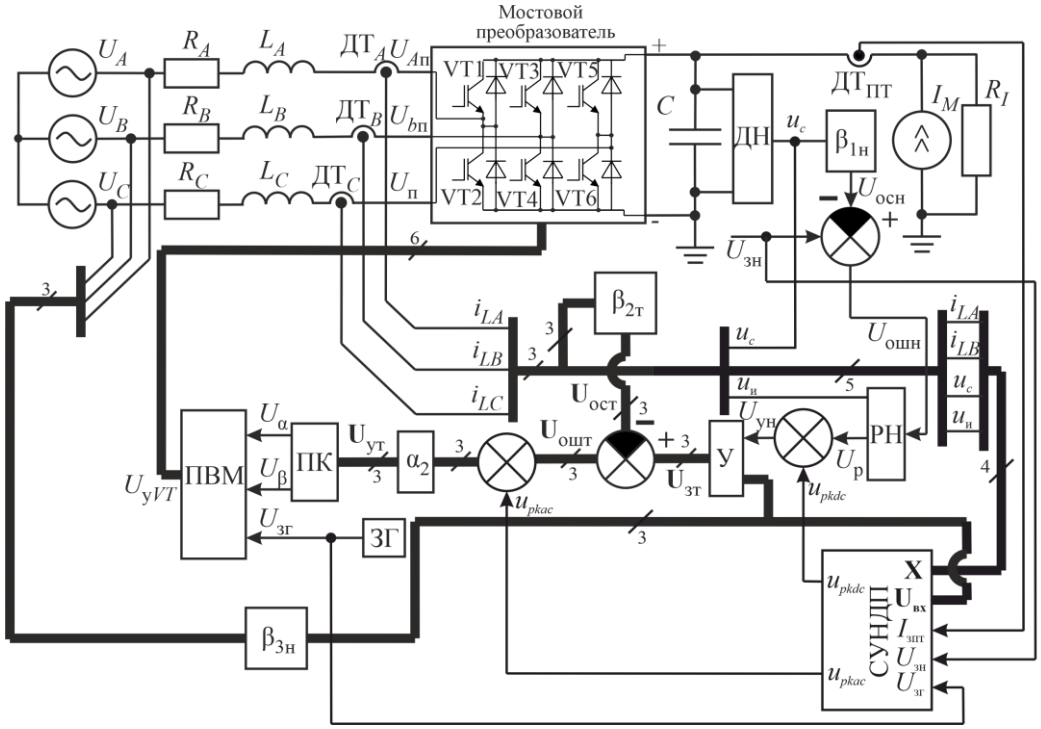


Рис. 1. Структурная схема трехфазного рекуперирующего преобразователя с системой управления на основе метода направления на цель

На рис. 1 используются обозначения: U_A, U_B, U_C – фазные напряжения питающей сети; L_A, L_B, L_C – дроссели фильтра; R_A, R_B, R_C – активные сопротивления дросселей фильтра; C – конденсатор фильтра; I_M – источник тока, имитирующий рекуперирующую нагрузку; R_I – внутреннее сопротивление источника тока I_M; $ДТ_A$, $ДТ_B$, $ДТ_C$ – датчики входного тока; $ДТ_П$ – датчик тока звена постоянного тока; ДН – датчик напряжения звена постоянного тока с коэффициентом $\beta_{1н}$; «мостовой преобразователь» – трехфазный мостовой преобразователь; $\beta_{2т}$ – коэффициент обратной связи по сетевым токам; $\beta_{3н}$ – коэффициент усиления датчиков входного напряжения; РН – регулятор напряжения; α_2 – коэффициент пропорционального регулятора тока; У – блок перемножения сигналов; ПК – преобразователь координ-

нат *A–B–C* в координаты α–β; ЗГ – задающий генератор; ПВМ – пространственно-векторный модулятор; СУНДП – система управления нелинейными динамическими процессами; $U_{\text{осн}}$ – сигнал обратной связи по напряжению; $\mathbf{U}_{\text{ост}} = [U_{\text{ост}A}, U_{\text{ост}B}, U_{\text{ост}C}]$ – вектор сигналов обратной связи по току фаз *A*, *B*, *C*; $U_{\text{ошн}}$ – сигнал ошибки по напряжению; $\mathbf{U}_{\text{ошт}} = [U_{\text{ошт}A}, U_{\text{ошт}B}, U_{\text{ошт}C}]^{\text{T}}$ – вектор сигналов ошибки по токам фаз; $U_{\text{зн}}$ – сигнал задания по напряжению; $\mathbf{U}_{\text{зт}} = [U_{\text{зт}A}, U_{\text{зт}B}, U_{\text{зт}C}]^{\text{T}}$ – вектор сигналов задания на ток фаз; $U_{\text{ун}}$ – сигнал управления контура звена постоянного тока; $\mathbf{U}_{\text{ут}} = [U_{\text{у}A}, U_{\text{у}B}, U_{\text{у}C}]^{\text{T}}$ – вектор сигналов управления контуров сетевых токов; $U_{\text{зг}}$ – напряжение задающего генератора; $U_{\text{уVT}}$ – сигналы управления транзисторами преобразователя; $\mathbf{U}_{\text{вх}}$ – вектор входных фазных напряжений; $\mathbf{X}$ – вектор фазовых переменных системы дифференциальных уравнений, описывающих электромагнитные процессы в системе $\mathbf{X}=(i_{LA}, i_{LB}, u_c, u_{\text{и}})^{\text{T}}=(x_1, x_2, x_3, x_4)^{\text{T}}$; i_{LA} – сетевой ток фазы *A*; i_{LB} – сетевой тока фазы *B*; u_c – напряжение на конденсаторе звена постоянного тока; $u_{\text{и}}$ – выходное напряжение интегратора в составе ПИ-регулятора напряжения; u_{pkdc} – корректирующее воздействие СУНДП, подаваемое в контур звена постоянного напряжения; u_{pkac} – корректирующее воздействие, подаваемое в контуры стабилизации сетевых токов.

Передаточная функция ПИ-регулятора напряжения имеет вид [2]

$$W(p) = \alpha_1 + \frac{1}{Tp + K},$$

где α_1 – коэффициент пропорциональной части ПИ-регулятора; *T* – постоянная времени интегратора ПИ-регулятора; *K* – коэффициент, учитывающий неидеальность реального ПИ-регулятора.

Рассматриваемая система управления (см. рис. 1) состоит из основной системы управления и СУНДП.

Основная система управления в составе рассматриваемой системы управления является известной двухконтурной системой с умножителем, где внешний контур – это контур стабилизации напряжения звена постоянного тока, а внутренний контур – это контур стабилизации фазных сетевых токов. Рассмотрим принцип ее действия. Для начала считаем, что СУНДП дезактивирована и не подает корректирующие воздействия в контуры основной системы управления, т.е. $u_{pkdc} = 0$ и $u_{pkac} = 0$ (см. рис. 1), т.е. система управления работает как классическая – без управления нелинейными динамическими процессами.

Сигнал обратной связи по напряжению $U_{\text{осн}}$ вычитается из сигнала задания на напряжение звена постоянного тока, и сигнал ошибки $U_{\text{ошн}}$ поступает на вход регулятора напряжения РН. Выходной сигнал РН $U_{\text{р}}$ поступает на вход умножителя У, на другой вход которого поступают масштабированные с множителем $\beta_{\text{зн}}$ сигналы фазных напряжений. Таким образом, временные зависимости компонентов вектора задания на сетевые токи $\mathbf{U}_{\text{зт}}$ по форме идентичны фазным напряжениям, а амплитуда определяется $U_{\text{р}}$. Далее из вектора сигналов задания на ток $\mathbf{U}_{\text{зт}}$ вычитается вектор сигналов обратных связей по сетевым фазным токам $\mathbf{U}_{\text{ост}}$ и вектор сигналов ошибок по сетевым токам поступает на регуляторы тока с коэффициентами α_2 (см. рис. 1). Вектор сигналов управления $\mathbf{U}_{\text{ут}}$ поступает на преобразователь координат Кларка, который преобразует координаты *A–B–C* в координаты α–β. Сигналы U_α и U_β далее поступают на пространственно-векторный модулятор. Основной задачей модулятора является формирование заданного положения и длины результирующего вектора фазных напряжений преобразователя $U_{A\text{п}}$, $U_{B\text{п}}$, $U_{C\text{п}}$, подаваемых в сеть через индуктивные фильтры L_A, L_B, L_C, что позволяет сформировать заданную форму сетевых токов. При этом стоит отметить, что для обеспечения гармонических колебаний тока в противофазе с входными напряжениями коэффициент α_2 должен быть отрицательным.

На рис. 2, *а* представлена векторная диаграмма, поясняющая принцип пространственно-векторной модуляции [12]. В данном случае будет рассматриваться односторонняя пространственно-векторная модуляция.

Как известно, с помощью мостового трехфазного преобразователя напряжения можно сформировать 6 ненулевых базовых векторов $\bar{U}_1 - \bar{U}_6$, каждый из которых соответствует определенной комбинации включенных ключей (рис. 2). Также есть нулевые векторы, которым соответствуют комбинации 1, 3, 5 или 2, 4, 6 [12].

Для формирования произвольного положения результирующего вектора напряжения $\bar{U}$ необходимо осуществить поочередное формирование базовых векторов, ограничивающих сектор, где должен располагаться результирующий вектор напряжения и одного из нулевых векторов. Так, на рис. 2, *б* представлены пояснения для сектора 1 (см. рис. 2, *а*).

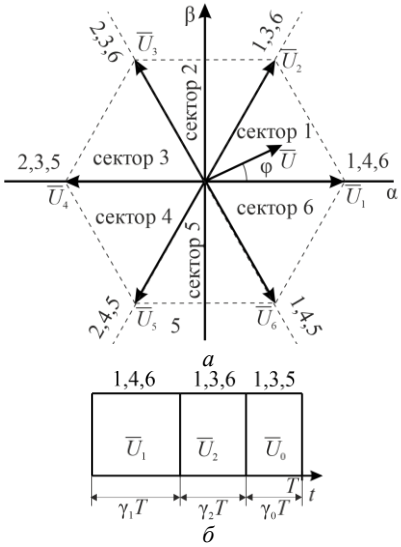


Рис. 2. К пояснению принципа формирования вектора выходного напряжения силовой части рекуперирующего преобразователя: *а* – векторная диаграмма; *б* – алгоритм переключения ключей в секторе 1

Коэффициенты γ_i, определяющие длительности формирования различных векторов, рассчитываются по выражениям [12]:

$$\gamma_1 = \mu \frac{2}{\sqrt{3}} \sin\left(\frac{\pi}{3} - \varphi\right);$$

$$\gamma_2 = \mu \frac{2}{\sqrt{3}} \sin\varphi;$$

$$\gamma_0 = 1 - \gamma_1 - \gamma_2,$$

где φ – требуемый угол поворота результирующего вектора напряжения в пределах сектора, μ – глубина модуляции, которая рассчитывается по выражению [12]

$$\mu = \frac{3}{2} \frac{U_{\text{фн}}}{U_c},$$

где $U_{\text{фн}}$ – выходное фазное напряжение трехфазного преобразователя, U_c – постоянное напряжение на конденсаторе.

Более подробное описание ПВМ представлено в [12].

Система управления нелинейными динамическими процессами

Функциональная схема СУНДП, предлагаемая в данной работе, представлена на рис. 3.

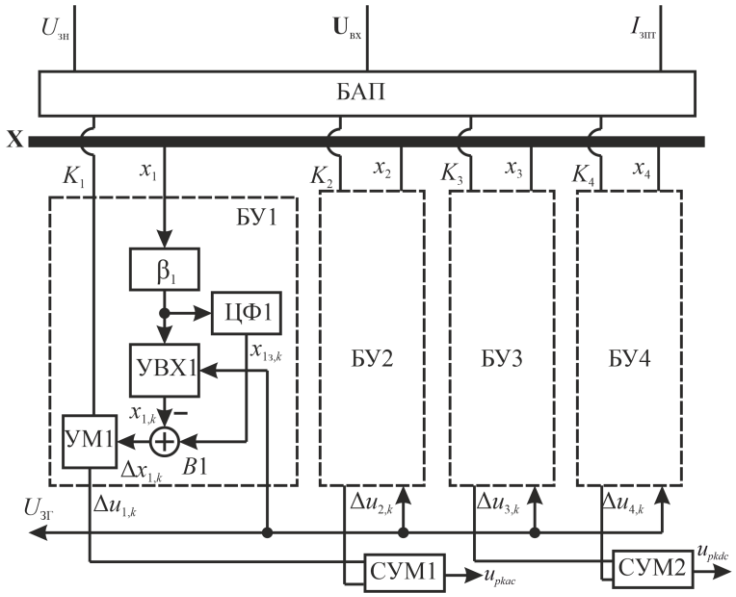


Рис. 3. СУНДП на основе метода направления на цель

Здесь приняты обозначения: БАП – блок адаптации параметров;, БУ*i* – блок управления по *i*-й фазовой переменной x_i;, β_i – масштабирующий усилитель *i*-й фазовой переменной с коэффициентом β_i;, УВХ*i* – устройство выборки-хранения блока БУ*i*;, ЦФ*i* – цифровой фильтр фазовой переменной x_i; УМ*i* – умножитель блока БУ*i*;, В*i* – вычитатель блока БУ*i*;, $x_{i,k}$ – значение *i*-й фазовой переменной в *k*-й дискретный момент времени;, $x_{iз,k}$ – задание на *i*-ю фазовую переменную x_i в *k*-й дискретный момент времени;, $\Delta u_{i,k}$ – корректирующее воздействие по *i*-й фазовой переменной;, СУМ1, СУМ2 – сумматоры корректирующих воздействий $\Delta u_{i,k}$.

Основной задачей СУНДП является стабилизация так называемых неподвижных точек отображения Пуанкаре. Как известно, для анализа нелинейных динамических систем с колебаниями используется метод точечных отображений.

Каждый тактовый интервал ПВМ описывается нелинейным дискретным отображением вида

$$\mathbf{X}_{p,k} = \Psi(\mathbf{X}_{p,k-1}),$$

где $\mathbf{X}_{p,k-1} = (x_{1,p,k-1}, x_{2,p,k-1}, x_{3,p,k-1}, x_{4,p,k-1})^{\mathrm{T}}$ и $\mathbf{X}_k = (x_{1,p,k}, x_{2,p,k}, x_{3,p,k}, x_{4,p,k})^{\mathrm{T}}$ – векторы переменных состояния в начале *k*-го и (*k*+1)-го тактового интервала соответственно с *p*-го периода входного напряжения.

В системах с низкочастотными периодическими воздействиями используется кратность квантования $q = f_q/f_s$, где f_q – частота квантования ПВМ, f_s – частота сетевого напряжения. Кратность квантования показывает, какое количество тактовых интервалов укладывается на периоде сетевого напряжения. Период сетевого напряжения с индексом *p* характеризуется *q* точками $\mathbf{X}_{p,0}$, $\mathbf{X}_{p,1}$, … $\mathbf{X}_{p,q-1}$ (отображением Пуанкаре), которые в установившемся периодическом режиме не меняют свои координаты. На рис. 4 представлена временная диаграмма фазовой переменной $x_1 = i_{LA}$, где в дискретные моменты времени черными кружками отмечены компоненты $x_{1,p-1,k}$ векторов $\mathbf{X}_{p-1,k}$.

Стробоскопическое отображение для системы с низкочастотными периодическими воздействиями при целочисленной кратности квантования *q* имеет вид

$$\mathbf{X}_p = \Psi^{(q)}(\mathbf{X}_{p-1}) \equiv \underbrace{\Psi \circ \Psi \circ \Psi \circ \Psi \circ \ldots \circ \Psi}_{q \text{ раз}}, \quad (1)$$

где *p* – номер итерации отображения и при этом для цикла периода один (1-цикл): $\mathbf{X}_p = \mathbf{X}_{p,0} = \mathbf{X}_{p+1} = \mathbf{X}_{p,q}$ (см. рис. 4).

Детализованное аналитическое описание стробоскопического отображения рассматриваемой

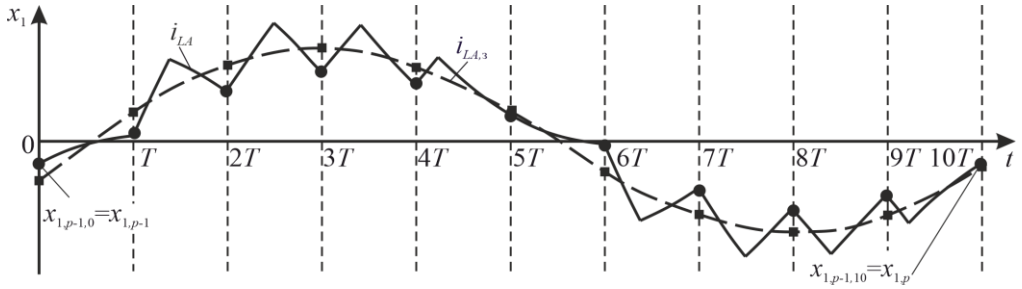


Рис. 4. К пояснению стробоскопического отображения

системы в целом аналогично выражению для систем со скалярной широтно-импульсной модуляцией [2] за исключением алгоритма расчета моментов коммутации на тактовом интервале. В данной статье оно подробно рассматриваться не будет из-за ограничения объема.

Рассмотрим понятие желаемого динамического режима. Под желаемым динамическим режимом ТРП будем понимать режим, в котором максимальный период электромагнитных процессов в ТРП равен периоду сетевого напряжения, т.е. $\mathbf{X}_p = \mathbf{X}_{p-1} = \mathbf{X}^*$, где $p = 1, 2, 3\ldots$, а $\mathbf{X}^*$ – неподвижная точка желаемого режима. Данный режим называется однократным режимом или 1-циклом.

В нежелательных динамическим режимах, сопровождающихся существенным искажением синусоидальности входного тока, максимальный период процессов в ТРП в m раз больше ($\mathbf{X}_p = \mathbf{X}_{p-m}$), чем период сетевого напряжения, где m – это так называемая кратность цикла. Данный режим называется m-циклом. Также могут возникать хаотические колебания. В областях параметров внешних воздействий, где реализуются нежелательные режимы, желаемый режим, как правило, существует, но является неустойчивым.

Для анализа устойчивости желаемого режима необходимо рассчитать так называемую матрицу монодромии, которая с учетом (1) определяется как [4, 5]

$$M = \frac{d\Psi^{(q)}(\mathbf{X}^*)}{d\mathbf{X}_{p-1}}. \qquad (2)$$

Желаемый режим устойчив, когда все собственные значения матрицы монодромии M лежат в пределах единичного круга [5].

Основной задачей СУНДП является стабилизация желаемого динамического режима (1-цикла) в широком диапазоне изменения параметров внешних воздействий путем введения в начале каждого тактового интервала корректирующих воздействий в основной контур управления. Для этого, как видно из рис. 4, по каждой фазовой переменной рассчитывается невязка

$$\Delta x_{i,k} = x_{i,k} - x_{i3,k}, \qquad (3)$$

где $x_{i3,k}$ – i-я координата k-й неподвижной точки отображения Пуанкаре желаемого режима в k-й дискретный момент времени; $x_{i,k}$ – текущее значение i-й координаты неподвижной точки отображения Пуанкаре в k-й дискретный момент времени.

Невязки $\Delta x_{i,k}$ умножаются с помощью умножителей УМi на коэффициенты K_i, вычисляемые блоком адаптации параметров (БАП). Коэффициенты K_i вычисляются таким образом, чтобы желаемый режим стал устойчивым, т.е. все собственные значения матрицы монодромии (2) стали меньше единицы. Для поиска оптимальных коэффициентов при каждом наборе параметров внешних воздействий применялся метод Нелдера–Мида по аналогии с [2]. Предварительный расчет оптимальных коэффициентов выполняется на этапе проектирования с использованием персональной ЭВМ в заданном диапазоне изменения внешних воздействий системы (см. входы БАП на рис. 3): входного фазного напряжения $U_{\text{вх}}$, тока звена постоянного тока I_M, задания на напряжение звена постоянного тока $U_{\text{зн}}$, а полученные результаты в форме таблицы загружаются в микроконтроллер, который реализует логику работы БАП.

Таким образом, каждый блок БУi выдает корректирующее воздействие

$$\Delta u_{i,k} = K_i \Delta x_{i,k}.$$

Как видно из рис. 1, СУНДП формирует два корректирующих воздействия: u_{pkdc} подается в контур стабилизации напряжения звена постоянного тока, так что

$$U_{\text{ун}} = U_{\text{р}} + u_{pkdc},$$

а u_{pkac} подается в контуры стабилизации сетевых токов, так что

$$\mathbf{U}_{\text{ут}} = \alpha_2 \begin{bmatrix} U_{\text{ош}A} + u_{pkac} \\ U_{\text{ош}B} + u_{pkac} \\ U_{\text{ош}C} + u_{pkac} \end{bmatrix}.$$

При этом, как следует из рис. 3:

$$u_{pkdc} = \Delta u_{3,k} + \Delta u_{4,k};$$

$$u_{pkac} = \Delta u_{1,k} + \Delta u_{2,k}.$$

Очевидно, что при работе в желаемом режиме невязки $\Delta x_{i,k} = 0$ и корректирующие воздействия в контуры управления не подаются.

Характерной чертой метода направления на цель является необходимость предварительной оценки координат неподвижных точек отображения Пуанкаре желаемого режима $x_{i3,k}$.

Оценку координат неподвижных точек желаемого режима предлагается проводить приближенно с помощью изменений в реальном времени на объекте управления с последующей цифровой обработкой полученных данных. Для этого физические ве-

личины, являющиеся фазовыми переменными математической модели силовой части устройства (i_{LA}, i_{LB}, u_c, $u_и$) [2], подаются на цифровые фильтры ЦФi, каждый из которых ориентирован на решение специфической задачи.

При этом принимаем следующие допущения:

– амплитуда высокочастотных (с частотой ПВМ) пульсаций переменных состояния невелика;

– амплитуду пульсаций выходного сигнала интегратора в составе ПИ-регулятора считаем незначительной и учитываем только постоянную составляющую, так что цифровая обработка $u_и$ не требуется.

При цифровой обработке напряжения на конденсаторе u_c будем выделять его среднее значение (постоянную составляющую) и гармонику с частотой 300 Гц (определяется пульсностью мостовой трехфазной схемы $p = 6$).

Для выделения среднего значения u_c использовался фильтр нижних частот с конечной импульсной характеристикой 8-го порядка, передаточная функция которого имеет вид

$$W_{03}(z) = b_0 \cdot \prod_{k=1}^{L} \frac{1 + b_{1k} z^{-1} + b_{2k} z^{-2}}{1 + a_{1k} z^{-1} + a_{2k} z^{-2}},$$

где L – количество секций фильтра. При 8-м порядке $L = 4$. Коэффициенты фильтра, при которых проводилось моделирование, следующие $b_0 = 1{,}391 \cdot 10^{-17}$; $b_{11} = 2$; $b_{21} = 1$; $a_{11} = -1{,}99$; $a_{21} = 0{,}99$; $b_{12} = 2$; $b_{22} = 1$; $a_{12} = -1{,}98$; $a_{22} = 0{,}98$; $b_{13} = 2$; $b_{23} = 1$; $a_{13} = -1{,}97$; $a_{23} = 0{,}97$; $b_{14} = 2$; $b_{24} = 1$; $a_{14} = -1{,}97$; $a_{24} = 0{,}97$.

Для выделения гармоники u_c с частотой 300 Гц использовался алгоритм Герцеля [14], который позволяет рассчитать амплитуду и фазу заданной гармоники с последующим переходом во временную область.

При обработке фазовых переменных i_{LA} и i_{LB} выделялась гармоника с частотой напряжения сети (50 Гц) также с применением алгоритма Герцеля.

Таким образом, на выходе блоков ЦФi формируются кривые $i_{LA,з}(t)$, $i_{LB,з}(t)$, $u_{с,з}(t)$, $u_{и,з}(t)$ (причем $u_{и,з}(t) = u_и(t)$). Одна из них ($i_{LA,з}(t)$) представлена на рис. 4.

Координаты q неподвижных точек желаемого 1-цикла определяются как $i_{LA,з}(kT)$, $i_{LB,з}(kT)$, $u_{с,з}(kT)$, $u_{и,з}(kT)$, где $k = 0, 1, \ldots q - 1$ (см. на рис. 4 на примере $i_{LA,з}(kT)$ отмечены черными квадратами).

Моделирование рекуперирующего преобразователя

При моделировании использовалась как математическая модель в форме стробоскопического отображения [2] после соответствующей модификации, так и среда Simulink. При моделировании были использованы следующие параметры: частота сетевого напряжения $\omega_с = 314$ рад/с ($f_с = 50$ Гц), кратность квантования $q = 80$, параметры дросселей фильтров: $R_A = R_B = R_C = 2$ Ом; $L_A = L_B = L_C = 20$ мГн; емкость конденсатора звена постоянного тока $C = 56$ мкФ; $R_I = 1$ МОм; $\beta_{1н} = 0{,}01$; $\alpha_1 = 0{,}1$; $K = 0{,}0001$; $T = 0{,}01$; $\beta_{2т} = 0{,}3$; $\beta_{3н} = 0{,}003$; $\alpha_т = 0{,}9$; $U_{зн} = 8$ В.

Результаты моделирования представлены на рис. 5.

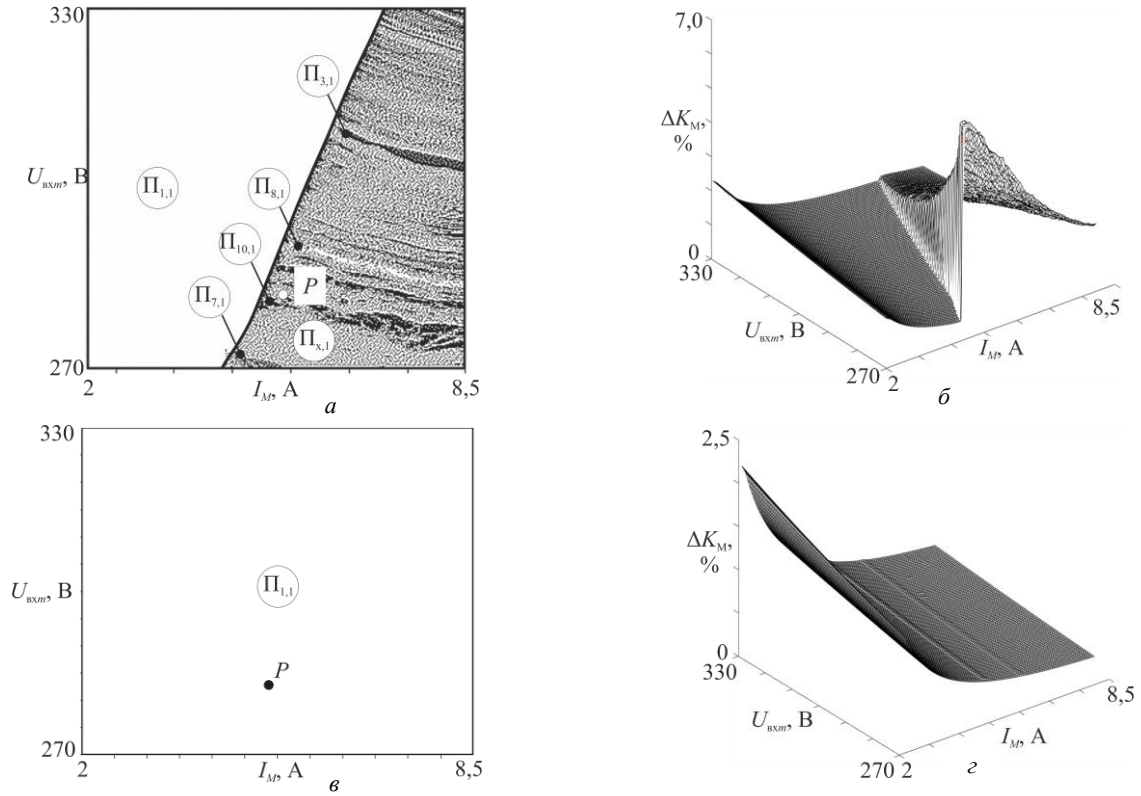


Рис. 5. Двухпараметрические диаграммы: *а* – карта динамических режимов без использования СУНДП; *б* – диаграмма абсолютного отклонения коэффициента мощности без использования СУНДП; *в* – карта динамических режимов с использованием СУНДП, *г* – диаграмма абсолютного отклонения коэффициента мощности с использованием СУНДП

На картах динамических режимов символами $П_{i,j}$ отмечены области существования различных динамических режимов (i – кратность цикла в данной области, j – номер области с кратностью цикла i на карте). В областях $П_{\infty,j}$ наблюдаются нежелательные хаотические или квазипериодические режимы.

Абсолютное отклонение коэффициента мощности от 100% рассчитывается как

$$K_{\text{М}} = 100 - \left| K_{\text{и}} \cos(\varphi) \right|,$$

где $K_{\text{и}}$ – коэффициент искажения, φ – угол сдвига между фазным напряжением и первой гармоникой выходного тока, при этом

$$K_{\text{и}} = \frac{I_{\text{ф1}}}{I_{\text{ф}}} 100\%,$$

где $I_{\text{ф1}}$ – действующее значение первой гармоники фазного тока, $I_{\text{ф}}$ – действующее значение фазного тока.

Сопоставление карты динамических режимов (см. рис. 5, *а*) и диаграммы абсолютного отклонения коэффициента мощности (см. рис. 5, *б*) показало, что в области нежелательных динамических режимов коэффициент мощности заметно меньше 100%, что говорит об ухудшении качества сетевого тока при рекуперации. Без применения СУНДП максимальное абсолютное отклонение коэффициента мощности составило 7% при I_M = 5 А и $U_{\text{вых}\,m}$ = 270 В.

Применение СУНДП полностью устранило нежелательные динамические режимы (см. рис. 5, в), и на всей площади карты наблюдается желаемый 1-цикл. Анализ рис. 5, *г* показал снижение абсолютного отклонения коэффициента мощности, которое составило не более 2% при I_M = 2 А и $U_{\text{вх}\,m}$ = 330 В.

На рис. 6 приведены временные диаграммы, построенные при I_M=5,5 А и $U_{\text{вх},m}$=280 В (точка *P* на рис. 5). В момент времени t_c=0,26 с произошла активация СУНДП. Из рисунка видно, что применение СУНДП на основе метода направления на цель обеспечило переход системы в желаемый динамический режим, характеризующийся синусоидальной формой сетевого тока ТРП. Длительность переходного процесса составила порядка $t_{\text{пп}}$ = 0,26 с.

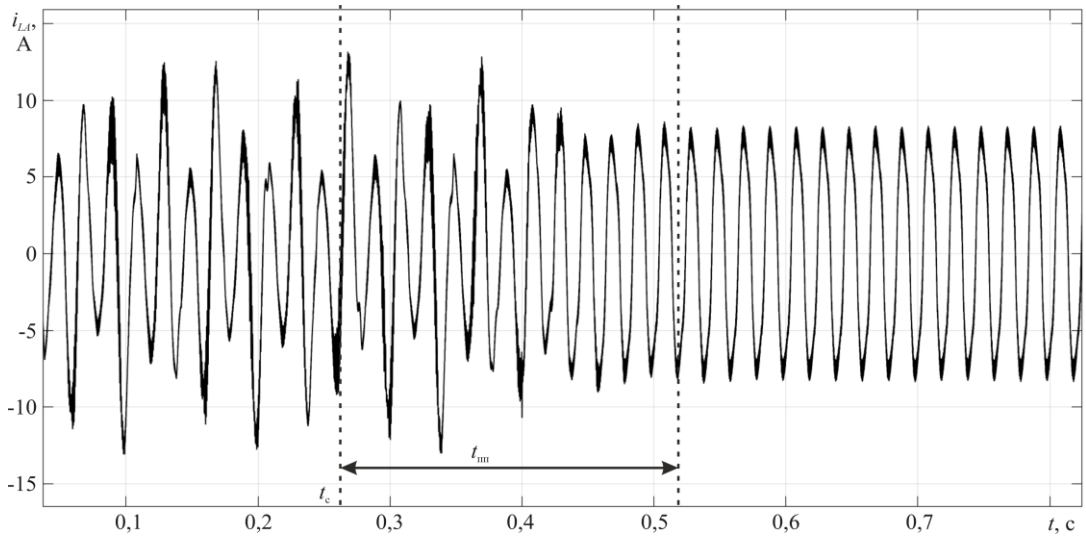


Рис. 6. Временные диаграммы тока дросселя i_{LA} при запуске СУНДП

Заключение

В данной работе рассмотрены вопросы построения системы управления трехфазным рекуперирующим преобразователем с учетом динамических нелинейностей. На основании полученных результатов можно сделать следующие выводы:

1. Разработана система управления трехфазным рекуперирующим преобразователем напряжения на основе пространственно-векторной модуляции с функцией управления на основе направления на цель.

2. Предлагаемая система управления учитывает возможность возникновения нежелательных динамических режимов при изменении параметров внешних воздействий в широком диапазоне.

3. Выполнено математическое моделирование электромагнитных процессов в устройстве с использованием нелинейной динамической модели и построены двупараметрические диаграммы.

4. Применение метода направления на цель позволило полностью устранить нежелательные динамические режимы в выбранных диапазонах параметров внешних воздействий и тем самым повысить коэффициент мощности, а следовательно, качество сетевого тока и напряжения звена постоянного тока. При этом стоит заметить, что быстродействие СУНДП на основе метода направления на цель несколько хуже, чем СУНДП на основе запаздывающей обратной связи [2], но при этом эффективность устранения нежелательных режимов в широком диапазоне изменения параметров внешних воздействий выше.

5. Полученные результаты после адаптации в перспективе могут быть распространены на устройства с другой структурой основной системы управления ТРП.

6. Предлагаемая система управления может быть реализована на современных цифровых про-

граммируемых микросхемах с функцией цифровой обработки сигналов.

За рамками данной работы остались вопросы обеспечения заданного быстродействия системы управления, построенной на основе метода направления на цель в условиях ступенчато меняющихся параметров внешних воздействий. Это может являться предметом исследования для отдельной статьи. Очевидно, что введение СУНДП снижает быстродействие системы в целом, но при этом стоит заметить, что устранение нежелательных динамических режимов с использованием стандартного подхода (дополнительный параметрический синтез регуляторов основной системы управления) также приводит к снижению быстродействия. В этой ситуации важно обеспечить, чтобы система управления с СУНДП была более эффективной с точки зрения быстродействия, чем обычная система управления, скорректированная с использованием стандартного подхода. На данный момент обнадеживающие результаты были получены одним из авторов для базовых преобразователей постоянного напряжения, которые в будущем требуется распространить и на рассматриваемый в данной работе класс систем.

А.И. Андрияновым разработана система управления рекуперирующим преобразователем напряжения, формирование алгоритмов расчета периодических режимов и анализа локальной устойчивости, разработано программное обеспечение, проведены расчет динамических режимов системы, анализ динамических режимов работы системы.

М.В. Баранчиковым реализованы адаптация математической модели трехфазного рекуперирующего преобразователя и анализ работы цифровых фильтров.

Литература

1. Kolar J.W. The essence of three-phase PFC rectifier systems. Part I / J.W. Kolar, T. Friedli // IEEE Transactions on Power Electronics. – 2013. – Vol. 28, No. 1. – P. 176–198.

2. Андриянов А.И. Развитие теории управления нелинейными динамическими процессами импульсных систем электропитания: дис. … -ра техн. наук. – Чебоксары, 2022. – 515 с.

3. Banerjee S. Nonlinear Phenomena in Power Electronics: Bifurcations, Chaos, Control and Applications / S. Banerjee, G.C. Verghese. – N.Y.: Wiley-IEEE Press, 2001. – 472 p.

4. Нелинейная динамика полупроводниковых преобразователей / А.В. Кобзев, Г.Я. Михальченко, А.И. Андриянов, С.Г. Михальченко. – Томск: Том. гос. ун-т систем упр. и радиоэлектроники, 2007. – 224 с.

5. Жусубалиев Ж.Т. Бифуркации и хаос в релейных и широтно-импульсных системах автоматического управления / Ж.Т. Жусубалиев, Ю.В. Колоколов. – М.: Машиностроение-1, 2001. – 120 с.

6. Low-Frequency Hopf Bifurcation and Its Effects on Stability Margin in Three-Phase PFC Power Supplies Connected to Non Ideal Power Grid / M. Huang, C.K. Tse, S.C. Wong, X. Ruan, C. Wan // IEEE Transactions on Circuits and Systems I: Regular Papers. – Dec. 2013. – Vol. 60, No. 12. – P. 3328–3340.

7. Interacting Bifurcation Phenomenon in Three-Phase Voltage Source Converter Connected to Non-ideal Power Grid / M. Huang, C.K. Tse, S.C. Wong, X. Ruan, C. Wan // Industrial Electronics Society −39th Annual Conference of the IEEE. – Nov. 2013. – P. 8373–8378.

8. Jian S. Small-Signal Methods for AC Distributed Power Systems–A Review // IEEE Transactions on Power Electronics. – Nov. 2009. – Vol. 24, No. 11. – P. 2545–2554.

9. Naihong H. Study on chaotic control of SPWM inverter and Its optimization / H. Naihong, Z. Yufei, C. Junning // Journal of Information & Computational Science. – 2012. – No. 2. – P. 497–504.

10. Fast-scale instability phenomena and chaotic control of voltage control single-phase full-bridge inverter via varying load resistance / F.-H. Hsieh, P.-L. Chang, Y.-S. Chen, H.-K. Wang, J.-C. Hwang // 2009 4th IEEE Conference on Industrial Electronics and Applications. – Xian, China: IEEE, 2009. – P. 3422–3427.

11. Control of fast scale bifurcations in Power-Factor correction converters / D. Giaouris, S. Banerjee, B. Zahawi, V. Pickert // IEEE Transactions on Circuits and Systems II: Express Briefs. – 2007. – Vol. 54, No. 9. – P. 805–809.

12. Усольцев А.А. Частотное управление асинхронными двигателями: учеб. пособие. – СПб.: СПбГУ ИТМО, 2006. – 95 с.

13. Andriyanov A.I. A comparative analysis of efficiency of nonlinear dynamics control methods for a buck converter // IOP Conference Series: Materials Science and Engineering. – 2017. – No. 177(1): 012001. DOI: 10.1088/1757-899X/177/1/012001.

14. Goertzel G. An Algorithm for the Evaluation of Finite Trigonometric Series // The American Mathematical Monthly. – 1958. – Vol. 65, No. 1. – P. 34–35.

Андриянов Алексей Иванович
Д-р техн. наук, доцент каф. электронных, радиоэлектронных и электротехнических систем (ЭРЭиЭС)
Брянского государственного технического ун-та (БГТУ)
50 лет Октября бул., 7, г. Брянск, Россия, 241035
ORCID: 0000-0002-4083-040X
Тел.: +7 (483-2) 56-36-02
Эл. почта: mail@ahaos.ru

Баранчиков Максим Викторович
Аспирант каф. ЭРЭиЭС БГТУ
50 лет Октября бул., 7, г. Брянск, Россия, 241035
Тел.: +7-952-960-27-40
Эл. почта: mbaranchikov@mail.ru

Andriyanov A.I., Baranchikov M.V.

Control of nonlinear dynamic processes of three-phase regenerative converters with space-vector modulation

A control system for nonlinear dynamic processes of three-phase regenerative converters is considered. The system is built on the basis of the target-oriented control and allows to provide the desired dynamic mode without additional parametric synthesis. It eliminates the contradiction between the requirements for the switching frequency or the parameters of the transient process in the system and the requirements for the desired dynamic mode when the system parameters change over a wide range. A control system for nonlinear dynamic processes based on the method of directing to the purpose is proposed, that allows solving the specified problem. When implementing the system under consideration, it is assumed to

evaluate the coordinates of fixed points of the desired mode based on measurements on a real control object with subsequent digital processing of the received signals in order to isolate the main harmonics. The simulation of the considered system and the efficiency of the proposed control system for nonlinear dynamic processes are performed. The proposed approach can be applied in other power conversion systems with low-frequency periodic impacts in conditions of low-frequency distortion of the shape of currents or voltage as a result of bifurcations.

Keywords: three-phase regenerative converter, nonlinear dynamics, bifurcation, control system, target oriented control, desired dynamic mode, low-frequency periodic effects.

DOI: 10.21293/1818-0442-2022-25-4-125-133

References

1. Kolar J. W., Friedli T. The essence of three-phase PFC rectifier systems. Part I. *IEEE Transactions on Power Electronics*, 2013, vol. 28, no. 1, pp. 176–198.

2. Andriyanov A.I. *Razvitie teorii upravleniya nelineynimi dinamicheskimi processami impulsih sistem elektropitaniya* [Development of the theory of control of nonlinear dynamic processes of pulsed power supply systems]. Cheboksary, 2022, 515 p. (in Russ.).

3. Banerjee S. Nonlinear Phenomena in Power Electronics: Bifurcations, Chaos, Control, and Applications. New York, *Wiley-IEEE Press*, 2001, 472 p.

4. Kobzev A.V. *Nelineynaya dinamika poluprovodnikovih preobrazovateley*. [Nonlinear dynamics of semiconductor converters]. Tomsk, TUSUR University, 2007, 224 p. (in Russ.).

5. Zhusubaliev Zh. T. *Bifurkaciya i haos v releynih i shirotno-impulsnih sistemah avtomaticheskogo upravleniya.* [Bifurcations and chaos in relay and pulse–width automatic control systems]. Moscow, Mechanical engineering-1, 2001, 120 p. (in Russ.).

6. Huang M., Tse C.K., Wong S.C., Ruan X., Wan C. Low-Frequency Hopf Bifurcation and Its Effects on Stability Margin in Three-Phase PFC Power Supplies Connected to Non-Ideal Power Grid. *IEEE Transactions on Circuits and Systems I: Regular Papers*, Dec. 2013, vol. 60, no. 12, pp. 3328–3340.

7. Huang M., Tse C.K., Wong S.C., Ruan X., Wan C. Interacting Bifurcation Phenomenon in Three-Phase Voltage Source Converter Connected to Non-ideal Power Grid. *Industrial Electronics Society – 39th Annual Conference of the IEEE*, Nov. 2013, pp. 8373–8378.

8. Jian S. Small-Signal Methods for AC Distributed Power Systems-A Review. *IEEE Transactions on Power Electronics*, Nov. 2009, vol. 24, no. 11, pp. 2545–2554.

9. Naihong H, Yufei Z., Junning C. Study on chaotic control of SPWM inverter and Its optimization. *Journal of Information & Computational Science*, 2012, no. 2, pp. 497–504.

10. Hsieh F.-H., Chang P.-L., Chen Y.-S., Wang H.-K., Hwang J.-C. Fast-scale instability phenomena and chaotic control of voltage control single-phase full-bridge inverter via varying load resistance. *2009 4th IEEE Conference on Industrial Electronics and Applications*, Xian, China: IEEE, 2009, pp. 3422–3427.

11. Giaouris D., Banerjee S., Zahawi B., Pickert V. Control of fast scale bifurcations in Power-Factor correction converters. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2007, vol. 54, no. 9, pp. 805–809.

12. Usolcev A.A. *Chastotnoe upravlenie asinhronnimi dvigatelyami*. [Frequency control of asynchronous motors]. St. Petersburg State University ITMO, 2006, 95 p. (in Russ.).

13. Andriyanov, A.I. A comparative analysis of efficiency of nonlinear dynamics control methods for a buck converter. *IOP Conference Series: Materials Science and Engineering*, Institute of Physics Publishing, 2017, 177(1): 012001. DOI: 10.1088/1757-899X/177/1/012001.

14. Goertzel G. An Algorithm for the Evaluation of Finite Trigonometric Series. *The American Mathematical Monthly*, 1958, vol. 65, no. 1, pp. 34–35

Alexey I. Andriyanov
Doctor of Science in Engineering, Associate Professor
Department of Electronics, Radioelectronic
and Electrotechnical Systems,
Bryansk State Technical University
7, 50 let Oktyabrya blvd., Bryansk, Russia, 241035
ORCID: 0000-0002-4083-040X
Phone: +7 (483-2) 56-36-02
Email: mail@ahaos.ru

Maksim V. Baranchikov
Postgraduate student, Department of Electronics,
Radioelectronic and Electrotechnical Systems,
Bryansk State Technical University
7, 50 let Oktyabrya blvd., Bryansk, Russia, 241035
Phone: +7-952-960-27-40
Email: mbaranchikov@mail.ru

УДК 621.314.6

А.В. Фролов, Н.Ю. Грунина

Исследование особенностей работы однополупериодного выпрямителя на ёмкостную нагрузку

Приводятся результаты теоретических расчётов и компьютерного моделирования в программе «SimInTech» работы однофазного однополупериодного выпрямителя с ёмкостным фильтром. Приводятся зависимости среднего значения, коэффициента пульсаций и минимального значения напряжения нагрузки от постоянной времени фильтра. Авторами получены графические зависимости и предложены аналитические выражения для расчета параметров напряжения, справедливые при малых постоянных времени фильтра ($0{,}1 < \tau < 100T$), проведена их верификация аналитически (с помощью численного решения уравнений) и имитационным моделированием в программе SimInTech. Точность аппроксимации предложенных выражений составила не менее 98%.

Ключевые слова: выпрямитель, моделирование, SimInTech, ёмкостный фильтр, среднее напряжение, коэффициент пульсаций.

DOI: 10.21293/1818-0442-2022-25-4-134-139

Как известно, сглаживающий фильтр является неотъемлемой частью любого источника вторичного электропитания и применяется для сглаживания пульсаций постоянного напряжения. Эти фильтры устанавливаются на выходе выпрямителя, а в импульсных схемах – на выходе схем силовых ключей. Применяемая для *LC*-фильтров классическая методика анализа работы схем проста и надёжна, но она не учитывает особенности работы выпрямителя с *C*-фильтром, которые заключаются в том, что среднее значение напряжения нагрузки, как и его коэффициент пульсаций, в значительной степени зависит от ёмкости конденсатора фильтра и величины активного сопротивления нагрузки. При этом режим работы схемы определяется величиной нагрузки. Так, например, при работе однофазного однополупериодного выпрямителя с ёмкостным фильтром его выходное напряжение значительно меняет свою форму в зависимости от тока нагрузки или от ёмкости фильтра (рис. 1) [1–3]. Это является широко известным фактом. Более того, очевидно, что среднее значение выходного напряжения будет изменяться в пределах от среднего до амплитудного значения входного напряжения выпрямителя, т.е. для однополупериодной схемы изменение составляет более чем в три раза относительно расчётного значения. Изменяется также и коэффициент пульсаций в зависимости от тока нагрузки от 0 (на холостом ходу) до $\pi/2$ (при больших нагрузках). Не менее интересен вопрос изменения минимального мгновенного значения напряжения нагрузки от ее характера. Вышесказанное иллюстрируется диаграммами, приведёнными на рис. 1, при ёмкости сглаживающего фильтра 100 мкФ и нагрузках от 2 Ом до 2 кОм.

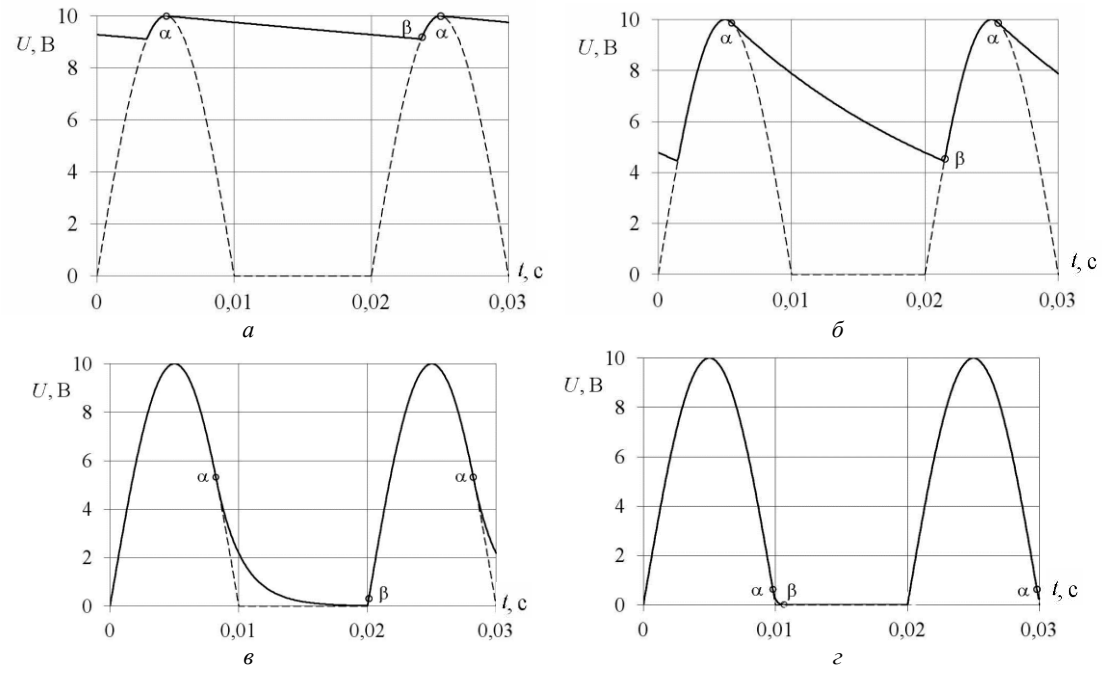


Рис. 1. Диаграммы выходного напряжения однофазного однополупериодного выпрямителя с ёмкостным фильтром при постоянных времени цепи разряда: $\tau = 10T$ (*а*); $\tau = T$ (*б*); $\tau = 0{,}1T$ (*в*); $\tau = 0{,}01T$ (*г*)

Зависимости среднего напряжения нагрузки от значения ёмкости фильтра в литературе описываются достаточно приближённо [1–10], часто определяются сложным образом с помощью номограмм и только для граничных режимов [18]

$$\frac{R_{\text{вн}}}{R_{\text{н}}} \geq \frac{10}{(m\omega CR_{\text{н}})^2} \quad \text{либо} \quad \frac{R_{\text{вн}}}{R_{\text{н}}} < \frac{4}{(m\omega CR_{\text{н}})^2},$$

где $R_{\text{н}}$ – сопротивление нагрузки, Ом.

Формул расчёта ёмкостного фильтра в современной литературе встречается несколько, и они противоречивы [3, 4, 6, 16], некоторые из них:

$$K_{\text{сп}} = 2\pi fCR_{\text{н}} + 1, \quad (1)$$

$$K_{\text{сп}} = \sqrt{(2\pi fCR_{\text{н}})^2 + 1}, \quad (2)$$

$$\begin{cases} K_{\text{п}} = \dfrac{1}{\sqrt{3}(4fCR_{\text{н}} - 1)}, \\ CR_{\text{н}} > \dfrac{1}{2\pi f}, \end{cases} \quad (3)$$

где $K_{\text{п}}$ – коэффициент пульсаций напряжения; $K_{\text{сп}}$ – коэффициент сглаживания пульсаций; f – частота пульсаций, Гц; C – ёмкость конденсатора, Ф.

В связи с актуальностью выбранной темы исследований в статье приводятся результаты теоретических и модельных исследований влияния постоянной времени цепи нагрузки выпрямителя (ёмкости сглаживающего фильтра и активного сопротивления нагрузки) на параметры выходного напряжения: среднего и минимального значений, а также коэффициента пульсаций.

Методика исследований

Теоретические исследования выполнялись на основе схемы выпрямителя с фильтром (рис. 2). Для упрощения математических расчётов параметры элементов схемы идеализировались: нагрузка представлялась идеальным резистором; внутреннее сопротивление выпрямителя принималось много меньше сопротивления нагрузки; падение напряжения на диоде, обратный ток диода и омическое сопротивление диода не учитывались.

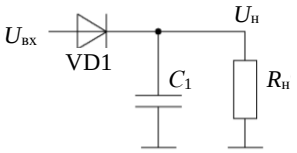


Рис. 2. Схема однофазного однополупериодного выпрямителя с ёмкостным фильтром

Вместо натурных испытаний выполнялось имитационное моделирование [5–7], [11–15], так как оно обеспечивает достаточно достоверные результаты, но не требует изготовления испытательного оборудования и отличается меньшей трудоёмкостью. Модельные исследования выполнялись с помощью программного симулятора SimInTech (рис. 3).

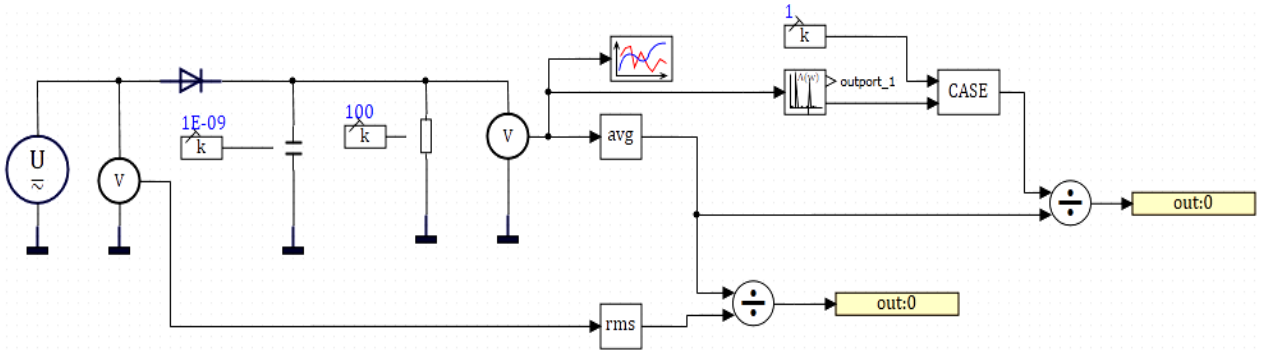


Рис. 3. Модель исследуемой схемы в программе SimInTech

Параметры элементов модели:

– источник входного сигнала (U) – амплитуда 100 В; частота 10 Гц; сопротивление источника – нет;

– диод – 1N4004 (сопротивление утечки перехода – 10 МОм; последовательное сопротивление – 42,9 мОм; ток насыщения – 31,98 нА);

– сопротивление нагрузки – 100 Ом, что обеспечивало среднее значение тока диода не более 1 А;

– ёмкость фильтра – 10 мкФ … 0,1 Ф, что обеспечивало изменение постоянной времени цепи нагрузки $\tau = 0,01T...100T$.

Модель автоматически рассчитывает среднее значение (*avg*) выходного напряжения и действующее значение (*rms*) входного напряжения, а также коэффициент пульсаций выходного напряжения. Минимальное значение выходного напряжения определялось с помощью инструмента моделирования «TimeGraphic». Измерения напряжений выполнялись с помощью вольтметров (*V*). Блоки констант (*k*) задавали значения ёмкости конденсатора, сопротивления нагрузки.

Параметры расчёта: минимальный шаг – 5 мкс; максимальный шаг – 100 мкс; начальный шаг интегрирования – 0 с; метод интегрирования – *RK*45; относительная ошибка 10^{-4}; абсолютная ошибка – 10^{-6}; относительная ошибка сравнения времени – 10^{-12}; шаг синхронизации задачи – 100 мкс.

Результаты исследований и их обсуждение

Для однофазной однополупериодной схемы с ёмкостным фильтром период выходного напряжения можно разбить на два интервала: интервал разряда конденсатора фильтра через нагрузку и интервал заряда конденсатора фильтра от выпрямителя. Заряд конденсатора фильтра осуществляется выходным напряжением выпрямителя, которое описывается формулой

$$\begin{cases} U_1(t) = U_m \sin(\omega t), \ T < t < \dfrac{T}{2}, \\ U_1(t) = 0, \dfrac{T}{2} < t < T, \end{cases}$$
$$\omega = 2\pi f,$$
$$f = 1/T,$$

где $U_1(t)$ – выходное напряжение выпрямителя без фильтра, В; U_m – амплитуда входного напряжения выпрямителя, В; ω – частота напряжения, рад/с; T – период напряжения, с; f – частота напряжения, Гц.

Разряд конденсатора выполняется через активную нагрузку по следующему закону:

$$U_2(t) = U_1(\alpha) e^{-\frac{t-\alpha}{\tau}} = U_m \sin(\omega\alpha) e^{-\frac{t-\alpha}{\tau}},$$
$$\tau = CR_н,$$

где $U_2(t)$ – выходное напряжение фильтра во время разряда конденсатора, В; α – время коммутации (начала разряда), с; τ – постоянная времени цепи, с. Разряд конденсатора происходит при закрытом диоде выпрямителя. А диод закрывается в случае, если напряжение на конденсаторе превышает выходное напряжение выпрямителя: $U_2(t) > U_1(t)$. Поэтому точка коммутации α соответствует моменту времени, начиная с которого будет выполняться это неравенство.

Функция $U_1(t)$ на интервале $T/4 \le t \le T/2$ монотонно убывает, а скорость ее убывания растёт с увеличением t и определяется по величине первой производной

$$-\frac{dU_1(t)}{dt} = -U_m \omega \cos(\omega t).$$

Функция $U_2(t)$ на этом же интервале также монотонно убывает, а скорость убывания функции падает с ростом t:

$$-\frac{dU_2(t)}{dt} = \frac{U_m}{\tau} \sin(\omega\alpha) e^{-\frac{t-\alpha}{\tau}}.$$

Поэтому точка коммутации α будет соответствовать моменту времени, в котором равны как обе функции, так и их производные. Этому моменту соответствует время

$$\alpha = \frac{atg(-\omega\tau) + \pi}{\omega}.$$

Вторая точка коммутации β соответствует точке пересечения функций $U_1(t)$ и $U_2(t)$ на интервале $T/2 \le t \le 5T/4$. На этом интервале функция $U_1(t)$ либо равна нулю, либо монотонно возрастает, а функция $U_2(t)$ монотонно убывает. Поэтому для нахождения угла коммутации β необходимо решить уравнение

$$\begin{cases} U_m \sin(\omega\beta) = U_m \sin(\omega\alpha) e^{-\frac{\beta-\alpha}{\tau}}, \\ T/2 \le t \le 5T/4. \end{cases}$$

Аналитическое решение этого уравнения представляется затруднительным, поэтому угол коммутации определялся численными методами.

Напряжение нагрузки анализируемой схемы выпрямителя с ёмкостным фильтром можно описать следующей формулой:

$$U_н(t) = \begin{cases} U_1(t), U_1(t) \ge U_2(t), \\ U_2(t), U_1(t) < U_2(t), \end{cases}$$
$$\alpha \le t \le \alpha + T.$$

Относительное среднее значение напряжения нагрузки рассчитывалось численными методами по формуле

$$U_н = \frac{\sqrt{2}}{U_m} \frac{1}{T} \int_{\alpha}^{\alpha+T} U_н(t) dt. \quad (4)$$

Коэффициент пульсаций напряжения нагрузки рассчитывался следующим образом:

$$\begin{cases} K_п = \dfrac{U_г}{U_н}, \\ U_г = \sqrt{A^2 + B^2}, \\ A = \dfrac{2}{T} \int_{\alpha}^{\alpha+T} U_н(t) \cos\left(\dfrac{2\pi t}{T}\right) dt, \\ B = \dfrac{2}{T} \int_{\alpha}^{\alpha+T} U_н(t) \sin\left(\dfrac{2\pi t}{T}\right) dt, \end{cases} \quad (5)$$

где $K_п$ – коэффициент пульсаций напряжения; $U_г$ – амплитуда первой гармоники напряжения нагрузки, В; $U_н$ – среднее значение напряжения нагрузки, В; A, B – косинусный и синусный коэффициенты первой гармоники ряда Фурье.

Результаты расчёта и моделирования работы схемы (в программе SimInTech) показаны на рис. 4–6. На рис. 4 представлена теоретически рассчитанная по формуле (4) зависимость относительного среднего напряжения нагрузки от значения постоянной времени фильтра (кривая *1*), а также отображены результаты моделирования работы схемы в программе SimInTech (точки *2*).

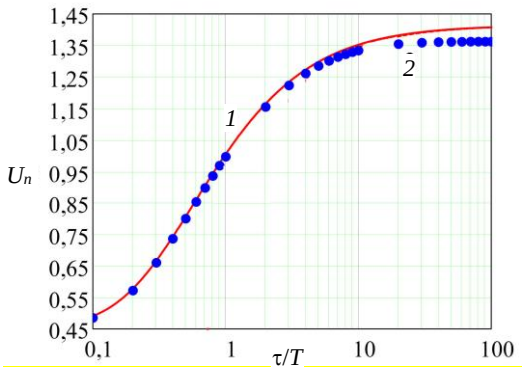


Рис. 4. Расчётная (*1*) и экспериментальная (*2*) зависимости относительного среднего напряжения нагрузки от постоянной времени цепи нагрузки

На рис. 5 представлена расчётная зависимость минимального напряжения нагрузки от значения постоянной времени *RC*-цепи (кривая *1*), а также отображены результаты моделирования работы схемы в программе SimInTech (точки *2*). Погрешность между расчётными значениями и результатами моделирования не превышает 2%.

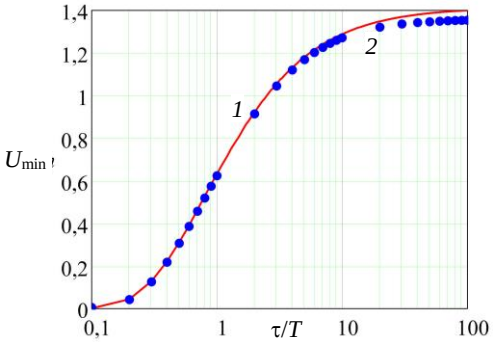


Рис. 5. Расчётная (*1*) и экспериментальная (*2*) зависимости относительного минимального напряжения нагрузки от постоянной времени цепи нагрузки

Расхождения теоретически рассчитанных значений с результатами моделирования вызваны тем, что при теоретическом расчёте схема идеализировалась, а при моделировании применялись параметры реального диода. Погрешность не превышает 4%.

На рис. 6 представлены: расчётная зависимость коэффициента пульсаций напряжения нагрузки от постоянной времени *RC*-цепи по формуле (5) – сплошная кривая 1; зависимость коэффициента пульсаций от постоянной времени цепи, полученная в результате моделирования в программе SimInTech, – точки 2, а также зависимости коэффициента пульсаций от постоянной времени цепи, полученные по известным формулам (1) и (2), – пунктирные кривые *3* и *4*.

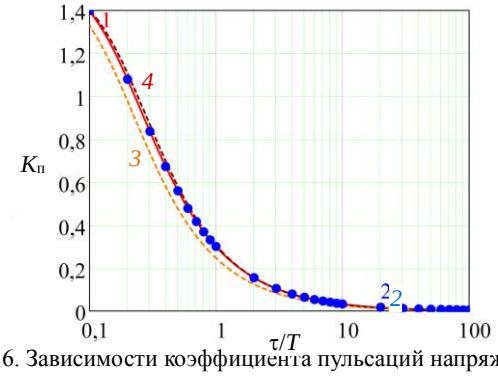


Рис. 6. Зависимости коэффициента пульсаций напряжения нагрузки от постоянной времени цепи нагрузки: расчётная (*1*), экспериментальная (*2*), аппроксимирующая по формуле (1) (*3*) и аппроксимирующая по формуле (2) (*4*)

Из известных зависимостей наиболее точно зависимость коэффициента пульсаций от постоянной времени цепи нагрузки описывает формула (2), при этом коэффициент детерминации составляет $R^2 = 0{,}979$.

Для обеспечения возможности применения полученных зависимостей в расчётах графики на рис. 4–6 можно аппроксимировать следующими аналитическими зависимостями:

$$U_n\left(\frac{\tau}{T}\right) = \sqrt{2}\left(1 - \frac{\pi - 1}{\sqrt[1,3]{\left(1{,}66\pi\frac{\tau}{T}\right)^{1,3} + \pi^{1,3}}}\right), \quad (6)$$

$$K_п\left(\frac{\tau}{T}\right) = \frac{\pi}{2\sqrt{\left(1{,}6\pi\frac{\tau}{T}\right)^2 + 1}}, \quad (7)$$

$$U_{min}\left(\frac{\tau}{T}\right) = \sqrt{2}\left(1 - \frac{1}{\sqrt[1,45]{\left(0{,}38\pi\frac{\tau}{T}\right)^{1,42} + 1}}\right). \quad (8)$$

При этом коэффициенты детерминации составляют $R^2 = 0{,}999$ в диапазоне $0{,}01T \le \tau \le 100T$.

Заключение

Наибольшие изменения среднего напряжения нагрузки, коэффициента пульсаций напряжения нагрузки и минимального мгновенного напряжения нагрузки происходят в диапазоне постоянных времени фильтра $0{,}1T < \tau \le 10T$. Зависимости параметров напряжения нагрузки от постоянной времени описать аналитически не удаётся, и при расчётах необходимо пользоваться либо графическими данными (см. рис. 4–6), либо рассчитывать численными методами. Приближённо можно использовать полученные авторами аппроксимирующие функции (6)–(8) с коэффициентом детерминации $R^2 = 0{,}999$ (в диапазоне $0{,}01T \le \tau \le 100T$).

Литература

1. Бурков А.Т. Электроника и преобразовательная техника. – М.: УМЦ ЖДТ, 2015. – 307 с.

2. Гейтенко Е.Н. Источники вторичного электропитания. Схемотехника и расчёт. – М.: СОЛОН-ПРЕСС, 2008. – 448 с.

3. Ефимов И.П. Источники питания РЭА. – Ульяновск: УлГТУ, 2002. – 136 с.

4. Бладыко Ю.В. Сглаживающие фильтры // Энергетика. Известия высших учебных заведений и энергетических объединений СНГ. – 2010. – № 2. – С. 36–40.

5. Петров А. Трансформаторы, выпрямители, фильтры [Электронный ресурс]. – Режим доступа: https://www.radioradar.net/hand_book/documentation/tran.html#5, свободный (дата обращения: 11.10.2022).

6. Романов В.П. Электропитание средств вычислительной техники. – Новокузнецк: ФГОУ СПО «Кузнецкий индустриальный техникум», 2008. – 94 с.

7. Сажнёв А.М. Электропитание устройств и систем связи / А.М. Сажнёв, Л.Г. Рогулина, С.С. Абрамов. – Новосибирск: ГОУ ВПО СибГУТИ, 2008. – 112 с.

8. Климаш В.С. Разработка конденсаторных установок и способа регулирования реактивной мощности в системах промышленного электроснабжения / В.С. Климаш, Б.Д. Табаров // Учёные записки Комсомольского-на-Амуре государственного технического университета. – 2022. – №1 (57). – С. 7–14. DOI: 10.17084/20764359-2022-57-7.

9. Иванов С.Н. Теоретические основы математического моделирования процессов преобразования мощности в совмещённых энергетических устройствах / С.Н. Иванов, К.К. Ким, О.В. Приходченко и др. // Учёные записки Комсомольского-на-Амуре государственного технического университета. – 2020. – № 1 (41). – С. 37–44.

10. Егоров В.А. Микроконтроллерная система управления автономным инвертором с упрощённой простран-

ственно-временной широтно-импульсной модуляцией / В.А. Егоров, Ю.Г. Егорова, Е.В. Плотников // Учёные записки Комсомольского-на-Амуре государственного технического университета. – 2020. – № 3 (43). – С. 36–42.

11. Болдырев В.В. Разработка интеллектуального модуля управления автоматизированной автономной системой энергообеспечения / В.В. Болдырев, М.А. Горькавый // Учёные записки Комсомольского-на-Амуре государственного технического университета. – 2020. – № 3 (43). – С. 9–18.

12. Иванов С.Н. Анализ электромеханических систем методами имитационного моделирования / С.Н. Иванов, К.К. Ким, А.А. Просолович и др. // Учёные записки Комсомольского-на-Амуре государственного технического университета. – 2021. – № 3 (51). – С. 29–38. DOI: 10.17084/20764359-2021-51-29.

13. Сочелев А.Ф. Математическая модель регулятора переменного напряжения с вольтодобавочным каналом // Учёные записки Комсомольского-на-Амуре государственного технического университета. – 2019. – № 3 (39). – С. 27–37.

14. Ахрамович С.А. Использование среды динамического моделирования технических систем SIMINTECH в задачах полунатурного моделирования / С.А. Ахрамович, А.В. Сычёв, А.М. Колпаков и др. // Тезисы докл. XXIV Междунар. науч. конф. «Системный анализ, управление и навигация». – М.: Изд-во МАИ-Принт, 2019. – С. 71–73.

15. Воронцов И.Н. Моделирование в SIMINTECH устройств силовой электроники / И.Н. Воронцов, И.С. Ситников // Матер. 76-й студенческой науч. конф. – Брянск: Изд-во Брян. гос. техн. ун-та, 2021. – С. 597–598.

16. Ллойд П. Справочник по полупроводниковой электронике. – М.: Машиностроение, 1975. – 508 с.

17. Борисов П.А. Расчет и моделирование выпрямителей: учеб. пособие по курсу «Элементы систем автоматики». – Ч. I / П.А. Борисов, В.С. Томасов. – СПб.: СПб ГУ ИТМО, 2009. – 169 с.

18. Коновалов Б.И. Основы преобразовательной техники: учеб. пособие / Б.И. Коновалов, В.С. Мишуров. – Томск: ТУСУР, 2015. – 197 с.

Фролов Алексей Валерьевич
Канд. техн. наук, доцент каф. промышленной электроники Комсомольского-на-Амуре государственного университета (КнАГУ)
Ленина ул., 27, г. Комсомольск-на-Амуре, Россия, 681013
ORCID: 0000-0002-9406-1095
Тел.: +7 (421-7) 24-11-92
Эл. почта: Afrolov.kms@mail.ru

Грунина Надежда Юрьевна
Студент каф. промышленной электроники КнАГУ
Ленина ул., 27, г. Комсомольск-на-Амуре, Россия, 681013
Тел.: +7 (421-7) 24-11-92
Эл. почта: Uheybyf1999uheybyf1999@gmail.com

Frolov A.V., Grunina N.Y.

Study of a single-wave rectifier with capacitive load

The article presents the results of theoretical calculations and SimInTech program simulation of a function of a single-phase single-wave rectifier with a capacitive filter and an active load. The correlation between the average load voltage, the minimum load voltage, the ripple factor and the RC load constant are given. The article shows that the available in literature approximating dependences of the load voltage characteristics do not correspond to either the results of theoretical calculations or the results of mathematical modeling. The found dependences allow to produce the optimal value of the smoothing filter capacitance for the desired load.

Keywords: rectifier, calculation, simulation, SimInTech, capacitive smoother, average voltage, ripple factor, minimum voltage.
DOI: 10.21293/1818-0442-2022-25-4-134-139

References

1. Burkov A.T. *Electronica i preobrazovatelnaya tehnica* [Electronics and transformative technology]. M., EMC RT, 2015, 307 p. (in Russ.).

2. Geytenko E.N. *Istochniki vtorichnogo eletropitaniya. Chemotehnika i raschet* [Secondary power sources. Circuit design and calculation]. Moscow, SOLON-PRESS, 2008, 448 p. (in Russ.).

3. Efimov I.P. *Istochniki pitaniya REA* [Power sources of electronic equipment]. Ulyanovsk, USTU, 2002, 136 p. (in Russ.).

4. Bladiko Y.V. [Ripple filter]. *Energy. News of higher educational institutions and energy associations of the CIS*, 2010, no. 2, pp. 36–40 (in Russ.).

5. Petrov A. [Transformers, rectifiers, filters]. Available at: https://www.radioradar.net/hand_book/documentation/tran.html#5, free (Accessed: October 11, 2022) (in Russ.).

6. Romanov V.P. *Electropitanie sredstv vichislitelnoy techniki* [Power supply of computer equipment]. Novokuznetsk, KIT, 2008, 94 p. (in Russ.).

7. Sajnev A.M., Rogulina L.G., Abramov S.S. *Electropitanie ustroistv i system svyazi* [Power supply of communication devices and systems]. Novosibirsk, SibSUTIS, 2008, 112 p. (in Russ.).

8. Klimash V.S., Tabarov B.D. [Development of capacitor devices and a method for regulating reactive power in industrial power supply systems]. *Scientific Notes of KnASTU*, 2022, no. 1 (57), pp. 7–14. DOI: 10.17084/20764359-2022-57-7 (in Russ.).

9. Ivanov S.N., Kim K.K., Prihodchenko O.V. [Theoretical foundations of mathematical modeling of power conversion processes in combined energy devices]. *Scientific Notes of KnASTU*, 2020, no. 1 (41), pp. 37–44 (in Russ.).

10. Egorov V.A., Egorova Y.G., Plotnikov E.V. [Microcontroller control system of an autonomous inverter with simplified space-time pulse-width modulation]. *Scientific Notes of KnASTU*, 2020, no. 3 (43), pp. 36–42 (in Russ.).

11. Boldirev V.V., Gorkaviy M.A. [Development of an intelligent control module for an automated autonomous power supply system]. *Scientific Notes of KnASTU*, 2020, no. 3 (43), pp. 9–18 (in Russ.).

12. Ivanov S.N., Kim K.K., Prosolovich A.A. [Analysis of electromechanical systems by simulation methods]. *Scientific Notes of KnASTU*, 2021, no. 3 (51), pp. 29–38. DOI: 10.17084/20764359-2021-51-29 (in Russ.).

13. Sochelev A.F. [Mathematical model of an alternating voltage regulator with an additional voltage channel]. *Scientific Notes of KnASTU*, 2019, no. 3 (39), pp. 27–37 (in Russ.).

14. Ahramovich A.A., Sichev A.V., Kolpakov A.M. [Using the SIMINTECH dynamic modeling environment for semi-natural modeling tasks]. *System Analysis, Management and Navigation*. Proceedings of the XXIV International scientific conference. M., MAI-PRINT, 2019. pp. 71–73 (in Russ.).

15. Vorontsov I.N., Sitnikov I.S. [SIMINTECH modeling of power electronics devices]. *Materials of the 76th Student Scientific Conference*. Proceedings of the 76th student scientific conference. Bryansk, BSTU, 2021, pp. 597–598 (in Russ.).

16. Lloyd P. *Spravochnik po poluprovodnikovoy electronike* [Handbook of Semiconductor Electronics]. M., Mechanical engineering. 508 p. (in Russ.).

17. Borisov P.A., Tomasov V.S. *Raschet I modelirovanie vipryamitiley* [Rectifires calculation and modeling]. Saint Petersburg, SPb GU ITMO. 169 p. (in Russ.).

18. Konovalov B.I., Mishurov V.S. *Osnovi preobrazovatelnoy* tehniki [Converter technology fundamentals]. Tomsk, TUSUR, 2015, 197 p. (in Russ.).

Aleksey V. Frolov
Candidate of Science in Engineering, Assistant professor,
Department of Industrial Electronics,
Komsomolsk-na-Amure State University
27, Lenin st., Komsomolsk-on-Amur, Russia, 681013
ORCID: 0000-0002-9406-1095
Phone: +7 (421-7) 24-11-92
Email: Afrolov.kms@mail.ru

Nadezhda Y. Grunina
Student,
Department of Industrial Electronics,
Komsomolsk-na-Amure State University
27, Lenin st., Komsomolsk-on-Amur, Russia, 681013
Phone: +7 (421-7) 24-11-92
Email: Uheybyf1999uheybyf1999@gmail.com

Требования к подготовке рукописей статей,

представляемых для публикации в журнале
«Доклады Томского государственного университета систем управления и радиоэлектроники»

1. Электронный вариант статьи должен быть представлен в виде файла, названного по-русски фамилией первого автора, на дискете или диске в формате Word 2003–2016. Предпочтительнее представить его по электронной почте.

2. Оригинал на бумажном носителе должен полностью соответствовать электронному варианту.

3. Статья должна иметь (в порядке следования): УДК; И.О. Фамилии авторов; заглавие; аннотация (не реферат); ключевые слова; основной текст статьи; список библиографий под подзаголовком «Литература»; сведения об авторах; далее на английском языке: Фамилии авторов И.О., заглавие статьи, аннотацию, ключевые слова. Сведения об авторах включают в себя фамилию, имя, отчество, ученую степень, ученое звание, должность, место работы, телефон, электронный адрес.

4. Текст статьи должен быть размещен в две колонки без принудительных переносов через один интервал шрифтом Times New Roman 10 кегля на одной стороне листа белой писчей бумаги формата А4, без помарок и вставок. Для облегчения форматирования прилагается **шаблон статьи**, который размещен на сайте: **journal.tusur.ru.** Размер статьи со всеми атрибутами должен быть, как правило, не более пяти страниц.

5. Одни и те же символы в тексте, формулах, таблицах и рисунках должны быть единообразными по написанию. Русские буквы и греческие символы набираются прямым шрифтом, а переменные, обозначенные латинскими – курсивом, кроме слов, их сокращений, имен функций, программ, фирм и химических формул.

6. Формулы должны быть набраны в формульном редакторе (MathType) программы Word. Русские буквы, греческие символы, математические знаки (+, –, ×, ∈, =, скобки, …) и цифры всегда набираются прямым не жирным шрифтом, а переменные (и кривые на графиках), обозначенные латинскими буквами или цифрами – курсивом, кроме англ. слов, их сокращений, имен функций, программ, фирм и химических формул (const, input; $\sin x(t_1)$; U_{in}; $I_{вх}$; T_z; β_2; H_2O, Adobe Acrobat, Cisco и т.д.); векторные величины – жирным, прямо (не курсив) – $\mathbf{A}_1$, $\mathbf{M}(f)$, $\boldsymbol{\beta}_x$. Шаблоны для набора формул необходимо взять на сайте из шаблона статьи.

7. Все употребляемые обозначения и сокращения должны быть пояснены.

8. Единицы измерения физических величин должны соответствовать Международной системе единиц (СИ) и написаны по-русски через пробел (*x*, ГГц; 20 ГГц; *T*, град; 7 °С). Десятичные числа пишутся через запятую (не точку).

9. Таблицы и рисунки должны иметь тематические заголовки (не повторяющие фразы-ссылки на них в тексте). (Рис. 1. Название рисунка; Таблица 1. Название таблицы). Большие блоки расшифровки условных обозначений лучше приводить в тексте. Подписи и надписи на рис. – Times New Roman, 9 пт (после масштабирования), не жирным, не курсивом, переменные – также, как и в тексте. На все рисунки и таблицы должны быть ссылки в тексте (… на рис. 3, … в табл. 2).

10. Рисунки и фотографии должны быть **черно-белыми**, четкими, контрастными, аккуратными, сгруппированными. Графики – не жирно, сетка – четко. Единицы измерения – на русском. Десятичная запятая (не точка). Рисунки могут быть выполнены в программах CorelDraw, Illustrator, Word, Visio и должны давать возможность внесения исправлений.

11. Иллюстрации, должны быть разрешением не менее 600 dpi. Масштаб изображения – 8 или 16,7 см по ширине (при условии читаемости всех надписей, выполненных шрифтом Times New Roman, после масштабирования – 9 кегль).

12. На все источники, указанные в списке литературы, должны быть ссылки по тексту (нумерация в порядке упоминания, например, [1, 2], [5–7]). Описание источников должно соответствовать ГОСТ 7.1–2003 и ГОСТ Р 7.0.5–2008 и содержать всю необходимую для идентификации источника информацию, а именно: *для непериодических изданий* – фамилию и инициалы автора, полное название работы, место издания, название издательства, год издания, количество страниц; *для периодических изданий* – фамилию, инициалы автора, полное название работы, название журнала, год выпуска, том, номер, номера страниц (см. примеры оформления библиографий).

Бумажный вариант рукописи статьи должен быть подписан авторами и (для сторонних авторов) иметь сопроводительное письмо на бланке организации.

Плата за публикацию рукописей не взимается.

Материальные претензии авторов, связанные с распространением материалов их статей после опубликования, не принимаются.

Авторы несут полную ответственность за содержание статей и за последствия, связанные с их публикацией.

Контактная информация
Адрес: 634050, Томск, пр. Ленина, 40.
Эл. почта: vnmas@tusur.ru. Тел.: +7 (382-2) 51-21-21

9 771818 044708 02007