ISSN 1818-0442
DOI: 10.21293/1818-0442

# ДОКЛАДЫ

## Томского государственного университета систем управления и радиоэлектроники

2023 • Том 26, № 4

Доклады ТУСУР. 2023 • Том 26, № 4

Министерство науки и высшего образования Российской Федерации

# ДОКЛАДЫ ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

**2023, том 26, № 4**

Периодический научный журнал

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

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



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

Свидетельство о регистрации СМИ выдано Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия: ПИ № ФС 77-19130

Учредитель: Томский государственный университет систем управления и радиоэлектроники

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

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

Подписано в печать 25.12.2023. Выход в свет 20.02.2024. Формат 60×84 1/8. Печ. л. 7. Тираж 500. Заказ 2. Цена 316 руб.

## Editorial board

**Содержание**

## ЭЛЕКТРОНИКА, РАДИОТЕХНИКА И СВЯЗЬ



## УПРАВЛЕНИЕ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА



## ЭЛЕКТОТЕХНИКА

## Contents

### ELECTRONICS, RADIO ENGINEERING AND COMMUNICATIONS



### CONTROL, COMPUTER SCIENCE AND INFORMATICS



### ELECTRICAL ENGINEERING

# ЭЛЕКТРОНИКА,
# РАДИОТЕХНИКА И СВЯЗЬ

УДК 621.396.41

**П.С. Тяпкин, Н.А. Важенин, А.П. Плохих**

# Анализ эффективности использования методов слепого разделения сигналов для борьбы с помеховым излучением электрических ракетных двигателей в системах космической связи

Рассмотрены вопросы применения алгоритмов слепого разделения сигналов в задачах повышения помехоустойчивости канала спутниковой связи с восьмипозиционной фазовой манипуляцией к воздействию помех, вызванных работой стационарных плазменных двигателей (СПД), которые являются одними из разновидностей электрических ракетных двигателей (ЭРД) [1]. В рамках исследования была разработана имитационная модель канала связи с разнесенным приемом на две антенны. При моделировании в качестве помех в канале связи были рассмотрены импульсные шумоподобные сигналы, формируемые в результате работы СПД. Используемый в исследовании алгоритм слепого разделения сигналов nc-FastICA основан на методе анализа независимых компонент. Результаты моделирования свидетельствуют о возможности эффективного использования алгоритмов слепого разделения сигналов для борьбы с помехами СПД. Применение рассмотренных в работе алгоритмов позволяет достичь выигрыша по вероятности битовой ошибки на два порядка и более. Так, был рассмотрен один из наихудших случаев приема сигнала: выигрыш от применения алгоритма nc-FastICA достигается при величинах битового отношения сигнал/шум более 5 дБ при значениях отношения помеха/сигнал в канале приёма информационного сигнала 10 дБ и в канале приема помехи от СПД 30 дБ.

**Ключевые слова:** слепое разделение сигналов, анализ независимых компонент, повышение помехоустойчивости систем связи, дальняя космическая связь, ЭРД.
**DOI:** 10.21293/1818-0442-2023-26-4-7-12

Использование электрических ракетных двигателей (ЭРД) для космических приложений в настоящее время быстро расширяется. В частности, стационарные плазменные двигатели (СПД) начинают широко применяться в задачах освоения космического пространства [1–4]. Проведенные исследования [1, 5] показали, что СПД являются источниками собственного электромагнитного излучения в полосе от сотен мегагерц до десятков гигагерц. Наиболее актуальной является задача борьбы с влиянием данного типа излучения в программах освоения дальнего космоса, когда уровень сигнала в месте приема на борту космического аппарата крайне мал. Было предложено применять методы слепого разделения сигналов для повышения помехоустойчивости спутниковых каналов связи при воздействии импульсных помех от СПД.

Для более точного анализа эффективности применения методов слепого разделения сигналов (СРС) для борьбы с помеховым излучением СПД представляет интерес использование при моделировании для описания помехи реализаций такого излучения, полученных экспериментально при изучении спектрально-временных характеристик излучения СПД [1].

**Методы слепого разделения сигналов в космической связи**

Под методами слепого разделения сигналов понимаются такие алгоритмы, задача которых заключается в разделении всех $N$ исходных сигналов $\boldsymbol{x}(t)$ из входных наблюдаемых сигналов (смесей) $\boldsymbol{y}(t)$, причем сами исходные сигналы и модель их смешивания $\mathbf{H}$ считаются неизвестными на приемной стороне. Под наблюдаемыми сигналами (смесями) в терминологии слепого разделения сигналов понимают несколько сигналов, сложенных между собой с разными весовыми коэффициентами.

Применительно к дискретным системам математически задача слепого разделения сигналов может быть описана следующим матричным выражением:

$$\mathbf{y} = \mathbf{H} \cdot \mathbf{x} + \mathbf{n}, \qquad (1)$$

где $\mathbf{y}$ – матрица наблюдаемых смесей размерностью $M \times T$, $\mathbf{x}$ – матрица исходных сигналов размерностью $N \times T$, $\mathbf{H}$ – матрица смешивания, $\mathbf{n}$ – матрица шумов, $N$ – количество исходных сигналов, $M$ – количество наблюдаемых смесей, $T$ – длина реализаций сигналов и шумов.

Задачей методов слепого разделения сигналов является поиск такой матрицы разделения $\mathbf{W} = \mathbf{H}^{-1}$, что

$$\mathbf{x} = \mathbf{W}\mathbf{y}. \qquad (2)$$

В рамках рассматриваемой задачи смеси включают в себя информационный сигнал ФМн-8, импульсную помеху от СПД и тепловой шум.

Наиболее предпочтительной и часто применяемой технологией слепого разделения сигналов является метод анализа независимых компонент (АНК), который основан на статистической независимости исходных сигналов.

В практических приложениях при использовании метода АНК для эффективного и точного разделения исходных сигналов требуется выполнение трёх допущений [6–8].

1. Исходные сигналы должны быть взаимно статистически независимыми. Или в статистическом математическом описании

$$w(S) = \prod_{m=1}^{M} w_m(s_m), \qquad (3)$$

где $w()$ – закон распределения соответствующего процесса.

2. Компоненты независимых источников (сигналов) имеют негауссовый закон распределения вероятностей, т.е. исходные сигналы имеют статистики более высокого порядка отличные от нуля, например, эксцесс или кумулянт четвёртого порядка. Из этого предположения следует, что алгоритмы слепого разделения сигналов на базе метода АНК не способны разделять смеси мультигауссовских сигналов.

3. Количество наблюдаемых сигналов должно быть таким же или более, чем количество исходных сигналов.

Алгоритмами слепого разделения сигналов не осуществляются идентификация и поиск полезного сигнала и помехи в принятых смесях. Эта задача должна осуществляться последующими каскадами приемника.

В данной работе для решения задачи слепого разделения сигналов из принятых смесей был рассмотрен алгоритм non-circle complex FastICA (nc-FastICA) [11, 12], основанный на методе АНК. Выбор данного алгоритма в имитационной модели основан на популярности алгоритма FastICA в исследовательских задачах, благодаря его высокой (среди других рассмотренных алгоритмов) точности разделения сигналов, а также тем, что nc-FastICA способен осуществлять обработку комплексных сигналов в отличие от FastICA, который работает только с вещественными данными.

**Имитационная модель канала связи**

Для исследования эффективности применения алгоритма слепого разделения сигналов nc-FastICA для борьбы с импульсными шумовыми помехами от СПД была разработана имитационная модель канала связи с восьмипозиционной фазовой манипуляцией (ФМн-8) и разнесенным приемом на две антенны.

Комплексный вектор смесей на входе приемника, состоящих из сигнала ФМн-8, импульсной помехи и тепловых шумов, может быть представлен как

$$\dot{\mathbf{S}}_{\text{BX}i} = a_{\text{C}i} \cdot \dot{\mathbf{S}}_C + a_{\text{П}i} \cdot \dot{\mathbf{S}}_{\text{П}} + \dot{\mathbf{n}}_i, \qquad (4)$$

где $\dot{\mathbf{S}}_{\text{BX}i}$ – вектор входных смесей на $i$-м входе приемника, $\dot{\mathbf{S}}_{\text{C}}$ – вектор отсчетов полезного сигнала ФМн-8, $\dot{\mathbf{S}}_{\text{П}}$ – вектор отсчетов импульсной помехи от ЭРД, $a_{\text{C}i}$ и $a_{\text{П}i}$ – весовые коэффициенты при полезном сигнале и при импульсной помехе соответственно, $\dot{\mathbf{n}}_i$ – вектор отсчетов тепловых шумов $i$-го приемника, $i = 1, 2$.

На рис. 1 приведена блок-схема разработанной имитационной модели. Данная имитационная модель описывает процессы передачи радиосигналов с заданной модуляцией по каналу связи, в котором кроме тепловых шумов имеется импульсная шумоподобная помеха с заданными спектрально-временными характеристиками.

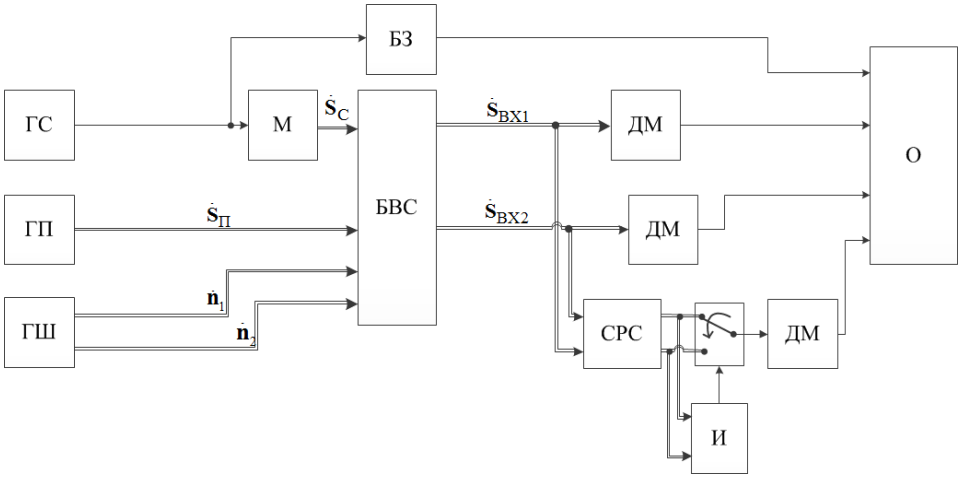



Рис. 1. Блок-схема имитационной модели

Моделирование осуществляется с использованием метода комплексной огибающей. В данном случае в качестве помехи рассматривается радиоизлучение СПД. Для моделирования использовались квадратурные реализации такого излучения, полученные экспериментально.

Функционирование модели происходит следующим образом: передающая часть формирует информационный сигнал и помеху и состоит из генератора информационного сигнала (см. блок «ГС» на рис. 1), модулятора (см. блок «М» на рис. 1). В блоке весового суммирования (см. блок «БВС» на рис. 1) к входному сигналу с задаваемыми весовыми коэффициентами добавляются помехи, сформированные генератором помех (см. блок «ГП» на рис. 1), тепловые шумы, формируемые генератором шума (см. блок «ГШ» на рис. 1), образуя тем самым две смеси. Величины отношения сигнал/шум в двух смесях принимались равными между собой. Затем сформированные смеси демодулируются (см. блоки «ДМ»

на рис. 1). Также смеси поступают на блок слепого разделения сигналов (см. блок «СРС» на рис. 1), на выходе которого формируются разделённые сигнал и импульсная помеха. Задача идентификации полезного сигнала решается с использованием блока идентификации полезного сигнала (см. блок «И» на рис. 1).

Идентификация сигнала осуществляется на основе анализа законов распределения (ЗР) разделенных сигналов и сравнения их с ЗР, характерным для фазоманипулированных сигналов. Блок идентификации устанавливает положение переключателя так, чтобы на блок демодулятора после переключателя поступал обнаруженный полезный сигнал с выхода блока слепого разделения сигналов.

Блок оценки вероятности битовой ошибки (см. блок «О» на рис. 1) производит сравнение задержанного блоком задержки (см. блок «БЗ» на рис. 1) исходного информационного сигнала с двумя демодулированными принятыми смесями без слепого разделения сигналов, а также с демодулированным сигналом на выходе блока слепого разделения сигналов. В результате производится оценка вероятности битовой ошибки.

**Параметры имитационного моделирования**

Для проведения имитационного моделирования были выбраны следующие параметры и допущения:

Битовая скорость передаваемых данных: 500 кбит/с.

Метод модуляции: ФМн-8, помехоустойчивое кодирование отсутствует.

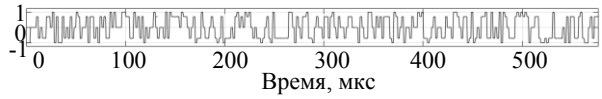
Частота дискретизации принятых смесей составляет 5 МГц.

Для подготовки результирующих графиков по результатам моделирования был рассмотрен пример одного из наихудших случаев приема сигнала от наземной станции: величины битового ОСШ в канале варьировались в диапазоне 0…13 дБ, величины отношения помеха/сигнал в первой смеси составляли 10 дБ, во второй – 30 дБ. Величина средней скважности импульсной помехи от СПД составляла 0,17.

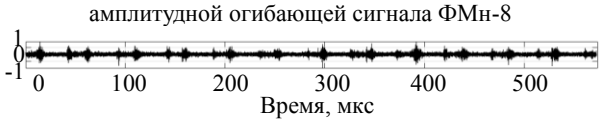
**Результаты имитационного моделирования**

На рис. 2 приведены эпюры сигналов, полученные во время имитационного моделирования. Нормированная синфазная компонента комплексной амплитудной огибающей сигнала ФМн-8 приведена на рис. 2, *а*. Данный сигнал смешивается с импульсной помехой и тепловыми шумами. Реализации синфазных компонент комплексных амплитудных огибающих данных смесей приведены на рис. 2, *б* и *г*. На рис. 2, *в* и *д* отображены битовые ошибки, возникающие в результате сравнения передаваемой последовательности бит и принятых демодулированных смесей сигналов с тепловыми шумами и импульсной помехой. Величины битового отношения сигнал/шум в двух принятых каналах выбраны одинаковыми и составляют 15 дБ.

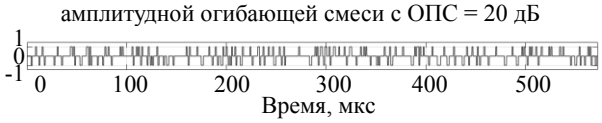
На рис. 3 приведены эпюры, полученные в результате слепого разделения принятых смесей, которые наглядно показывают, что использование СРС существенно сокращает количество битовых ошибок при передаче информации, несмотря на то, что уровень помехи многократно превышает уровень принимаемого (полезного) сигнала. Так, на рис. 3, *а* и *б* приведены синфазные компоненты комплексной амплитудной огибающей сигнала ФМн-8 (см. рис. 3, *а*) и импульсной помехи (см. рис. 3, *б*), полученные в результате использования алгоритма слепого разделения сигналов nc-FastICA. Видно, что разделенные сигнал и импульсная помеха визуально соответствуют исходным сигналам.



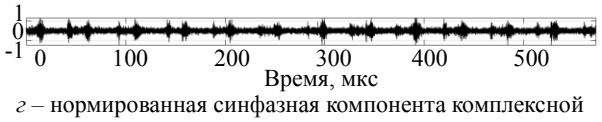

*а* – нормированная синфазная компонента комплексной амплитудной огибающей сигнала ФМн-8




*б* – нормированная синфазная компонента комплексной амплитудной огибающей смеси с ОПС = 20 дБ



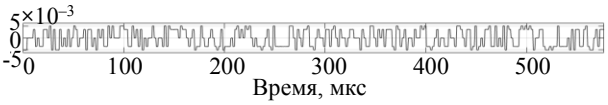

*в* – битовые ошибки, полученные в результате демодуляции принятой смеси (ОПС = 20 дБ) и сравнения с передаваемой битовой последовательностью



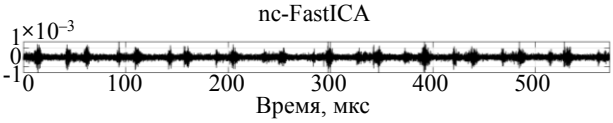

*г* – нормированная синфазная компонента комплексной амплитудной огибающей смеси с ОПС = 10 дБ


*д* – битовые ошибки, полученные в результате демодуляции принятой смеси (ОПС = 10 дБ) и сравнения с передаваемой битовой последовательностью

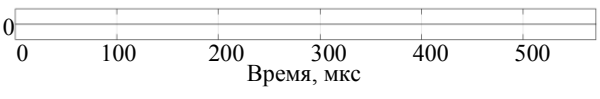
Рис. 2. Примеры эпюр сигналов при моделировании без использования СРС




*а* – синфазная компонента комплексной амплитудной огибающей сигнала ФМн-8 на выходе блока алгоритма nc-FastICA




*б* – синфазная компонента комплексной амплитудной огибающей помехового излучения от СПД на выходе блока алгоритма nc-FastICA




*в* – битовые ошибки, полученные в результате демодуляции разделенного из смесей сигнала ФМн-8 и сравнения с передаваемой битовой последовательностью

Рис. 3. Примеры эпюр сигналов при моделировании при использовании СРС

Это же подтверждает отсутствие битовых ошибок при демодуляции разделенного сигнала ФМн-8

на рис. 3, *в*. Следовательно, для данных характеристик и параметров имитационной модели алгоритм слепого разделения сигналов nc-FastICA позволяет устранять битовые ошибки, связанные с воздействием импульсных помех от ЭРД даже при больших величинах ОПС.

В результате моделирования были получены серии графиков зависимости вероятности битовой ошибки от величин битового отношения сигнал/шум при разных значениях величины помеха/сигнал в канале и средней скважности импульсной помехи. Для вероятности $1 \cdot 10^{-3}$ точность оценки битовой ошибки на основании проведенного моделирования составила 15% с доверительной вероятностью 0,9. Пример полученных результатов приведён на рис. 4.

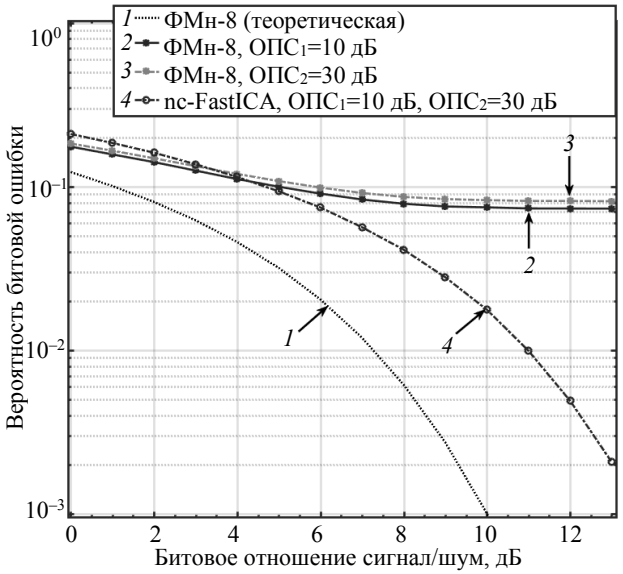



Рис. 4. График зависимости вероятности битовой ошибки от величины битового отношения сигнал/шум

Результаты моделирования, приведенные на рис. 4, были получены при средней скважности импульсной помехи $T_{\text{помехи}}$, равной 0,17.

Из рисунка видно, что экспериментальная кривая вероятности битовой ошибки (см. рис. 4, кривая *4*), соответствующая демодуляции сигнала ФМн-8 после слепого разделения, примерно на 4 дБ отстоит от теоретической кривой (см. рис. 4, кривая *1*). Но, в отличие от кривых, полученных в результате демодуляции принятых смесей без слепой обработки, с увеличением величины битового отношения сигнал/шум от 5 дБ и выше, данная кривая имеет убывающий характер. Кривые вероятностей битовой ошибки при демодуляции принятых смесей (см. рис. 3, кривые *2* и *3*) с увеличением битового отношения сигнал/шум перестают убывать, останавливаясь на значениях $7{,}3 \cdot 10^{-2}$ (ОПС = 10 дБ) и $8{,}14 \cdot 10^{-2}$ (ОПС = 30 дБ).

По полученным кривым можно определить значение энергетического выигрыша от применения алгоритма слепого разделения сигналов nc-FastICA: для этого при разных значениях вероятности битовой ошибки определим соответствующие им значения битового отношения сигнал/шум для случаев без слепого разделения сигналов и с применением алгоритма СРС.

Из рис. 4 определим, что до значения вероятности битовой ошибки $1{,}08 \cdot 10^{-1}$ в первом канале приема и $1{,}27 \cdot 10^{-1}$ во втором канале наблюдается энергетический проигрыш до 1 дБ. При вероятности битовой ошибки $8{,}36 \cdot 10^{-2}$ энергетический выигрыш относительно второго канала приема составляет примерно 2 дБ. Подобная величина энергетического выигрыша относительно первого канала приема достигается при вероятности битовой ошибки, равной $8{,}11 \cdot 10^{-2}$. При значениях вероятности битовой ошибки менее $7{,}3 \cdot 10^{-2}$ в первом канале и менее $8{,}14 \cdot 10^{-2}$ во втором канале становится невозможным определить величину энергетического выигрыша: кривая резко устремляется в бесконечность.

Таким образом, было принято решение определять величину выигрыша от применения алгоритмов слепого разделения сигналов по разнице вероятностей битовых ошибок при одинаковых значениях битового отношения сигнал/шум. Обозначим данную разницу вероятностей битовых ошибок как выигрыш по вероятности битовой ошибки. График зависимости выигрыша по вероятности битовой ошибки (в разах) от величины битового отношения сигнал/шум приведен на рис. 5.

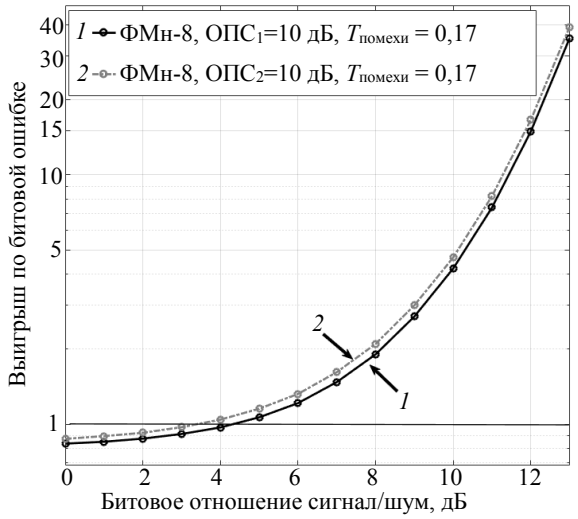



Рис. 5. График зависимости выигрыша по битовой ошибке от величин битового отношения сигнал/шум при применении алгоритма nc-FastICA

Из этого графика наглядно видно на примере алгоритма nc-FastICA, насколько эффективно могут применяться алгоритмы слепого разделения сигналов для повышения помехоустойчивости в каналах связи с импульсными помехами от СПД.

Так, например, при применении алгоритма nc-FastICA в канале связи с ФМн-8 и величиной битового отношения сигнал/шум равной 12 дБ, можно добиться вероятности битовой ошибки, равной

$4{,}93\cdot10^{-3}$, в то время как без слепой обработки при той же величине битового отношения сигнал/шум вероятность битовой ошибки составит $7{,}34\cdot10^{-2}$ при демодуляции смеси с отношением помеха-сигнал равным 10 дБ и $8{,}17\cdot10^{-2}$, с отношением помеха/сигнал 30 дБ соответственно.

**Заключение**

В работе оценена эффективность использования алгоритмов слепого разделения для каналов связи с фазовой манипуляцией и квазипериодической шумоподобной импульсной помехой от стационарных плазменных двигателей. На основе полученных результатов можно сделать вывод, что применение алгоритма nc-FastICA позволяет существенно повысить помехоустойчивость каналов связи с ФМн-8 при воздействии импульсных помех от СПД. Показано, что при приёме сигнала ФМн-8 с импульсной помехой от СПД со средней скважностью 0,17 и отношениями помеха/сигнал 10 дБ в первом канале и 30 дБ во втором, при величине битового отношения сигнал/шум, равного 13 дБ, вероятность битовой ошибки равна $2{,}08\cdot10^{-3}$, что примерно в 35 раз ниже, чем в случае приема этих же смесей без слепой обработки.

Исследование выполнено при поддержке гранта Российского научного фонда № 23-19-00515, https://rscf.ru/project/23-19-00515.

*Литература*

1. Электрические ракетные двигатели космических аппаратов и их влияние на радиосистемы космической связи / Н.А. Важенин, В.А. Обухов, А.П. Плохих, Г.А. Попов. – М.: ФИЗМАТЛИТ, 2013. – 432 с.

2. The Technological and Commercial Expansion of Electric Propulsion in the Past 24 Years. / D. Lev, R. Myers, K. Lemmer, J. Kolbeck, M. Keidar, H. Koizumi, H. Liang, D. Yu, T. Schönherr, J. Gonzalez et al. // Proceedings of the 35th International Electric Propulsion Conference, Atlanta, GA, USA, 8–12 October 2017 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/326925975_The_Technological_and_Commercial_Expansion_of_Electric_ Propulsion_in_the_Past_24_Years, свободный (дата обращения: 18.11.2023).

3. Koppel C. The Smart-1 Electric Propulsion Subsystem / C. Koppel, D. Estublier // Proceedings of the 39th AIAA/ASME/SAE/ASEE Joint Propulsion Conference and Exhibit, Huntsville, AL, USA, 20–23 July 2003 [Электронный ресурс]. – Режим доступа: https://sci.esa.int/documents/34677/36590/1567255180622-AIAA2004-3435-koppel-smart09.pdf, свободный (дата обращения: 18.11.2023).

4. Development of the Psyche Mission for NASA's Discovery Program. / D.Y. Oh, S. Collins, D. Goebel, B. Hart, G. Lantoine, S. Snyder, G. Whiffen, L. Elkins-Tanton, P. Lord, Z. Pirkl et al. // Proceedings of the 35th International Electric Propulsion Conference, Atlanta, GA, USA, 8–12 October 2017. Aerospace 2020, 7, 120 26 of 30 [Электронный ресурс]. – Режим доступа: http://electricrocket.org/2019/192.pdf, свободный (дата обращения: 18.11.2023).

5. Плохих А.П. Анализ влияния электромагнитного излучения стационарных плазменных двигателей на помехоустойчивость канала связи «земля – космический аппарат» / А.П. Плохих, Н.А. Важенин, Г.А. Попов // Космические исследования. – 2019. – Т. 57, № 5. – С. 339–346.

6. Naik G.R. Blind Source Separation: Advances in Theory, Algorithms and Applications / G.R. Naik, W. Wang, eds. // Signals and Communication Technology. Blind Source Separation. – Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. – 551 p.

7. Yu X. Blind source separation: theory and applications. / X. Yu, D. Hu, J. Xu. – John Wiley & Sons, Singapore Pte. Ltd., 2014. – 366 p.

8. Либеровский Н.Ю. Математическое моделирование слепого разделения двух вещественных сигналов с использованием кумулянтов четвертого порядка / Н.Ю. Либеровский, Д.С. Чиров, В.С. Припутин // Вестник ЮУрГУ ММП. Сер.: Математическое моделирование и программирование. – 2020. – Т. 13, № 2. – С. 43–53.

9. Belouchrani A. A blind source separation technique using second-order statistics / A. Belouchrani, K. Abed-Meraim, J.F. Cardoso, E. Moulines // IEEE Transactions on Signal Processing. – 1997. – Vol. 45, No. 2. – P. 434–444.

10. Sahonero-Alvarez G. A Comparison of SOBI, FastICA, JADE and Infomax Algorithms / G. Sahonero-Alvarez, H. Calderon // Proceedings of the 8th international multiconference on complexity, informatics and cybernetics. – 2017. – P. 17–22.

11. Novey M. On Extending the Complex FastICA Algorithm to Noncircular Sources / M. Novey, T. Adali // IEEE Transactions on Signal Processing. – 2008. – Vol. 56, No. 5. – P. 2148–2154.

12. Xie G. An Improved Complex-valued FastICA Algorithm for Jamming Signals Sorting in Beidou Navigation Satellite System / G. Xie, H. Tang, R. Xue //2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP). – Shanghai, China: IEEE, 2020. – P. 20–25.

---

**Тяпкин Павел Станиславович**
Аспирант каф. 408 «Инфокоммуникации»
Московского авиационного института (МАИ)
Волоколамское шоссе, д. 4, г. Москва, Россия, 125993
Тел.: +7-999-969-79-87
Эл. почта: tjapkinp@yandex.ru

**Важенин Николай Афанасьевич**
Д-р техн. наук, проф. каф. 408 «Инфокоммуникации» МАИ
Волоколамское шоссе, д. 4, г. Москва, Россия, 125993
Тел.: +7 (499) 158-40-82
Эл. почта: VazheninNA@mai.ru

**Плохих Андрей Павлович**
Д-р техн. наук, проф. каф. 408 «Инфокоммуникации» МАИ
Волоколамское шоссе, д. 4, г. Москва, Россия, 125993
Тел.: +7 (499) 158-00-20
Эл. почта: plokhikh2001@mail.ru

Tyapkin P.S., Vazhenin N.A., Plokhikh A.P.

**Efficiency analysis for the application of blind signal separation methods to counter interference radiation from electric propulsions in space communication systems**

The article considers the use of blind signal separation algorithms to improve interference immunity of the satellite communication channel with octal phase shift keying as applied to the interference, that is caused by the operation of stationary plasma thrusters (SPT), and represents one of the varieties of

electric propulsion [1]. During the study, a simulation model of communication channel with an additional channel for receiving interference from SPT was developed. While modeling, some pulsed noise-like signals, formed as a result of SPT operation, were considered as interference in the communication channel. The blind signal separation algorithm nc-FastICA used in the study is based on the method of independent component analysis. The main task of the modeling was to verify the applicability of blind signal separation methods to counter the interference from SPT in the communication channel. The simulation results proved the possibility of efficient use of blind signal separation algorithms to counter SPT interference. Application of the considered algorithm allows achieving a gain in bit error rate by two and more orders of magnitude. Thus, one of the worst cases of signal reception was considered: the gain from the use of the nc-FastICA algorithm is achieved when the bit signal-to-noise ratio is more than 10 dB and when the interference-to-signal ratio in the signal-receiving channel is 10 dB and in the interference receiving channel from the SPT is 30 dB.

**Keywords:** blind signal separation, independent component analysis, improvement of communication system interference immunity, deep space communication, EP.
**DOI:** 10.21293/1818-0442-2023-26-4-7-12

*References*

1. Vazhenin N.A., Obuhov V.A., Plokhikh A.P., Popov G.A. *Elektricheskie raketnye dvigateli kosmicheskih apparatov i ih vliyanie na radiosistemy kosmicheskoj svyazi* [Electric rocket engines of spacecraft and their influence on space communication radio systems]. M., FIZMATLIT, 2013, 432 p. (in Russ.).

2. Lev D., Myers R., Lemmer K., Kolbeck J., Keidar M., Koizumi H., Liang H., Yu D., Schönherr T., Gonzalez J. et al. The Technological and Commercial Expansion of Electric Propulsion in the Past 24 Years. *Proceedings of the 35th International Electric Propulsion Conference*, Atlanta, GA, USA, 8–12 October 2017. Available at: https://www.researchgate.net/publication/326925975_The_Technological_and_Commercial_Expansion_of_Electric_Propulsion_in_the_Past_24_Years/, free (Accessed: November 18, 2023).

3. Koppel C., Estublier D. The Smart-1 Electric Propulsion Subsystem. *Proceedings of the 39th AIAA/ASME/SAE/ASEE Joint Propulsion Conference and Exhibit*, Huntsville, AL, USA, 20–23 July 2003. Available at: https://sci.esa.int/documents/34677/36590/1567255180622-AIAA2004-3435-koppel-smart09.pdf, free (Accessed: November 18, 2023).

4. Oh D.Y., Collins S., Goebel D., Hart B., Lantoine G., Snyder S., Whiffen G., Elkins-Tanton L., Lord P., Pirkl Z. et al. Development of the Psyche Mission for NASA's Discovery Program. *Proceedings of the 35th International Electric Propulsion Conference*, Atlanta, GA, USA, 8–12 October 2017. Aerospace 2020, 7, 120 26 of 30 Available at: http://electricrocket.org/2019/192.pdf, free (Accessed: November 18, 2023).

5. Plokhikh AP., Vazhenin N.A., Popov G.A. Analysis of the influence of electromagnetic emission from stationary plasma thrusters on the interference immunity of the Earth-spacecraft communication channel. *Cosmic Research*. 2019, vol. 57, no. 5, pp. 339–346 (in Russ.).

6. Naik G.R., Wang W., eds. Blind Source Separation: Advances in Theory, Algorithms and Applications: Signals and Communication Technology. Blind Source Separation. Berlin, Heidelberg*: Springer Berlin Heidelberg*, 2014, 551 p.

7. Yu X., Hu D., Xu J. Blind source separation: theory and applications. Blind source separation. *Singapore: John Wiley & Sons Singapore Pte. Ltd*, 2014, 366 p.

8. Liberovskiy N.Y., Chirov D.S., Priputin V.S., Development of the two real signals blind separation method using fourth-order cumulants. *Bulletin of the South Ural State University. Series "Mathematical Modelling, Programming & Computer Software" (Bulletin SUSU MMCS)*, 2020, vol. 13, no. 2, pp. 43–53 (in Russ.).

9. Belouchrani A., Abed-Meraim K., Cardoso J.-F., Moulines E. A blind source separation technique using second-order statistics. *IEEE Transactions on Signal Processing*, 1997, vol. 45, no. 2, pp. 434–444.

10. Sahonero-Alvarez G., Calderon H. A Comparison of SOBI, FastICA, JADE and Infomax Algorithms. *Proceedings of the 8th International Multi-conference on Complexity, Informatics and Cybernetics*, 2017.

11. Novey M., Adali T. On Extending the Complex FastICA Algorithm to Noncircular Sources. *IEEE Transactions on Signal Processing*, 2008, vol. 56, no. 5, pp. 2148–2154.

12. Xie G., Tang H., Xue R. An Improved Complex-valued FastICA Algorithm for Jamming Signals Sorting in Beidou Navigation Satellite System. *2020- IEEE 3rd International Conference on Information Communication and Signal Processing* (*ICICSP*). Shanghai, China: IEEE, 2020, pp. 20–25.

**Pavel S. Tyapkin**
Postgraduate student, Department 408 «Infocommunications»
Moscow Aviation Institute (MAI)
4, Volokolamskoe shosse, Moscow, Russia, 125993
Phone: +7-999-969-79-87
Email: tjapkinp@yandex.ru

**Nikolay A. Vazhenin**
Doctor of Science in Engineering, Professor, Department 408 «Infocommunications» MAI
4, Volokolamskoe shosse, Moscow, Russia, 125993
Phone: +7 (499) 158-40-82
Email: VazheninNA@mai.ru

**Andrey P. Plokhikh**
Doctor of Science in Engineering, Professor,
Department 408 «Infocommunications» MAI
4, Volokolamskoe shosse, Moscow, Russia, 125993
Phone: +7 (499) 158-00-20
Email: plokhikh2001@mail.ru

УДК 537.874.4

**А.Е. Байкалова, Э.В. Семенов**

# Экспериментальное исследование нелинейной эффективной площади рассеяния объектов в видеоимпульсном режиме

Впервые (судя по литературным источникам) представлена количественная информация о нелинейных рассеивающих свойствах объектов зондирования при воздействии сигналов, близких к видеоимпульсным, что позволит предъявлять требования к передатчикам и приемникам нелинейных видеоимпульсных локаторов. Для проведения исследований разработан прототип нелинейного видеоимпульсного локатора на лабораторных приборах. В апертуре антенны он создает импульсное поле интенсивностью 35 Вт/м$^2$ с длительностью фронта 0,23 нс. В качестве объектов зондирования используются кольца диаметром 6 см из медного провода поперечным сечением 4 мм$^2$ (короткозамкнутое кольцо в качестве линейного объекта и кольцо, в разрыв которого включен диод HSMS-8101 в качестве нелинейного объекта). Нелинейная эффективная площадь рассеяния (НЭПР) нелинейного объекта составила 0,041 мм$^2$, что укладывается в типичный диапазон НЭПР объектов для обычной (гармонической) нелинейной локации.

**Ключевые слова:** нелинейность, локатор, эффективная площадь рассеяния, сверхширокополосное зондирование.
**DOI:** 10.21293/1818-0442-2023-26-4-13-18

Применение сверхширокополосных видеоимпульсных сигналов потенциально позволяет увеличить дальность, разрешающую способность по дальности и проникающую способность нелинейной локации [1–3]. При использовании коротких видеоимпульсных сигналов (в сравнении с радиоимпульсами большой длительности) увеличивается пиковая мощность зондирующего сигнала при фиксированной средней мощности. Это позволяет рассчитывать на увеличение уровня нелинейного отклика, поскольку при более мощных воздействиях объект отказывается в режиме более сильной нелинейности. Кроме того, увеличивается проникающая способность за счет наличия низкочастотной части спектра.

В работах [2, 4] рассматриваются установки, которые могут послужить прототипами для создания видеоимпульсных нелинейных локаторов. Однако в этих статьях протестирована их работа на относительно крупных объектах с фронтальным поперечным сечением около 0,05 м$^2$. Поэтому актуальной остается повышение чувствительности этих установок по отношению к нелинейным объектам.

В настоящей статье рассмотрен прототип нелинейного видеоимпульсного локатора с улучшенной чувствительностью и показана возможность обнаружения с его помощью малоразмерных нелинейных объектов.

Обнаружительная способность систем локации определяется рассеивающими свойствами объектов. Традиционным параметром, описывающим рассеивающие свойства объекта в линейной локации, служит эффективная площадь рассеяния (ЭПР), являющаяся отношением полной рассеянной объектом мощности к интенсивности зондирующего поля [5]. Для объектов с нелинейным откликом можно определить аналогичный параметр, называемый нелинейной эффективной поверхностью рассеяния (НЭПР), определяемый как отношение мощности нелинейного отклика объекта к интенсивности зондирующего поля [6–10].

Как правило, в существующих работах по измерению НЭПР экспериментальные исследования проводятся в гармоническом режиме, с определенными шириной спектра и длительностью сигнала [6–10]. Для видеоимпульсного режима, по нашим сведениям, таких публикаций нет, поэтому в настоящей статье представлена методика расчета нелинейной эффективной площади рассеяния видеоимпульсных сигналов исследуемыми объектами.

**Прототип нелинейного видеоимпульсного локатора**

Структурная схема разработанного нелинейного видеоимпульсного локатора представлена на рис. 1. За основу мы приняли прототип, описанный в [4].

В качестве зондирующих импульсов используются сверхширокополосные сигналы положительной $x_1$ и отрицательной $x_2$ полярности (рис. 2), формируемые двухтактным обострителем импульсов [11].

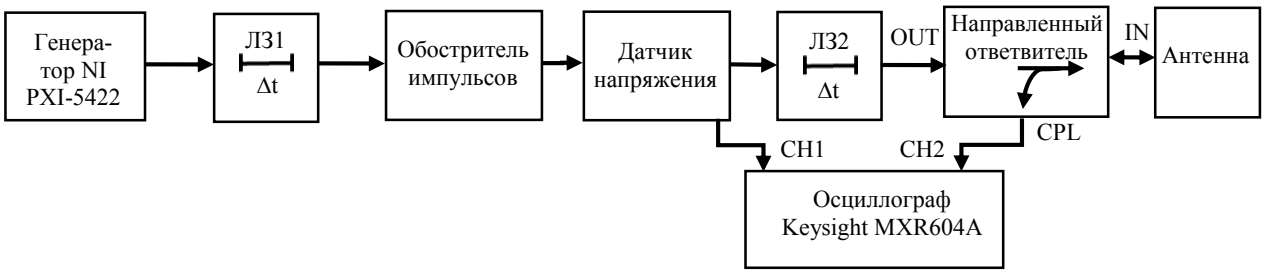



Рис. 1. Структурная схема прототипа нелинейного видеоимпульсного локатора

На его вход подается запускающий сигнал: меандр амплитудой 12 В от генератора National Instruments PXI-5422. Поскольку вход обострителя не является согласованным по волновому сопротивлению, сигнал на него подается через линию задержки Л31 (для уменьшения влияния переотражений во входной цепи). Амплитуда быстрой части фронта выходного сигнала обострителя импульсов составляет 7,2 В. Длительность фронтов сигнала на согласованной нагрузке равна 0,23 нс.

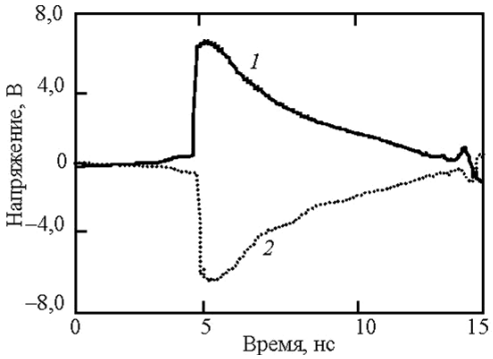



Рис. 2. Зондирующие сигналы $x_1$ (*1*) и $x_2$ (*2*)

В данной работе используется метод определения нелинейности [4], в котором нелинейный отклик объекта $\varepsilon(t)$ отыскивается как взвешенная разность откликов $u_{1,2}$ на зондирующие сигналы $x_{1,2}$ разной полярности:

$$\varepsilon(t) = u_1(t) - u_2(t) * x_1(t) * F^{-1}\{1/F[x_2(t)]\},$$

где $F$ и $F^{-1}$ – прямое и обратное преобразование Фурье соответственно, $*$ – символ свертки.

Интересующие нас объекты содержат *p–n*-переходы, которые дают различные отклики на сигналы разной полярности, что и создает разностный сигнал при обработке откликов (нелинейный отклик). Для учета возможного различия формы зондирующих сигналов требуется регистрировать не только отклики от объектов, но и зондирующие сигналы. Для этого к выходу обострителя импульсов присоединен датчик напряжения, состоящий из резистора сопротивлением 470 Ом, который подключен к проходящему коаксиальному волноводу. Сигнал с выхода датчика напряжения подается на первый канал регистрирующего устройства (осциллографа).

В представленных исследованиях используется однополярный ступенчатый зондирующий сигнал [4], поэтому от антенн возникает достаточно сильное отражение (преимущественно в области нижних частот). Если не предпринять специальных мер, то это отражение попадает в канал регистрации зондирующих сигналов. Для исключения этого эффекта после датчика напряжения включена линия задержки Л32. Она сдвигает отражения от антенны за пределы окна наблюдения.

В качестве антенны использована совмещенная приемопередающая антенна типа «улитка» [12]. Она выполнена из листа латуни и помещена в пластиковый корпус размерами 26×19,5×17,5 см. Комбинированная антенна излучает сигнал в пространство и принимает отраженный сигнал, который регистрируется вторым каналом осциллографа. Отделение отраженной от объекта волны обеспечивает направленный ответвитель Mini-Circuits ZUDC20-183+ [13].

Отраженная от объекта волна регистрируется на выходе CPL направленного ответвителя (см. рис. 1). Использованный направленный ответвитель, по данным производителя [13], вносит ослабление от своего входа IN до выхода CPL, равное 20 дБ. Соответственно, для получения отклика объекта из сигнала, зарегистрированного вторым каналом осциллографа, нужно зарегистрированный сигнал увеличить на 20 дБ. Далее в статье на графиках и в формулах фигурируют уже отклики объекта.

**Исследуемые объекты**

В качестве тестового используется объект с известными параметрами: кольцо диаметром 6 см из медного провода поперечным сечением 4 мм$^2$, в разрыве которого находится диод HSMS-8101 [14] (рис. 3, *а*). По предварительным оценкам, отражение от такого кольца может примерно соответствовать отражению от малоразмерных электронных устройств.

*а* *б*

Рис. 3. Тестовые объекты:
*а* – кольцо с диодом, *б* – короткозамкнутое кольцо

Регистрирующая система локатора обладает собственной нелинейностью, величину которой нужно знать, чтобы по превышении этой величины обнаруживать нелинейные объекты. Для оценки собственной нелинейности приемной системы локатора использован тестовый линейный объект. Он представляет собой короткозамкнутое кольцо с такой же геометрией (см. рис. 3, *б*).

**Радиолокационный отклик от линейного и нелинейного объектов**

Тестовые объекты поочередно располагались на расстоянии 3 см от антенны на ее оптической оси (расстояние, согласно [15], рассчитывалось от антенны до центра объекта). Плоскости колец были перпендикулярны вектору магнитного поля. Далее отклики на импульсы разной полярности регистрировались осциллографом и обрабатывались с использованием калибровки на свободное пространство [4].

Данная калибровка состоит в том, что приемной системой локатора регистрируется сигнал в отсутствие исследуемого объекта. Весь этот сигнал рассматривается как систематическая погрешность и затем вычитается из сигнала, зарегистрированного приемником при наличии объекта зонирования.

На рис. 4 изображены общий отклик (кривая *1*) и нелинейные отклики (кривые *2* и *3*) для объекта, представленного короткозамкнутым кольцом. Здесь и далее под общим откликом объекта понимается его отклик на зондирующий сигнал положительной полярности. Кривая *2* получена при регистрации сигналов стробоскопическим осциллографом Pico Technology 9301-25 [16] (как в [4]), а кривая *3* – с использованием осциллографа реального времени Keysight MXR604A [17]. Можно видеть, что стробоскопический осциллограф имеет значительно большие собственные нелинейные искажения. Причина этого, по нашим оценкам, состоит в систематическом смещении отдельных фрагментов сигнала при установке задержки стробирующего импульса [18]. Поэтому далее регистрация сигналов выполнялась осциллографом Keysight MXR604A.

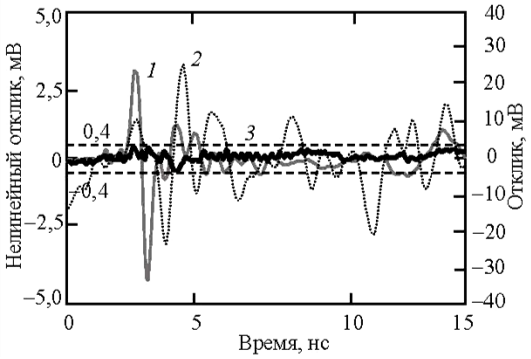



Рис. 4. Общий отклик (*1*) и нелинейные отклики для объекта, представленного короткозамкнутым кольцом: *2* – при регистрации сигналов стробоскопическим осциллографом; *3* – при регистрации осциллографом реального времени

При использовании осциллографа реального времени амплитуда нелинейного отклика, регистрируемого при линейных свойствах исследуемого объекта (собственная нелинейность приемника), не превышает 0,4 мВ (горизонтальные штриховые линии). Это составляет примерно 1,3 % по сравнению с уровнем общего отклика, равного 32 мВ. Эта величина (0,4 мВ) представляет собой порог, определенное превышение которого позволяет идентифицировать исследуемый объект как нелинейный.

На рис. 5 изображены общий (кривая *1*) и нелинейный (кривая *2*) отклики объекта, представленного кольцом с диодом.

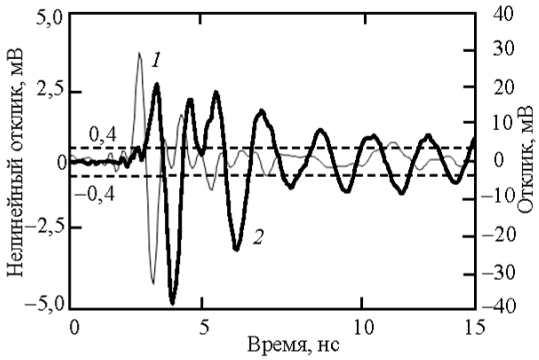



Рис. 5. Общий (*1*) и нелинейный (*2*) отклики для объекта, представленного кольцом с диодом

Можно заметить, что при аналогичном уровне общего отклика регистрируется нелинейный отклик (5,0 мВ), значительно превышающий указанный порог; объект идентифицируется как нелинейный.

**Методика расчета эффективной площади рассеяния**

НЭПР объекта $S$, как и ЭПР в линейной локации, определяется как отношение полной рассеянной объектом мощности $P_{об}$ к интенсивности падающего поля $I_{пад}$:

$$S = P_{об} / I_{пад}. \quad (1)$$

Данные энергетические параметры будут определяться по отношению к пиковым значениям сигналов.

Классически ЭПР объекта определяется в дальней зоне антенны в условиях плоской волны. Однако специфика нелинейных локаторов небольшой мощности не позволяет выполнить это условие: интенсивность поля вдали от антенны будет слишком малой, и объект не будет проявлять нелинейность в достаточной степени. Поэтому в данном случае объект располагается вблизи антенны. Так можно поступить потому, что антенна (рис. 6) включает ТЕМ-рупор, в котором формируется волна, близкая к плоской поперечной. Конечно, в устье рупора (апертура антенны) имеют место краевые эффекты, что обусловливает некоторую методическую погрешность в определении ЭПР.

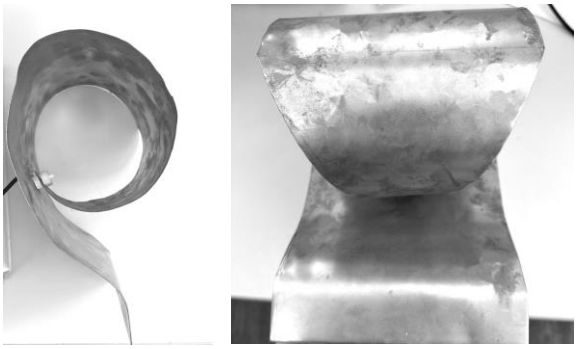


Рис. 6. Общий вид приемопередающей антенны и геометрические размеры рупора

Интенсивность поля в апертуре антенны можно определить как отношение пиковой мощности передатчика $P_{пер}$ к площади устья рупора антенны $S_{ант}$. Мощность передатчика, при этом будет определяться как отношение квадрата максимума генерируемого напряжения, равного 7,2 В, к волновому сопротивлению подводящей линии, равному 50 Ом (1,0 Вт). Тогда интенсивность падающего поля вблизи антенны можно определить по формуле

$$I_{пад} = P_{пер} / S_{ант}. \quad (2)$$

Площадь устья рупора антенны определяется как произведение высоты и ширины рупора антенны (см. рис. 6) и составляет 0,0298 м$^2$. Получаем, что интенсивность падающего поля вблизи антенны, в соответствии с (2), будет составлять 34,8 Вт/м$^2$.

Рассеянная объектом мощность $P_{об}$ при этом будет определяться в момент времени, когда напряжение отклика объекта в приемном тракте $U_{об}$ достигает своего максимума, по следующей формуле:

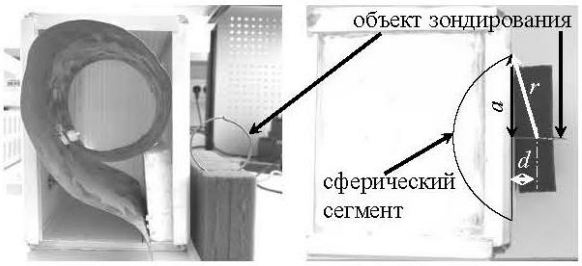
$$P_{об} = k\, U^2_{об} / \rho, \qquad (3)$$

где ρ – волновое сопротивление нагрузки антенны, $k$ – коэффициент, учитывающий, что антенна принимает только часть мощности, рассеянной объектом.

Для отыскания коэффициента $k$ примем, что излучение объекта является изотропным. Будем считать также, что апертура антенны лежит в основании сферического сегмента и площадь этого основания равна апертуре $S_{ант}$. При этом условии радиус основания сферического сегмента равен $a = \sqrt{S_{ант} / \pi}$. Для вышеуказанной площади апертуры получаем $a$ = 97,4 мм. Расстояние $d$ от центра объекта зондирования до апертуры равно 30 мм (рис. 7), откуда находим радиус $r$ сферы, из которой образован сегмент: $r = \sqrt{a^2 + d^2} = 102$ мм. Высота сегмента $h = r - d = 72$ мм. Отсюда по известной формуле находим площадь сферического сегмента $A = 2\pi r h = 0{,}0461$ м$^2$. Отношение полной площади сферы $4\pi r^2$ к площади сферического сегмента $A$ и даст коэффициент $k$:

$$k = 4\pi r^2 / A.$$

В нашем случае $k$ = 2,83.




*а* *б*

Рис. 7. Геометрия эксперимента:
*а* – вид сбоку, *б* – вид сверху

Исходя из экспериментальных графиков, представленных на рис. 5, амплитуды общего и нелинейного откликов объекта составляют 32 и 5,0 мВ соответственно. Таким образом, вычислив по (3) мощность общего и нелинейного откликов и отнеся ее по (1) к интенсивности падающего поля, получим эффективные поверхности рассеяния (ЭПР и НЭПР) тестового объекта. Для кольца, в разрыв которого установлен диод, получаем ЭПР и НЭПР 1,7 и 0,041 мм$^2$ соответственно.

При оценке погрешности полученных результатов мы исходим из того, случайной погрешностью при регистрации сигналов можно пренебречь. Действительно, экстремумы на кривой *3* рис. 4 четко синхронизированы с принимаемым сигналом, т.е. представляют собой систематическую погрешность по отношению к нему. Эти экстремумы обусловлены собственной нелинейностью приемного тракта и, как показано в проведенных экспериментах, не превышают по абсолютной величине 0,4 мВ. Получаем, что в отношении к общему и нелинейному откликам (амплитудой 32 и 5,0 мВ) эта систематическая погрешность составляет 1,3 и 8% соответственно.

Согласно [7], в гармоническом режиме измерения НЭПР большинства малоразмерных объектов составляют и 0,00001…0,1 мм$^2$ (НЭПР) на второй гармонике при $I_{пад}$ = 1 Вт/м$^2$. Мощность сигнала на второй гармонике квадратично зависит от $I_{пад}$, поэтому НЭПР увеличивается пропорционально интенсивности. Для использованной в данном эксперименте интенсивности 34,8 Вт/м$^2$ диапазон НЭПР составит 0,00035…3,5 мм$^2$.

Полученное значение нелинейной эффективной поверхности рассеяния объекта в видеоимпульсном режиме зондирования входит в диапазон НЭПР для обычной (гармонической) локации. Это, с одной стороны, указывает на корректность проведенного эксперимента, с другой – позволяет рассчитывать на перспективность развития нелинейной видеоимпульсной локации. Действительно, если отражательная способность объектов для гармонического и видеоимпульсного сигнала сопоставима, то, переходя к коротким видеоимпульсным воздействиям, мы можем значительно увеличить пиковую мощность сигнала, а следовательно, и дальность обнаружения объектов.

Отметим, что указанный в [7] диапазон НЭПР соответствует объектам с ЭПР 10…1000 см$^2$, что намного больше ЭПР объектов в нашем эксперименте. Несмотря на то, что тестовый объект обладает относительно небольшой площадью рассеяния, нелинейный видеоимпульсный локатор способен обнаружить его и отличить от линейного объекта.

**Заключение**

В данной работе впервые (судя по известным нам литературным источникам) была представлена количественная информация о нелинейных рассеивающих свойствах объектов при зондировании в видеоимпульсном режиме.

В качестве экспериментальной установки использовался прототип нелинейного видеоимпульсного локатора. Такой локатор является первым локатором с совмещенной приемной и передающей антеннами, который способен обнаружить нелинейные объекты в видеоимпульсном режиме.

Удалось обнаружить и идентифицировать по нелинейным свойствам объекты с эффективной площадью рассеяния 1,7 мм$^2$.

Полученные данные позволяют предъявлять требования к передатчику и приемнику нелинейного видеоимпульсного локатора для достижения требуемой дальности обнаружения объектов.

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации (проект № FWRM-2021-0015).

*Литература*

1. Semyonov E.V. Nonlinear scattering of narrowband and ultra-wideband signals at equal peak intensity // 15th International Scientific-Technical Conference on Actual Problems of Electronic Instrument Engineering (APEIE – 2021): proceedings. Novosibirsk, November 19–21, 2021. – P. 295–298.

2. Semyonov E.V. Modeling and Experimental Study of the Nonlinear Baseband Pulse Radar Prototype / E.V. Semyonov, A.V. Fateev, M.A. Nazarov, A.A. Berezin // Radiation and Scattering of Electromagnetic Waves (RSEMW). Divnomorskoe, Russian Federation. – 2023. – P. 428–431.

3. Якубов В.П. Использование сверхширокополосного излучения для диагностики нелинейностей / В.П. Якубов, Д.В. Лосев, А.И. Мальцев // Журнал радиоэлектроники. – 2000. – № 3 [Электронный ресурс]. – Режим доступа: http://jre.cplire.ru/jre/mar00/ 1/text.html, свободный (дата обращения: 25.11.2023).

4. Baikalova A.E. Means and Methods for Decoupling of Receiving and Transmitting Paths of Nonlinear Baseband Pulse Radar / A.E. Baikalova, E. V. Semyonov // Radiation and Scattering of Electromagnetic Waves (RSEMW). – Divnomorskoe, Russia, 2023. – P. 288–291.

5. Ширман Я.Д. Радиоэлектронные системы. Основы теории и построение: справочник / под ред. Я.Д. Ширмана. – М.: ЗАО «Маквис». – 1998. – 825 с.

6. Щербаков Г.Н. Исследование рассеивающих свойств нелинейного биконического отражателя физической модели боеприпаса с электронными устройствами / Г.Н. Щербаков, А.В. Николаев, Р.И. Усманов, Ю.А. Шлыков // Спецтехника и связь. – 2011. – № 1. – С. 33–39.

7. Щербаков Г.Н. К оценке фундаментальных пределов в нелинейной радиолокации / Ю.А. Шлыков, А.В. Николаев, А.В. Бровин // Спецтехника и связь. – 2008. – № 2. – С. 21–25.

8. Gallagher K.A. Harmonic Radar: Theory and Applications to Nonlinear Target Detection, Tracking, Imaging and Classification. The dissertation in electrical engineering. – The Pennsylvania State University, 2015. – 175 p. [Электронный ресурс]. – Режим доступа: https://etda.libraries.psu.edu/files/final_submissions/11380 (дата обращения: 15.12.2023).

9. Fazi C. Design Considerations for Nonlinear Scattering: Report of U.S. Army Research Laboratory No. ARL-TR-5684 / C. Fazi, F. Crowne, M. Ressler. – 2011. – 16 p. [Электронный ресурс]. – Режим доступа: https://www.govinfo.gov/content/pkg/GOVPUB-D101-PURL-gpo14593/pdf/GOVPUB-D101-PURL-gpo14593.pdf, свободный (дата обращения: 15.12.2023).

10. Anderson S.J. Nonlinear Scattering at HF: Prospects for Exploitation in OTH Radar Systems // Turkish Journal of Electrical Engineering and Computer Sciences. – 2010. – Vol. 18, No. 3. – P. 439–456.

11. Березин А.А. Двухтактный обостритель импульсов на диодах с накоплением заряда // СВЧ-техника и телекоммуникационные технологии (КрыМиКо–2022): матер. 32-й Междунар. конф. – Севастополь: Изд-во СевГУ, 2022. – С. 247–248.

12. Андреев Ю.А. Малогабаритные сверхширокополосные антенны для излучения мощных электромагнитных импульсов / Ю.А. Андреев, Ю.И. Буянов, В.И. Кошелев // Журнал радиоэлектроники. – 2015. – № 4 [Электронный ресурс]. – Режим доступа: http://jre.cplire.ru/alt/apr06/1/abstract.html, свободный (дата обращения: 28.11.2023).

13. Направленный ответвитель Mini Circuits ZUDC20-183+ [Электронный ресурс]. – Режим доступа: https://www.minicircuits.com/pdfs/ZUDC20-183+.pdf, свободный (дата обращения: 15.11.2023).

14. Высокочастотный диод Шотки HSMS-8101 [Электронный ресурс]. – Режим доступа: https://pdf1.alldatasheet.com/datasheet-pdf/view/527214/AVAGO/HSMS-8101.html, свободный (дата обращения: 20.11.2023).

15. Ruck G.T. Radar Cross Section Handbook / G.T. Ruck, D.E. Barric, W.D. Stuart, C.K. Krichbaum. – New York, USA: Springer, 1970. – 949 p.

16. Стробоскопические осциллографы USB PicoScope серии 9300 [Электронный ресурс]. – URL: https://www.picotech.com/download/datasheets/picoscope9300-series-sampling-oscilloscopes-data-sheet.pdf (дата обращения: 15.10.2023).

17. Осциллограф Keysight Infinium MXR604A [Электронный ресурс]. – URL: https://akmetron.ru/upload/iblock/fdc/fdcd1e56698db6933ddc19200552a729.pdf (дата обращения: 20.11.2023).

18. Шипилов С.Э. Нелинейные преобразования сигналов в импульсной радиотомографии / С.Э. Шипилов, В.П. Якубов // Известия высших учебных заведений. Физика. – 2020. – Т. 63, № 2. – С. 5–14.

---

**Байкалова Анна Евгеньевна**
Мл. науч. сотр. Института сильноточной электроники (ИСЭ) СО РАН, ассистент каф. радиоэлектроники и систем связи Томского государственного университета систем управления и радиоэлектроники (ТУСУР)
Академический пр-т, 2/3, г. Томск, Россия, 634055
Тел.: +7 (382-2) 49-15-44
Эл. почта: annabajkalova2016@gmail.com

**Семенов Эдуард Валерьевич**
Д-р техн. наук, с.н.с. ИСЭ СО РАН, проф. ТУСУРа
Академический пр-т, 2/3, г. Томск, Россия, 634055
ORCID: 0000-0001-5470-1185
Тел.: +7 (382-2) 49-15-44
Эл. почта: edwardsemyonov@narod.ru

Baikalova A.E., Semyonov E.V.

**Experimental study of object's nonlinear radar cross section in baseband pulse mode**

Quantitative information on the nonlinear scattering properties of probed objects at the impacts with signals close to baseband is presented, that will allow to make the requirements on transmitters and receivers of nonlinear baseband pulse radars. A prototype of a nonlinear baseband pulse radar using laboratory instruments has been developed. In the aperture of the antenna, it creates a pulsed field with an intensity of 35 W/m$^2$ and at a front duration of 0,23 ns. The rings with a diameter of 6 cm made of copper wire with a cross section of 4 mm$^2$ are used as sounding objects (a short-circuited ring as a linear object and a ring with the HSMS-8101 diode in its gap as a nonlinear object). The nonlinear radar cross section (NRCS) of a nonlinear object was 0,041 mm$^2$, that fits into the typical range of NRCS for objects in a conventional (harmonic) nonlinear sounding.

**Keywords:** nonlinearity, radar, radar cross section, ultra-wideband sounding.
**DOI:** 10.21293/1818-0442-2023-26-4-13-18

*References*

1. Semyonov E.V. Nonlinear scattering of narrowband and ultra-wideband signals at equal peak intensity. *Actual Problems of Electronic Instrument Engineering*. Proceedings of 15th International Scientific-Technical Conference. Novosibirsk, November 19–21, 2021, pp. 295–298.

2. Semyonov E.V., Fateev A.V., Nazarov M.A., Berezin A.A. Modeling and Experimental Study of the Nonlinear Baseband Pulse Radar Prototype. *Radiation and Scattering of Electromagnetic Waves*. Proceedings of International IEEE Conference. Divnomorskoe, Russia, 2023, pp. 428–431.

3. Yakubov V.P., Losev D.V., Maltsev A.I. *Ispol'zovanie sverhshirokopolosnogo izluchenija dlja diagnostiki nelinejnostej* [The Use of Ultra-Wideband Radiation for the Diagnosis of Nonlinearities]. Zhurnal radiojelektroniki [*Journal of Radio Electronics*], 2000, no. 3 (in Russ.). Available at: http://jre.cplire.ru/jre/mar00/1/text.html, free (Accessed: November 25, 2023).

4. Baikalova A.E., Semyonov E.V. Means and Methods for Decoupling of Receiving and Transmitting Paths of Nonlinear Baseband Pulse Radar. *Radiation and Scattering of Electromagnetic Waves*. Proceedings of International IEEE Conference. Divnomorskoe, Russia, 2023, pp. 288–291.

5. Shirman J. D. *Radioelektronnye systemy*. *Osnovy teorii i postroenie* [Radioelectronic Systems. Fundamentals of Theory and Construction]. Ed. by J.D. Shirman M.: CJSC «Makvis», 1998. 825 p. (in Russ.).

6. Shcherbakov G.N., Nikolaev A.V., Usmanov R.I., Shlykov Yu.A. *Issledovanie rasseivajushhih svojstv nelinejnogo bikonicheskogo otrazhatelja fizicheskoj modeli boepripasa s jelek-tronnymi ustrojstvami* [Investigation of scattering properties of a nonlinear biconic reflector of a physical model of ammunition with electronic devices]. *Special Equipment and Communications*, 2011, no. 1, pp. 33–39 (in Russ.).

7. Shcherbakov G.N., Shlykov Yu.A., Nikolaev A.V., Brovin A.V. [To the assessment of fundamental limits in nonlinear radar]. Spectehnika i svjaz' [*Special Equipment and Communications*], 2008, no. 2, pp. 21–25 (in Russ.).

8. Gallagher K. A. Harmonic Radar: Theory and Applications to Nonlinear Target Detection, Tracking, Imaging and Classification. Dissertation in electrical engineering. The Pennsylvania State University, 2015. Available at: https://etda.libraries.psu.edu/files/final_submissions/11380, free (Accessed: December 15, 2023).

9. Fazi C., Crowne F., Ressler M. Design Considerations for Nonlinear Scattering: Report of U.S. Army Research Laboratory No. ARL-TR-5684. 2011. Available at: https://www.govinfo.gov/content/pkg/GOVPUB-D101-PURL-gpo14593/pdf/GOVPUB-D101-PURL-gpo14593.pdf, free (Accessed: December 15, 2023).

10. Anderson S.J. Nonlinear scattering at HF: Prospects for exploitation in OTH radar systems. *Turkish Journal of Electrical Engineering and Computer Sciences*, 2010, vol. 18, no. 3, pp. 439–456.

11. Berezin A.A. *Dvuhtaktnyj obostritel' impul'sov na diodah s nakopleniem zarjada* [Two-Stroke Step Recovery Diode Pulse Sharpener]. SVCh-tehnika i telekommunikacionnye tehnologii (CriMiCo 2022). Materialy 32 Mezhdunarod. konf. [*Microwave & Telecommunication Technology*. Proceedings of the 32nd International Conference]. Sevastopol, SevSU, 2022, pp. 247–248 (in Russ.).

12. Andreev Yu.A., Buyanov Yu.I., Koshelev V.I. *Malogabaritnye sverhshirokopolosnye antenny dlja izluchenija moshhnyh jelektromagnitnyh impul'sov* [Small-Size Ultra-Wideband Antennas for the Radiation of Powerful Electromagnetic Pulses]. Zhurnal radiojelektroniki [*Journal of Radio Electronics*], 2015, no. 4 (in Russ.).

13. Directional coupler Mini Circuits ZUDC20-183+. Available at: https://www.minicircuits.com/pdfs/ZUDC20-183+.pdf, free (Accessed: November 15, 2023).

14. High-frequency Schottky diode HSMS-8101. Available at: https://pdf1.alldatasheet.com/datasheet-pdf/view/527214/AVAGO/HSMS-8101.html, free (Accessed: November 20, 2023).

15. Ruck G.T., Barric D.E., Stuart W.D., Krichbaum C.K. *Radar Cross Section Handbook*. New York, USA, Springer, 1970, 949 p.

16. Stroboscopic USB Oscilloscopes PicoScope Series 9300. Available at: https://www.picotech.com/download/datasheets/picoscope9300-series-sampling-oscilloscopes-datasheet.pdf, free (Accessed: October 15, 2023).

17. Keysight Infiniium MXR604A Oscilloscope. Available at: https://akmetron.ru/upload/iblock/fdc/fdcd1e56698db6933ddc19200552a729.pdf, free (Accessed: November 20, 2023).

18. Shipilov S.E., Yakubov V.P. Nonlinear Transformations of Pulsed Signals in Radar Tomography. *Russian Physics Journal*, 2020, vol. 63, no. 2, pp. 5–14.

---

**Anna E. Baikalova**
Junior Researcher, Institute of High Current Electronics,
Siberian Branch of the Russian Academy of Sciences
Assistant, Department of Radioelectronics
and Communication Systems, Tomsk State University
of Control Systems and Radioelectronics (TUSUR)
2/3, Akademichesky pr., Tomsk, Russia, 634055
Phone: +7 (382-2) 49-15-44
Email: annabajkalova2016@gmail.com

**Edward V. Semyonov**
Doctor of Science in Engineering, Senior Researcher,
Institute of High Current Electronics,
Siberian Branch of the Russian Academy of Sciences
Professor, TUSUR
2/3, Akademichesky pr., Tomsk, Russia, 634055
ORCID: 0000-0001-5470-1185
Phone: +7 (382-2) 49-15-44
Email: edwardsemyonov@narod.ru

УДК 621.317.08

**Г.Г. Порубов, В.П. Денисов**

# Алгоритм обработки сигналов в фазовых пеленгаторах с двумя линейными антенными решетками, расположенными под углом друг к другу

Предлагается алгоритм обработки сигналов в двухкоординатных фазовых радиопеленгаторах, антенные системы которых состоят из двух линейных решеток с произвольным количеством фазометрических баз в каждой, расположенных под углом друг к другу. Получены и проверены путем моделирования работы пеленгатора на ЭВМ соотношения для расчета вероятности разрешения неоднозначности фазовых измерений и СКО результатов измерений. Применение алгоритма приводит к упрощению обработки сигналов по сравнению с известными.
**Ключевые слова:** фазовый пеленгатор, разность фаз, пеленг.
**DOI:** 10.21293/1818-0442-2023-26-4-19-25

Предметом рассмотрения данной статьи является двухкоординатный фазовый пеленгатор, плоская антенная система которого состоит из двух линейных решеток, расположенных под углом друг к другу. Сложнейшей задачей обработки сигналов в подобных системах является устранение неоднозначности фазовых измерений и использование для оценки пеленга всей информации, содержащейся в совокупности разностей фаз на элементах антенной системы. Исторически первым и долгое время единственным методом обработки сигналов в многоканальных фазовых пеленгаторах был так называемый метод уточнений. Антенная система пеленгатора в виде линейной решетки содержала достаточно малую фазометрическую базу, обеспечивающую грубое, но однозначное пеленгование в заданном угловом секторе. Последовательное устранение неоднозначности от меньшей базы к большей обеспечивало однозначное пеленгование по самой большой базе [1, 2]. Недостатком данного подхода является то, что точность пеленгования определяется только одной базой, самой большой. Остальные измерения используются только для разрешения неоднозначности на этой базе. Часть информации о пеленге, содержащаяся в них, утрачивается.

Развитие статистических методов обработки информации привело к тому, что они стали применяться и для обработки неоднозначных измерений. Вся совокупность полученных разностей фаз стала использоваться для получения точного и однозначного измерения [3–7].

Основой статистического подхода является метод максимального правдоподобия. Первоначально он был развит для однокоординатных измерителей, а затем был применен к двухкоординатным пеленгаторам с антенными системами в виде плоской либо конформной решетки любой конфигурации [8, 9]. Метод не требует, чтобы одна из фазометрических баз обеспечивала однозначное измерение в заданном секторе, но базы должны относиться друг к другу как взаимно простые числа.

Недостатком метода является то, что для его реализации требуется знать закон распределения вероятностей погрешностей фазовых измерений. Другим недостатком метода является большой объем вычислений при корректном использовании.

Существуют также методы обработки совокупности измеренных разностей фаз, привязанные к антенным системам определенной структуры. Так, в статье [10] рассматривается пеленгатор, антенная система которого состоит из трех элементов, расположенных в линию. Производится три измерения разностей фаз, одно из которых с позиции монографии [8] является избыточным. Метод обеспечивает однозначное измерение пеленга в широком секторе, если измерительные базы относятся между собой как иррациональное число, например число Фидия [10]. Как достоинство метода отмечается отсутствие необходимости иметь однозначную фазометрическую базу.

Рассматриваемый в данной статье метод также привязан к антенной системе определенной структуры. Это антенная система, состоящая из двух линейных решеток, расположенных под углом дуг к другу. Статья является развитием прежней работы авторов, где линейные решетки расположены под углом девяносто градусов друг к другу [11]. Суть метода заключается в том, что вычисление углового положения источника радиоизлучения (ИРИ) выполняется сравнением совокупности измеренных разностей фаз (вектора измерений) с совокупностью расчетных разностей фаз, соответствующих некоторому углу прихода плоской волны, и подбор такого угла прихода, который наиболее соответствует результатам измерений. Применительно к пеленгаторам с линейными антенными решетками данный подход изложен в статье [12]. Его привлекательной стороной является то, что для вычислений не требуется знать закон распределения вероятностей погрешностей фазовых измерений. Специфическая конструкция антенной решетки не должна вызывать отторжения у читателя. Необходимость использования подобной решетки может быть вызвана конструкцией носителя пеленга-

тора. Пример встроенной антенной системы пеленгатора имеется, например, в работе [14]. В терминологии монографии [13] метод является непараметрическим.

Предположим, что антенная система пеленгатора расположена в плоскости $x_1 0_1 z$ и поднята относительно земли на высоту $h$ (рис. 1), а ось $0_1 y_1$ перпендикулярна к плоскости антенной решетки. Азимут $\alpha$ характеризует угловое положение объекта наблюдения $C(x_c, y_c)$ в плоскости земли, а угол места $\beta$ – положение объекта относительно плоскости $x_1\ 0_1\ y_1$.

Углы $\alpha_{x1}$ и $\alpha_z$ задают направление на объект наблюдения относительно осей координат $0_1 x_1$ и $0 z$. Обозначим направляющие косинусы принимаемой волны $\cos\alpha_{x1} = v_x$, $\cos\alpha_z = u_z$.

Используя рис. 1, получим следующие соотношения:

$$v_x = \cos\alpha_{x1} = \frac{0_1 x_{c1}}{0_1 C} = \sin\alpha\cos\beta, \qquad (1)$$

$$u_z = \cos\alpha_z = \frac{0_1 0}{0_1 C} = \sin\beta, \qquad (2)$$

где $0_1 x_{c1} = y_c C = 0C\sin\alpha$, $0_1 C = 0C/\cos\beta$, $0_1 0 = 0_1 C\sin\beta$.

Отметим, что углы $\alpha_{x1}$ и $\alpha_z$ полностью определяют угловое положение источника радиоизлучения относительно осей $0_1 x_1$ и $0 z$.

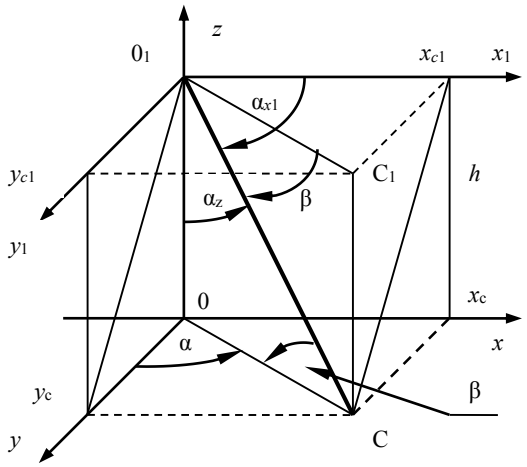



Рис. 1. Положение источника сигнала $C(x_c, y_c)$ и антенной системы пеленгатора (точка $0_1$) в трёхмерном пространстве

Линейные антенные решетки, образующие плоскую антенную решетку, относительно оси $0 z$ расположены симметрично под углами $\pm\theta$ (рис. 2). На рис. 2 приведены максимальные фазометрические базы линейных антенных решеток, образующих плоскую антенную решетку. Меньшие базы, используемые для разрешения неоднозначности измерений, будем называть дополнительными.

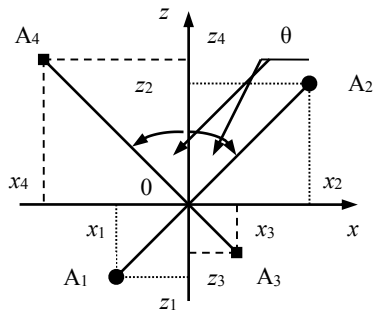



Рис. 2. Пример расположения антенн, образующих базы плоской антенной решетки пеленгатора

Перейдём к обозначениям баз и проекций баз на оси координат, принятым в работах по фазовым пеленгаторам: $l_1$ – база, образованная антеннами $A_1, A_2$; $l_{11}$ – база, образованная антеннами $A_3, A_4$; $l_{x1} = (x_2 - x_1)$ – проекция базы $l_1$ на координатную ось $x$; $l_{z1} = (z_2 - z_1)$ – проекция базы $l_1$ на координатную ось $z$; $l_{x11} = (x_4 - x_3)$ – проекция базы $l_{11}$ на координатную ось $x$; $l_{z11} = (z_4 - z_3)$ – проекция базы $l_{11}$ на координатную ось $z$.

Полные разности фаз на базах $l_1$ и $l_{11}$, при измерении в $\text{рад}/2\pi$, определяются по формулам [8]

$$\left.\begin{aligned} \Phi_1 &= \frac{l_{x1}}{\lambda}\cos\alpha_{x1} + \frac{l_{z1}}{\lambda}\cos\alpha_z, \\ \Phi_{11} &= \frac{l_{x11}}{\lambda}\cos\alpha_{x1} + \frac{l_{z11}}{\lambda}\cos\alpha_z. \end{aligned}\right\} \qquad (3)$$

Подставляя из (1), (2) в (3) значения $\cos\alpha_{x1}$ и $\cos\alpha_z$, получим формулы, определяющие полные разности фаз на базах $l_1$ и $l_{11}$ в зависимости от азимута и угла места:

$$\left.\begin{aligned} \Phi_1 &= \frac{l_{x1}}{\lambda}\sin\alpha\cos\beta + \frac{l_{z1}}{\lambda}\sin\beta + \delta_1 = \varphi_i + k_1, \\ \Phi_{11} &= \frac{l_{x11}}{\lambda}\sin\alpha\cos\beta + \frac{l_{z11}}{\lambda}\sin\beta + \delta_{11} = \varphi_{11} + k_{11}, \end{aligned}\right\} \qquad (4)$$

где $\alpha$ – азимут; $\beta$ – угол места; $\varphi_1$, $\varphi_{11}$ – измеренные разности фаз; $\delta_1$, $\delta_2$ – ошибки измерений разностей фаз; $k_1$, $k_{11}$ – число полных периодов разностей фаз, утраченных при измерении на базах $l_1$ и $l_{11}$; $l_{x1}$, $l_{z1}$, $l_{x11}$, $l_{z11}$ – проекции баз $l_1$ и $l_{11}$ на оси координат.

Ошибки измерения разностей фаз являются составной частью результатов измерений, поэтому они исключены из правых частей формул (4).

Проекции баз $l_1$ и $l_{11}$ на оси координат при положении антенных решеток относительно оси $z$ под углами $\theta_1 = 90° - \theta$ и $\theta_2 = 90° + \theta$ (см. рис. 2) будут равны

$$\left.\begin{aligned} l_{x1} &= l_1 \cos\theta_1, \\ l_{z1} &= l_1 \sin\theta_1, \\ l_{x11} &= l_{11} \cos\theta_2, \\ l_{z11} &= l_{11} \sin\theta_2. \end{aligned}\right\} \qquad (5)$$

Представим полные разности фаз (4) в следующем виде:

$$\left.\begin{aligned} \Phi_1 &= \varphi_{x1} + k_{x1} + \varphi_{z1} + k_{z1} = \\ &= (\varphi_{x1} + \varphi_{z1}) + (k_{x1} + k_{z1}) = \varphi_1 + k_1, \\ \Phi_{11} &= \varphi_{x11} + k_{x11} + \varphi_{z11} + k_{z11} = \\ &= (\varphi_{x11} + \varphi_{z11}) + (k_{x11} + k_{z11}) = \varphi_{11} + k_{11}\ , \end{aligned}\right\} \qquad (6)$$

где $\varphi_{x1}$, $\varphi_{x11}$ и $k_{x1}$, $k_{x11}$ – измеренные разности фаз и число полных периодов разностей фаз, утраченных при измерении на максимальных базах $l_1$ и $l_{11}$, зависящие от азимута (первые слагаемые формул (4)); $\varphi_{z1}$, $\varphi_{z11}$ и $k_{z1}$, $k_{z11}$ – измеренные разности фаз и число полных периодов разностей фаз, утраченных при измерении, зависящие от угла места (вторые слагаемые формул (4)).

Из формул (4) и (6) видно, что измеренные разности фаз $\varphi_1$, $\varphi_{11}$ на базах $l_1$, $l_{11}$ и число полных периодов разностей фаз, утраченных при измерении $k_1$, $k_{11}$, определяются суммой, в которой одно из слагаемых зависит от азимута, а другое от угла места.

При равенстве баз $l_1$ и $l_{11}$ их проекции на соответствующие оси координат будут равны по абсолютной величине (5). А различие по знаку проекций баз на координатную ось $x$ (5) позволяет определить суммы измеренных разностей фаз и суммы числа потерянных полных периодов, определяемых независимо азимутом и углом места, по формулам

$$\left.\begin{aligned} \varphi_{x1} + \varphi_{x11} &= \varphi_1 - \varphi_{11}, \\ \varphi_{z1} + \varphi_{z11} &= \varphi_1 + \varphi_{11}. \end{aligned}\right\} \qquad (7)$$

$$\left.\begin{aligned} k_{x1} + k_{x11} &= k_1 - k_{11}, \\ k_{z1} + k_{z11} &= k_1 + k_{11}. \end{aligned}\right\} \qquad (8)$$

Угол $\theta$ может быть выбран в пределах $0° < \theta < 90°$. При этом сохраняется возможность определения суммы измеренных разностей фаз и суммы их полных периодов, зависящих от азимута и угла места, по формулам (7), (8). Угол $\theta$ определяет положение линейных антенных решеток относительно осей координат и проекции каждой из баз $l_1$ и $l_{11}$ на оси координат, обеспечивая равенство проекций на ось $x$ и ось $z$.

Разности фаз и числа полных периодов разностей фаз, зависящие от азимута и угла места, по формулам (7), (8) используются далее для вычисления пеленгов по предлагаемому алгоритму.

Предположим далее, что линейные решетки, образующие антенную систему пеленгатора, содержат произвольное число фазометрических баз каждая.

Вектор баз на каждой из решеток в относительных единицах $n_i = l_i/\lambda$ запишем в виде

$$\mathbf{n} = (n_1,\ n_2,\ ...,n_n), \qquad (9)$$

где нижний индекс $n$ – количество фазометрических баз.

Предположим также, что фазометрические базы относятся между собой как взаимно простые числа. Тогда можно записать:

$$\mathbf{e}_i = \Delta_{\text{одн}} \mathbf{n}_i, \qquad (10)$$

где $\mathbf{e}_i$ – вектор взаимно простых целых чисел, а коэффициент $\Delta_{\text{одн}}$ имеет смысл интервала однозначного пеленгования по каждой из линейных решеток, измеренного по направляющему косинусу.

Действительно, пусть разность фаз измеряется в $\text{рад}/2\pi$. Тогда соотношение (10) представляет собой основную формулу фазовой пеленгации, связывающую направляющий косинус падающей волны с разностью фаз на разнесенных антеннах и измерительной базой, с той разницей, что в ней полные разности фаз на базах целые числа. При изменении угла прихода волны на величину, соответствующую $\Delta_{\text{одн}}$, полная разность фаз на каждой из фазометрических баз изменится на целое число периодов. Следовательно, измеряемая разность фаз не изменится, не изменится и индицируемый пеленг.

Будем полагать, что интервалы однозначного пеленгования по каждой из линейных решеток одинаковы. Методика расчета пространственного двумерного угла при заданных величинах $\Delta_{\text{одн}}$ в ортогональных плоскостях изложена в работе [9].

Для удобства выкладок условимся фазовые измерения представлять в $\text{рад}/2\pi$ и введём обозначения $\sin\alpha = v$, $\sin\beta = u$, $\cos\beta = w$.

Тогда формулу полной разностей фаз на $i$-й базе можно записать в виде формулы

$$\Phi_i = n_{xi} v w + n_{zi} u + \delta_i = \varphi_i + k_i, \qquad (11)$$

где $n_{xi} = n_i \cos\theta_i$ и $n_{zi} = n_i \sin\theta_i$ – проекции базы $n_i = l_i/\lambda$ на оси координат в длинах волн сигнала пеленгуемого источника; $\varphi_i$ – измеренная разность фаз с учетом погрешностей измерений; $\delta_i$ –погрешность измерений разности фаз; $k_i$ – число полных периодов разности фаз $\Phi_i$ на базе $l_i$, утраченных при измерении в силу периодичности сигналов.

Предварительно определяется максимально возможное число полных периодов разностей фаз $k_1$ и $k_{11}$, утрачиваемых при измерении на максимальных базах в пределах рабочего сектора пеленгатора при $l_1 = l_{11}$, по формуле

$$k_i = \langle l_1 \sin\alpha \rangle, \qquad (12)$$

где $l_1$ – максимальная база в целых числах; $\alpha = \pm\alpha_{\text{раб}}$ – рабочий сектор пеленгатора по азимуту; $\langle\cdot\rangle$ – операция округления до ближайшего целого.

При выбранной величине угла $\theta$ определяются суммы проекций максимальных баз в относительных величинах на координатные оси $x$ и $z$ по формулам

$$\left.\begin{aligned} n_{1sx} &= n_1 \cos\theta_1 - n_{11}\cos\theta_2, \\ n_{1sz} &= n_1 \sin\theta_1 + n_{11}\sin\theta_2, \end{aligned}\right\} \quad (13)$$

где $n_1$ и $n_{11}$ – максимальные базы в относительных величинах.

Определяются шаги изменения пеленга по азимуту $(\sin\alpha)$ и по углу места $(\sin\beta)$ при изменении полной разности фаз на $k_1 2\pi$ на базах, определённых как суммы проекций максимальных баз на оси координат (13), по формулам

$$\left.\begin{aligned} v_1 &= 1/n_{1sx}, \\ u_1 &= 1/n_{1sz}. \end{aligned}\right\} \quad (14)$$

Допустим, что по некоторому источнику, находящемуся на азимуте $\alpha_r$, и под углом места $\beta_r$ выполнено измерение разностей фаз. В соответствии с формулой (11) на $i$-й базе измеренная разность фаз будет

$$\varphi_{ri} = \Phi_i - \langle \Phi_i \rangle = \varphi_i, \quad (15)$$

где $\Phi_i$ – полная разность фаз; $\varphi_i$ – измеренная разность фаз, соответствующая углу прихода волны; $\langle\cdot\rangle$ – операция округления до ближайшего целого.

По результатам измерений получим два $n$-мерных вектора разностей фаз (15), где $n$ – число баз на каждой из линейных антенных решеток, образующих антенную систему,

$$\boldsymbol{\varphi}_r = (\varphi_{r1},\ \varphi_{r2},\ ...,\ \varphi_{rn}). \quad (16)$$

Определение числа потерянных периодов разностей фаз на каждой из максимальных баз выполняется сравнением векторов измеренных разностей фаз (16) с векторами расчётных разностей фаз

$$\boldsymbol{\varphi}_\rho = (\varphi_{\rho 1},\ \varphi_{\rho 2},\ ...,\ \varphi_{\rho n}). \quad (17)$$

Элементы вектора расчётных разностей фаз (17) находятся по нижеследующим формулам при последовательном задании числа утраченных периодов разностей фаз $k_1$ и $k_{11}$ на максимальных базах в пределах, определяемых по формуле (12):

$$\left.\begin{aligned} \varphi_{\rho i} &= \frac{(\varphi_{r1} + k_1)\ l_i}{l_1} - \left\langle \frac{(\varphi_{r1} + k_1)\ l_i}{l_1} \right\rangle, \\ \varphi_{\rho i} &= \frac{(\varphi_{r11} + k_{11})\ l_i}{l_{11}} - \left\langle \frac{(\varphi_{r11} + k_{11})\ l_i}{l_{11}} \right\rangle, \end{aligned}\right\} \quad (18)$$

где $\varphi_{r1}$, $\varphi_{r11}$ – измеренные разности фаз на максимальных базах (15); $k_1$, $k_{11}$ – число полных периодов разностей фаз на максимальных базах; $l_i$ – дополнительные базы; $l_1$, $l_{11}$ – максимальные базы; $\langle\cdot\rangle$ – операция округления до ближайшего целого.

После каждого шага вычислений определяются разности

$$\psi_i = \left(\varphi_{ri} - \varphi_{\rho i}\right) - \left\langle \left(\varphi_{ri} - \varphi_{\rho i}\right) \right\rangle, \quad (19)$$

где $\varphi_{ri}$ – результат измерения разности фаз на дополнительной базе $l_i$; $\varphi_{\rho i}$ – результат вычисления разности фаз по формуле (18) на дополнительной базе $l_i$; $\langle\cdot\rangle$ – операция округления до ближайшего целого.

Условие правильного определения числа потерянных периодов разностей фаз $k_1$, $k_{11}$ на каждой из максимальных баз $l_1$ и $l_{11}$ запишем в виде

$$|\psi_i| \le z_{\varphi i}, \quad (20)$$

где $i = 2, 3, ..., n$ – номера дополнительных баз; $z_{\varphi i}$ – разрешенная зона по фазе для дополнительной базы $l_i$, вычисленная по формуле

$$z_{\varphi i} = 0{,}5\Delta_i, \quad (21)$$

где $\Delta_i$ – изменение разности фаз на дополнительной базе $l_i$, соответствующее изменению угла прихода волны на антенную систему, при котором разность фаз на максимальной базе $l_1$ изменяется на $k_1 2\pi$ радиан. Здесь используется термин «разрешенная зона по фазе», введенный в статье [14]. Очевидно,

$$\Delta_i = k_1 2\pi \frac{l_i}{l_1} - \left\langle k_1 2\pi \frac{l_i}{l_1} \right\rangle. \quad (22)$$

Разрешенная зона $\Delta_i$ на дополнительной базе $l_i$ находится по формуле (22) при задании величины $k_1 \ne 0$ в пределах, следующих из формулы (12).

Если условие (20) не выполняется хотя бы по одной из дополнительных баз данной линейной антенной решетки, решение об определении числа потерянных разностей фаз не принимается и поиск продолжается.

При выполнении условия (20) по всем дополнительным базам каждой из линейных антенных решеток принимается решение об определении числа потерянных периодов разностей фаз $k_1$ и $k_{11}$ на максимальных базах $l_1$ и $l_{11}$.

В соответствии с формулой (7) определяются начальные значения синуса азимута и синуса угла места по результатам измерения разностей фаз на максимальных базах по формулам

$$\left.\begin{aligned} v_{\text{мин}} &= (\varphi_{r1} - \varphi_{r11})/n_{1sx}, \\ u_{\text{мин}} &= (\varphi_{r1} + \varphi_{r11})/n_{1sz}, \end{aligned}\right\} \quad (23)$$

где $\varphi_{r1}$ и $\varphi_{r11}$ – измеренные разности фаз на максимальных базах $l_1$, $l_{11}$ (15); $n_{1sx}$, $n_{1sz}$ – суммы проекций максимальных баз на оси координат, определяемые по формуле (13).

Вычисления синусов искомых пеленгов выполняются по формулам

$$\sin\beta_{\text{иск}} = \left(u_{\text{мин}} + u_1\left(k_1 + k_{11}\right)\right), \quad (24)$$

$$\sin\alpha_{\text{иск}} = \left(v_{\text{мин}} + v_1\left(k_1 - k_{11}\right)\right)\Big/\cos\beta_{\text{иск}}, \quad (25)$$

где $v_{\text{мин}}$ и $u_{\text{мин}}$ – начальные значения синусов азимута и угла места по формулам (23); $v_1$ и $u_1$ – шаг изменения пеленгов при изменении полной разности фаз на величину $k_1 2\pi$ на базах $n_{1sx}$, $n_{1sz}$, вычисленных по формулам (13); $k_1$ и $k_{11}$ – число потерянных периодов разностей фаз на максимальных базах $l_1$ и $l_{11}$, при задании которых в формулу (18) и при вычислении разности по формуле (19) выполняется условие (20).

Искомые пеленги вычисляются по формулам

$$\beta_{\text{иск}} = \arcsin\left(u_{\text{мин}} + u_1\left(k_1 + k_{11}\right)\right), \quad (26)$$

$$\alpha_{\text{иск}} = \arcsin\left[\left(v_{\text{мин}} + v_1\left(k_1 - k_{11}\right)\right)/\cos\beta_{\text{иск}}\right]. \quad (27)$$

Рассматриваемый алгоритм можно характеризовать вероятностью правильного вычисления пеленгов (не допускается грубых ошибок определения пеленга за счет неверного определения числа полных периодов разностей фаз) и точностью пеленгования при этом условии.

Условие отсутствия аномальных ошибок следует из алгоритма (20): они отсутствуют, если одновременно выполняются $2n$ соответствующих неравенств. Формулу для вычисления вероятности правильного пеленга (обозначим ее $P_0$) запишем в виде

$$P_0 = \int_{-z_{\varphi i}}^{z_{\varphi i}} \ldots \int_{-z_{\varphi 2n}}^{z_{\varphi 2n}} w_{2n-2}\left(y_2, \ldots, y_{2n}\right) dy_2, \ldots, dy_{2n}, \quad (28)$$

где $w_{2n-2}\left(y_3, \ldots, y_{2n}\right)$ – плотность распределения вероятностей случайных величин $\psi_i$ (19); $2n$ – общее число баз пеленгатора; $z_{\varphi i}$ – разрешенная зона по фазе базы $l_i$ (21).

Для дальнейших вычислений надо задать закон распределения вероятностей погрешностей фазовых измерений. Предположим, что это нормальные случайные величины с нулевыми средними значениями, равными дисперсиями $\sigma_\varphi^2$. Тогда $\psi_i$ также нормальные случайные величины с нулевыми средними значениями и СКО

$$\sigma_i = \sigma_\varphi \sqrt{\frac{l_1^2 + l_i^2 - 2 r_i l_1 l_i}{l_1^2}},$$

где $r_i$ – коэффициент корреляции погрешностей фазовых измерений на $i$-й и первой (максимальной) базах.

На рис. 3 приведена зависимость вероятности правильного пеленгования от фазовых ошибок для антенной системы, состоящей из двух линейных антенных решеток. Оценка выполнена по формуле (28) для структур антенных решеток $\mathbf{n} = \left(n_1, n_2, n_3\right) = \left(9, 6, 4\right)$ каждой, являющейся оптимальной по критерию максимума $P_0$ при заданных габаритных размерах антенной системы и числе антенн.

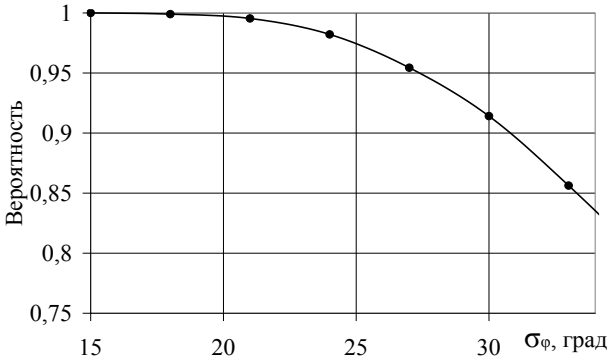



Рис. 3. Зависимость вероятности правильного пеленгования от фазовых ошибок по формуле (28)

Точность пеленгования по азимуту и углу места определяется суммой проекций максимальных баз на оси координат, определяемых по формулам (13), и погрешностями фазовых измерений на максимальных базах. При вычислении начальных значений синуса азимута и синуса угла по формулам (23) ошибки фазовых измерений суммируются.

На рис. 4 представлена зависимость погрешностей пеленгования по азимуту и углу места от угла $\theta$. Оценка выполнена для структур антенных решеток $\mathbf{n} = \left(n_1, n_2, n_3\right) = \left(9, 6, 4\right)$. При моделировании СКО погрешностей фазовых измерений задавалась равной $\sigma_\varphi = 25°$.

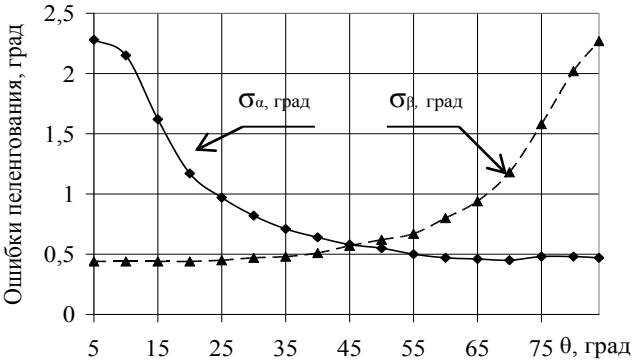



Рис. 4. Зависимость ошибки пеленгования по азимуту и углу места от величины угла $\theta$:
■ – $\sigma_\alpha$ ошибки пеленгования по азимуту;
▲ – $\sigma_\beta$ ошибки пеленгования по углу места

**Выводы**

Теоретические выкладки и моделирование работы двухкоординатного фазового пеленгатора по предлагаемому алгоритму показали его состоятельность. Алгоритм удобен, когда условия размещения антенной системы пеленгатора на его носителе заставляют делать ее в виде двух линейных решеток с произвольным количеством фазометрических баз в каждой, расположенных под углом друг к другу. Предложена и опробована путем моделирования на ЭВМ методика расчета вероятности правильного

разрешения неоднозначности фазовых измерений и СКО азимута и угла места.

Работа выполнена в рамках проекта по госзаданию Минобрнауки РФ № FE-2023-0014.

*Литература*

1. Теоретические основы радиолокации: учеб. пособие для вузов / под ред. В.Е. Дулевича. – М.: Сов. радио, 1978. – 608 с.

2. Радиотехнические системы: учеб. для вузов / под ред. Ю.М. Казаринова. – М.: Академия, 2008. – 590 с.

3. Собцов Н.В. Оценка максимального правдоподобия в многошкальной фазовой измерительной системе // Радиотехника и электроника. – 1973. – Т. 18, № 6. – С. 1180–1186.

4. А.с. 993146 СССР, МПК G01 25/00 (2000.01) Устройство разрешения неоднозначности фазовых измерений / И.Г. Неплохов. – Опубл.: 30.01.1983. Б.И. № 4. – С. 227.

5. Коротков П.И. Алгоритмы оценивания вектора параметров объекта для многоканальной фазовой измерительной системы: дисс. … канд. физ.-мат. наук. – Омск: Омск. гос. техн. ун-т, 2016. – 128 с.

6. Пензин В.К. Алгоритмы оперативной обработки многошкальных измерений по критерию максимального правдоподобия // Радиотехника и электроника. – 1990. – Т. 35, № 1. – С. 97.

7. Кинкулькин И.Е. Глобальные навигационные спутниковые системы: алгоритмы функционирования аппаратуры потребителя. – М.: Радиотехника, 2018. – 325 с.

8. Денисов В.П. Фазовые радиопеленгаторы / В.П. Денисов, Д.В. Дубинин. – Томск: Изд-во ТУСУРа, – 2002. – 251 с.

9. Белов В.И. Теория фазовых измерительных систем. – Томск: Изд-во ТУСУРа, 2007. – 147 с.

10. Измерение пеленга многоканальным фазовым пеленгатором методом целочисленной минимизации функционала неоднозначности / Н.Е. Замарин, В.В. Корнев, Г.Л. Акопян, А.П. Ковалев // Радиотехника. – 2023. – Т. 87, № 5. – С. 24–39.

11. Порубов Г.Г. Устранение неоднозначности измерений в фазовых пеленгаторах с двумя ортогональными линейными антенными решетками / Г.Г. Порубов, В.П. Денисов // Доклады ТУСУР. – 2022. – Т. 25, № 2. – С. 7–12.

12. Порубов Г.Г. Непараметрический алгоритм обработки сигналов в фазовых пеленгаторах с линейной антенной решеткой / Г.Г. Порубов, В.П. Денисов // Доклады ТУСУР. – 2021. – Т. 24, № 3. – С. 7–11.

13. Левин Б.Р. Теоретические основы статистической радиотехники: в 3 кн. – Кн. 3. – М.: Сов. радио, 1976. – 288 с.

14. Порубов Г.Г. Методика выбора оптимальных структур антенных решеток фазовых пеленгаторов и оценка вероятностных характеристик // Доклады ТУСУР. – 2017. – Т. 20, № 1. – С. 5–9.

---

**Порубов Геннадий Гаврилович**
Инженер ОАО «Научно-исследовательский институт автоматических приборов» (НИИАП), г. Новосибирск
Дзержинского пр-т, 87, г. Новосибирск, Россия, 630051
Тел.: +7 (383-2) 79-52-28
Эл. почта: porub27@mail.ru

**Денисов Вадим Прокопьевич**
Д-р техн. наук, проф. каф. радиотехнических систем (РТС) Томского государственного ун-та
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-36-70
Эл. почта: vadimdenisov418@gmail.com

Porubov G.G., Denisov V.P.

**Algorithm for signal processing in the phase radio finders with two linear aerials located at an angle to each other**

The article suggests an algorithm of processing the signals in two-coordinated phase radio finders. The aerial systems of this finders consist of two linear aerials with any number of phase-metric bases in each. The correlations for calculating the probability of ambiguity resolution of phase measurements and the standard error of the calculation results are obtained and checked by modeling the finder operation on computers. The use of the mentioned above algorithm simplifies the signal processing in comparison with the known ones.

**Keywords:** phase radio finder, phase difference, bearing.
**DOI:** 10.21293/1818-0442-2023-26-4-19-25

*References*

1. *Ttorticheskie osnovy daiolokatsii*: *uchebnoe posobie dlya vusjv* [Theoretical fundamentals of radiolocation: manual for higher institutions] edited by V.E. Dulevitch. Moscow, *Soviet Radio*, 1978, 608 p. (in Russ.).

2. *Radio tekhnicheskie sistemy: uchebnik dlya vusov* [Radiotechnical systems: manual for higher institutions] edited by Yu.M. Kazarinov. Moscow, «Academiya», 2008, 590 p. (in Russ.).

3. Sobtsov N.V. *Otsenka maksimaljnogo pravdopodobiya v mnogoshkalinoi fazovoj izmeriteljnnoi sisteme* [Estimation of maximum verisimilitude in the multiscale phase measurement system]. *Radio Engineering and Electronics*. 1973, vol. 18, no. 6, 1180 p. (in Russ.).

4. Neplokhov I.G. *Ustrojsttvo razresheniya neodnoznachnosti fasovykh izmerenij* [Device for solving the ambiguity of phase measurements]. Authorship Certificate USSR, no. 993146, 1983.

5. Korotkov P.I. *Algoritmy otsenivaniya vektora parametrov dlya mnogokanaljnoj fazovoj izmeriteljnoj sistyemy* [Algorithms of estimating the vector of object parameters for the multichannel phase measurement system]. Dissertation for the Candidate of Sciences degree. Omsk State Technical University, 2016, 128 p. (in Russ.).

6. Penzin V.K. *Algoritmy operativnoj obrabotki mnogoshkaljnykh izmerenij po kriteriyu maksimaljnogo pravdopodobiya* [Algorithm of operational processing of multiscale measurements by the criterion of maximum verisimilitude]. *Radio Engineering and Electronics,* 1990, vol. 35, no. 1, 97 p. (in Russ.).

7. Kinkulkin I.E. *Globaljnye navigatsionnye sputnikovye sistemy: algoritmy funktsionirovaniya apparatury potrebitelya* [Global navigation satellite systems: algorithms of functioning the user devices]. Moscow, *Radio Engineering*, 2018, 325 p. (in Russ.).

8. Denisov V.P., Dubinin D.V. *Fazovye radiopelengatori* [Phase radio direction finders]. Tomsk. Publishing office of TUSUR University, 2202, 251 p. (in Russ.).

9. Belov V.I. *Teoriya fazovyh izmeritelnih system* [Theory of phase measurement systems]. Tomsk. Publishing office of TUSUR University, 2007, 147 p. (in Russ.).

10. Zamarin N.E., Kornev V.V., Akopyan G.L., Kovalev A.P. *Ismerenie pelenga mnogokanalnym fasovym pelengatorom metodom tselochislennoj minimisatsii funktsionala neodnosnachnosti* [Bearing measurement by multi-channel phase radio finder through a method of integral minimization of ambiguity functional] // *Radiotechnics*, 2023. vol. 87, no. 5, pp. 24–39 (in Russ.).

11. Porubov G.G., Denisov V.P. *Ustranenie neodnoznachnosti izmerenij v fazovyh pelengatorah s dvumja ortogonalnymi linejnymi antennymi reshetkami* [Eliminating the measurement ambiguity in phase direction finders with two orthogonal linear aerial arrays]. *Proceedings of TUSUR University*, 2022, vol. 25, no. 2, pp. 7–12 (in Russ.).

12. Porubov G.G., Denisov V.P. *Neparametrichesky algoritm obrabotki signalov v fazovyh pelengatorah s linejnoi antennoi reshetkoi* [Nonparametric algorithm of processing the signals in phase direction finders with a linear aerial array]. *Proceedings of TUSUR University*, 2021, vol. 24, no. 3, pp. 7–11 (in Russ.).

13. Levin B. R. *Teoreticheskie osnovy statisticheskoj radiotekhniki* [Theoretical fundamentals of static radio engineering]. In 3 pt., pt. 3. Moscow, *Soviet Radio*, 1976. 288 p. (in Russ.).

14. Porubov G.G. *Metodika vybora optimaljnyh struktur antnnykh reshetok fazovykh radiopelengatopov i otzenka veroyatnostnykh kharacteristics* [Methods of choosing the optimal structures of the aerial arrays of the phase direction finders and the estimation of the probable characteristics]. *Proceedings of TUSUR University*, 2017, vol. 20, no. 1, pp. 5–9 (in Russ.).

---

**Gennady G. Porubov**
Engineer, Joint Stock Company «NIIAP», Novosibirsk
87, Dzerzhinsky pr., Novosibirsk, Russia, 630051
Phone: +7 (383-2) 79-52-28
Email: porub27@mail.ru

**Vadim P. Denisov**
Doctor of Science in Engineering, Professor,
Department of Radio Engineering Systems (RTS),
Tomsk State University of Control Systems
and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 41-36-70
Email: vadimdenisov418@gmail.com

# УПРАВЛЕНИЕ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА

УДК 004.056

**И.А. Огнев, И.В. Никрошкин, М.А. Медведев, А.Д. Красников**

# Исследование встроенных средств защиты информации Unix-систем на примере заражения вредоносным программным обеспечением

Приводится сравнительный анализ встроенных средств защиты информации операционных систем семейства Unix на примере заражения операционной системы вредоносным программным обеспечением. В рамках исследования были задействованы операционные системы с открытым исходным кодом – Debian и отечественные операционные системы – Alt Linux, RedOS, Astra Linux Special Edition. В качестве вредоносного программного обеспечения был использован вирус-шифровальщик (ransomware). Представленные результаты демонстрируют наибольшую способность операционной системы Astra Linux противостоять заражению вредоносным программным обеспечением.

**Ключевые слова:** информационная безопасность, защита информации, вредоносное программное обеспечение, вирус-шифровальщик, операционная система, средство защиты информации.
**DOI:** 10.21293/1818-0442-2023-26-4-29-34

Разнообразие вредоносных программ, которые широко используются, уменьшает эффективность текущих систем безопасности, что приводит к заражению миллионов устройств различными видами вредоносного ПО, такими как черви, вымогатели, бэкдоры, компьютерные вирусы и троянские программы [1–3]. Программы-вымогатели, также известные как шифровальщики, представляют собой тип атаки, при которой злоумышленники используют различные тактики и приемы для блокировки или шифрования данных жертвы [4–8]. Эта атака обычно заканчивается ультиматумом: жертва должна заплатить за разблокировку или дешифрование, иначе все ее данные будут потеряны. Хотя крипто-вымогатели являются наиболее распространенным типом атаки, программы-вымогатели блокировок все еще актуальны [9, 10], особенно на мобильных платформах [11].

Вредоносное программное обеспечение существует с начала 1970-х гг., когда вирус Creeper впервые появился в ARPANET. За ним последовали Elk Cloner и the Brain в 1980-х гг., причем последний стал первым компьютерным вирусом в дикой природе. Это ознаменовало эпоху, когда даже машины подвержены болезням [12, 13]. Антивирусные программы также появились в начале 1970-х гг., начиная с Reaper, который был разработан для борьбы с Creeper. С тех пор появилось множество вирусов и антивирусных программ, которые борются друг с другом. В цифровую эпоху безопасность компьютеров конечных пользователей в значительной степени зависит от эффективных антивирусных сканеров, что делает антивирусные программы незаменимыми [14].

Согласно отчетам, программы-шифровальщики представляют серьезную угрозу бизнес-процессам организаций. Из отчета Fortinet [15] следует, что:

1. Из 569 опрошенных организаций, реализовавших комплекс мер по борьбе с ВПО, половина пострадала от заражения программами-шифровальщиками.

2. Из организаций, столкнувшихся с инцидентом с программами-вымогателями, 71% заявили, что заплатили хотя бы часть требуемого выкупа.

3. 35% пострадавших от программ-вымогателей восстановили все свои данные после инцидента.

4. Стремительное развитие киберпреступного мира, в частности, бизнес-схемы злоумышленников Ransomware-as-a-Service (часть схемы Malware-as-a-Service), приводит к появлению новых и более изощренных экземпляров ВПО.

Согласно отчету Check Point [16], современные тренды в технологиях, используемых в разработке и доставке ВПО, с одной стороны, используют новейшие наработки в сфере искусственного интеллекта, с другой стороны, возвращаются к классическим методам доставки и распространению ВПО через USB-носители. Команда Check Point Research указывает на заметный всплеск кибератак по всему миру. Только во втором квартале года еженедельные кибератаки выросли на 8%, что стало самым значительным всплеском за последние два года.

Согласно аналитическому отчету Kaspersky [17], в 2022 г. шифровальщики были одной из самых опасных угроз информационной безопасности в мире. Новые варианты, обходящие существующие меры безопасности, появляются регулярно. При этом в отчете показано, что для противодействия ВПО необходимо использовать комплексный подход, состоящий из применения специализированных средств защиты информации для детектирования и удаления ВПО и из реализации мер по разграничению доступа и настройке активов с учетом требований по безопасности для снижения потерь при компрометации активов.

Согласно отчету Positive Technologies [18], активность программ-вымогателей значительно возросла в 1-м квартале 2023 г.: доля программ-вымогателей в атаках вредоносных программ на организации составила 53%, что на 9% больше, чем в предыдущем квартале, а количество инцидентов увеличи-

лось на 77% по сравнению с 1-м кварталом 2022 г. Основные мотивы злоумышленников – кража конфиденциальной информации и нарушения или остановка основной деятельности организаций.

Тем не менее ряд организаций не реализует эффективные методы защиты от киберугроз или использует реализованные методы неэффективно [19–23].

**Постановка задачи**

Для противодействия ВПО, включая программы-шифровальщики, применяются 2 типа методов:

1) применение антивирусных программ, призванных детектировать и удалять ВПО до того, как оно будет выполнено и будет нанесен ущерб. Данный метод постоянно развивается и совершенствуется [24–29];

2) применение политик разграничения доступа и настроек технических средств с учетом требований по безопасности с целью минимизации ущерба от реализованных программ-шифровальщиков [17].

Целью данного исследования является оценка эффективности встроенных средств защиты информации операционных систем семейства Unix, реализующих политики разграничения доступа в системе. Учитывая факт наличия санкций со стороны заграничных коммерческих организаций, реализующих операционные системы, а также политику импортозамещения в Российской Федерации, при которой субъекты КИИ обязаны перейти на отечественные операционные системы, которые, в свою очередь, принадлежат семейству Unix, исследование эффективности встроенных средств защиты информации противодействию ВПО представляет наибольший интерес в рассматриваемом случае.

При таком подходе рассмотрим встроенные средства и методы защиты информации операционных систем и оценим их эффективность по следующим параметрам:

– скорость заражения файловой системы ОС;

– процент заражения файловой системы ОС;

– сохранение работоспособности ОС.

**Описание объекта исследования**

Объект исследования – механизмы разграничения доступа операционных систем (ОС) семейства Unix:

– Debian.

– Alt Linux.

– RedOS.

– Astra Linux Special Edition.

При этом под доступом в данной работе понимается наличие прав на изменение объектов системы.

Механизмы разграничения доступа, применяемые в рассматриваемых ОС, можно разделить на 2 категории:

– механизм дискреционного разграничения доступа. Данный механизм работает по принципу точечного назначения прав доступа субъектов системы к объектам – пользователь имеет доступ к объекту, если он является суперпользователем или владельцем объекта, входит в группу пользователей, которым разрешен доступ к объекту, доступ к объекту разрешен всем пользователям системы:

$$R_{\mathrm{d}} = \begin{cases} 1, P \Leftrightarrow P_{\mathrm{s}} \bigcup P \Leftrightarrow P_{\mathrm{o}} \bigcup P \Leftrightarrow P_{\mathrm{g}} \bigcup P \Leftrightarrow P_{\mathrm{ot}}, \\ 0, \end{cases} \quad (1)$$

где $R_{\mathrm{d}}$ – дискреционные права доступа субъекта системы; $P$ – пользователь системы, $P_{\mathrm{s}}$ – суперпользователь системы, $P_{\mathrm{o}}$ – владелец объекта системы, $P_g$ – группа пользователей системы, $P_{\mathrm{ot}}$ – остальные пользователи системы;

– механизм мандатного разграничения доступа. Данный принцип работает по принципу разделения объектов и субъектов системы на разные группы иерархически или неиерархически.

Иерархический принцип подразумевает назначение специальных меток в числовом виде (мандатных меток), и доступ назначается на основании результата сравнения меток.

$$R_{\mathrm{mh}} = \begin{cases} 1, M_{\mathrm{s}} \geq M_{\mathrm{o}}, \\ 0, M_{\mathrm{s}} < M_{\mathrm{o}}, \end{cases} \quad (2)$$

где $M_{\mathrm{s}}$ – мандатная метка субъекта системы (пользователя), $M_{\mathrm{o}}$ – мандатная метка объекта системы, $R_{\mathrm{mh}}$ – иерархические мандатные права доступа субъекта системы. При $R_{\mathrm{mh}} = 0$ пользователь не имеет доступа к объекту системы, а при $R_{\mathrm{mh}} = 1$ – имеет.

Неиерархический метод подразумевает разделение субъектов и объектов системы на специальные категории (мандатные категории). Субъекты имеют доступ к объектам только в рамках одной категории:

$$R_{\mathrm{mnh}} = \begin{cases} 1, K_{\mathrm{s}} \Leftrightarrow K_{\mathrm{o}}, \\ 0, \end{cases} \quad (3)$$

где $K_s$ – мандатная категория субъекта системы, $K_o$ – мандатная категория объекта системы, $R_{\mathrm{mnh}}$ – неиерархические мандатные права доступа субъекта системы. При $R_{\mathrm{mnh}} = 0$ пользователь не имеет доступа к объекту системы, а при $\mathrm{R}_{\mathrm{mnh}} = 1$ – имеет.

**Постановка эксперимента**

Метод исследования – наблюдение за распространением программы-шифровальщика по файловой системе ОС (ФС).

Особенности постановки эксперимента:

– программа-шифровальщик не содержит опциональный функционал, направленный на повышение привилегий или закрепление в системе;

– все ОС устанавливались на одинаковые аппаратные составляющие, поэтому далее не будет учитываться зависимость скорости шифрования от аппаратных особенностей ПК.

Исследуемые параметры:

1) скорость заражения файловой системы ОС – $U_{\text{шиф}}$:

$$U_{\text{шиф}} = \frac{V_{\text{шиф}}}{t_{\text{шиф}}}, \quad (4)$$

где $V_{\text{шиф}}$ – объем зашифрованных данных в Мбайт, $t_{\text{шиф}}$ – время, потраченное на шифрование данных в секундах;

2) процент заражения файловой системы ОС – $V_{\text{зар}}$:

$$V_{\text{зар}} = \frac{V_{\text{шиф}}}{V_{\text{общ}}} \times 100\%, \qquad (5)$$

где $V_{\text{шиф}}$ – объем зашифрованных данных в Мбайт, $V_{\text{общ}}$ – общий объем данных в Мбайт. При этом $V_{\text{шиф}} \subseteq V_{\text{общ}}$, а $V_{\text{общ}} \supseteq (F_{\text{крит}} \cup F_{\text{ч.крит}} \cup F_{\text{псев}})$, где $F_{\text{крит}}$ – множество разделов файловой системы ОС, критичных для работоспособности системы (разделы /bin, /sbin, /boot, /lib, /lib64, /etc), $F_{\text{ч.крит}}$ – множество разделов файловой системы ОС, шифрование которых приведет к незначительным нарушениям работоспособности системы или не приведет к нарушению работоспособности системы (/tmp, /home, /media, /mnt, /opt, /root, /srv), $F_{\text{псев}}$ – множество разделов файловой системы ОС, которые являются псевдофайловыми системами (/proc, /run, /sys, /dev);

– сохранение работоспособности ОС – $K$:

$$K = \begin{cases} 2, \ F_{\text{крит}} \subseteq V_{\text{шиф}}, \\ 1, \ (F_{\text{крит}} \not\subseteq V_{\text{шиф}}) \wedge (F_{\text{ч.крит}} \subseteq V_{\text{шиф}}), \\ 0, \ (F_{\text{крит}} \cup F_{\text{ч.крит}}) \not\subseteq V_{\text{шиф}}. \end{cases} \qquad (6)$$

Физический смысл данной формулы заключается в следующем: при значении, равном 0, целевая система полностью сохраняет работоспособность, при $K$, равном 1, система сохраняет работоспособность частично (часть прикладного программного обеспечения выходит из строя), а при $K$, равным 2, целевая система полностью теряет работоспособность.

**Результаты**

Рассмотрим два случая.

*Случай 1*. Программа-шифровальщик направлена на получение выкупа от пользователя (цель программы-шифровальщика – захватить пользовательские файлы, оставив систему работоспособной).

*Случай 2*. Программа-шифровальщик направлена на реализацию деструктивного воздействия на систему (цель программы-шифровальщика – нарушить или прекратить нормальное функционирование системы).

В случае 1 целью программы-шифровальщика будет являться каталог /home, который входит в множество $F_{\text{ч.крит}}$. В табл. 1 показаны результаты наблюдений над работой программы-шифровальщика в условиях функционирования ОС без встроенных средств защиты информации.

Таблица 1

**Работа программы-шифровальщика без встроенных СЗИ с шифрованием пользовательских каталогов**

| ОС | Наличие прав суперпользователя | Скорость шифрования, Мбит/с | Процент поражения ФС, % | Сохранение работоспособности ФС |
|---|---|---|---|---|
| Debian | Нет | 3,77 | 0,72 | 0 |
| | Есть | 31,52 | 17,26 | 1 |
| RedOS | Нет | 12,31 | 0,03 | 0 |
| | Есть | 41,96 | 2,66 | 1 |
| Astra Linux | Нет | 2,20 | 0,24 | 1 |
| | Есть | 66,77 | 24,16 | 1 |
| Alt Linux | Нет | 0,76 | 0,0044 | 0 |
| | Есть | 72,36 | 2,12 | 1 |

Из табл. 1 виден закономерный результат, что наличие прав суперпользователя при исполнении программы-шифровальщика приводит к более серьезным последствиям для системы – шифрование большего количества каталогов и нарушение работоспособности прикладного ПО. При этом во всех случаях цель программы-шифровальщика достигнута. Различия среди показателей скорости шифрования и процента поражения файловой системы обусловлены различным комплектом поставки ОС.

Далее рассмотрим работу программы-шифровальщика в таких же условиях, но при включенных встроенных средствах защиты (табл. 2).

Таблица 2

**Работа программы-шифровальщика со встроенными СЗИ с шифрованием пользовательских каталогов**

| ОС | Наличие прав суперпользователя | Скорость шифрования, Мбит/с | Процент поражения ФС, % | Сохранение работоспособности ФС |
|---|---|---|---|---|
| Debian | Нет | 3,77 | 0,72 | 0 |
| | Есть | 31,52 | 17,26 | 1 |
| RedOS | Нет | 11,58 | 0,03 | 0 |
| | Есть | 42,18 | 2,48 | 1 |
| Astra Linux | Нет | 0,06 | 0,007 | 0 |
| | Есть | 13,12 | 1,57 | 0 |
| Alt Linux | Нет | 0,76 | 0,0044 | 0 |
| | Есть | 72,36 | 2,12 | 1 |

Результат похож на предыдущий – цель программы-шифровальщика достигнута, однако в данном случае Astra Linux показал полное сохранение работоспособности прикладного ПО в любых условиях, что демонстрирует ограничение суперпользователя в правах.

Далее рассмотрим случай 2 в условиях функционирования ОС без встроенных средств защиты (табл. 3) и со встроенными средствами защиты (табл. 4).

Полученные данные также показывают критичность захвата учетной записи суперпользователя, а также демонстрируют способность ОС Astra Linux сохранять работоспособность системы даже при компрометации учетной записи суперпользователя.

Таблица 3

**Работа программы-шифровальщика без встроенных СЗИ с шифрованием всех каталогов**

| ОС | Наличие прав суперпользователя | Скорость шифрования, Мбит/с | Процент поражения ФС, % | Сохранение работоспособности ФС |
|---|---|---|---|---|
| Debian | Нет | 3,41 | 0,73 | 0 |
| | Есть | 31,22 | 18,31 | 2 |
| RedOS | Нет | 1,64 | 0,03 | 0 |
| | Есть | 36,13 | 3,64 | 2 |
| Astra Linux | Нет | 1,91 | 0,23 | 1 |
| | Есть | 63,84 | 25,67 | 2 |
| Alt Linux | Нет | 0,13 | 0,0044 | 0 |
| | Есть | 32,72 | 2,98 | 2 |

Таблица 4

**Работа программы-шифровальщика со встроенными СЗИ с шифрованием всех каталогов**

| ОС | Наличие прав суперпользователя | Скорость шифрования, Мбит/с | Процент поражения ФС, % | Сохранение работоспособности ФС |
|---|---|---|---|---|
| Debian | Нет | 3,41 | 0,73 | 0 |
| | Есть | 31,22 | 18,31 | 2 |
| RedOS | Нет | 1,65 | 0,03 | 0 |
| | Есть | 31,11 | 3,47 | 2 |
| Astra Linux | Нет | 0,06 | 0,007 | 0 |
| | Есть | 11,38 | 1,57 | 0 |
| Alt Linux | Нет | 0,13 | 0,0044 | 0 |
| | Есть | 32,72 | 2,98 | 2 |

**Заключение**

Ряд проведенных экспериментов показал несостоятельность встроенных средств защиты информации различных систем на базе Unix перед программами-шифровальщиками, целью которых является шифрование пользовательских файлов и требование выкупа за информацию. Для защиты от таких угроз необходимо использовать средства антивирусной защиты, EDR-решения и системы резервного копирования.

В случае если целью программы-шифровальщика является нарушение или прекращение работоспособности системы, то проведенные эксперименты показывают большую критичность учетной записи суперпользователя, а также высокую эффективность подхода, применяемого в ОС Astra Linux – ограничение прав суперпользователя.

*Литература*

1. Maniriho P. API-MalDetect: Automated malware detection framework for windows based on API calls and deep learning techniques / P. Maniriho, A.N. Mahmood, M.J.M. Chowdhury // Journal of Network and Computer Applications. – Amsterdam: Elsevier Ltd., 2023. – P. 1–18.

2. Jing C. Ensemble dynamic behavior detection method for adversarial malware / C. Jing, Y. Wu, C. Cui // Future Gener. Comput. Syst. – 2022. – No. 130. – P. 193–206.

3. Maniriho P. A study on malicious software behavior analysis and detection techniques: Taxonomy, current trends and challenges / P. Maniriho, A.N. Mahmood, M.J.M. Chowdhury // Future Gener. Comput. Syst. – 2022. – No. 130. – P. 1–18.

4. Лабутин Н.Г. Предотвращение проникновения вирусов-шифровальщиков в корпоративные информационные системы // Современные тенденции развития науки и технологий. – Белгород: ООО «Агентство перспективных научных исследований», 2017. – С. 113–115.

5. Байздренко Е.А. Информационные угрозы для малого бизнеса: вирусы-шифровальщики // Актуальные вопросы учета и управления в условиях информационной экономики. – Севастополь: ООО «Рибест», 2018. – С. 270–274.

6. Путивльская И.Ю. Анализ рынка вирусов шифровальщиков / И.Ю. Путивльская, А.О. Ткач // Наука и образование: отечественный и зарубежный опыт. – Белгород: ООО «ГиК», 2018. – С. 37–41.

7. Тепловодских А.Д. Аспекты защиты от вирусов-шифровальщиков / А.Д. Тепловодских, С.С. Зотов // Аллея науки. – 2017. – № 12. – С. 367–371.

8. Долматов М.П. Вирусы-шифровальщики / М.П. Долматов, К.А. Ярмош, В.Л. Склярук // Современные проблемы радиоэлектроники и телекоммуникаций. – 2018. – № 1. – С. 209.

9. Begovic K. Cryptographic ransomware encryption detection: Survey / K. Begovic, A. Al–Ali, Q. Malluhi // Computers & Security. – 2023. – № 132. – P. 1–16.

10. Berrueta E. Survey on Detection Techniques for Cryptographic Ransomware / E. Berrueta, D. Morato, E. Magana, M.A. Izal // IEEE Access. – 2016. – № 7. – P. 1–21.

11. Su D. Detecting Android locker–ransomware on Chinese social networks / D. Su, J. Liu, X. Wang, W. Wang // IEEE Access. – 2017. – P. 20381–20393 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/329769980_Detecting_Android_Locker-Ransomware_on_Chinese_Social_Networks (дата обращения: 12.10.2023).

12. Murali R. Evolving malware variants as antigens for antivirus systems / R. Murali, P. Thangavel, C.Sh. Velayutham // Expert Systems with Applications. – 2023. – № 226. – P. 1–15.

13. Dwan B. The computer virus – From there to here: An historical perspective // Computer Fraud & Security. – 2000. – № 12. – P. 13–16.

14. Mawgoud A.A. A malware obfuscation AI technique to evade antivirus detection in counter forensic domain Enabling AI applications in data science / A.A. Mawgoud, H.M. Rady, B.S. Tawfik // Springer. – 2021. – P. 597–615 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/344349230_A_Malware_Obfuscation_AI_Technique_to_Evade_Antivirus_Detection_in_Counter_Forensic_Domain (дата обращения: 12.10.2023).

15. The 2023 Global Ransomware Report [Электронный ресурс]. – Режим доступа: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf (дата обращения: 08.09.2023).

16. 2023 Mid-year cyber security report: report reveals 48 ransomware groups have breached over 2,200 victims [Электронный ресурс]. – Режим доступа: https://research.checkpoint.com/2023/2023-mid-year-cyber-security-report-report-reveals-48-ransomware-groups-have-breached-over-2200-victims/ (дата обращения: 08.09.2023).

17. Аналитический отчёт: техники, тактики и процедуры (TTPs) группировок шифровальщиков [Электронный ресурс]. – Режим доступа: https://go.kaspersky.com/rs/802-IJN-240/images/Report_Common%20TTPs%20of%20modern%20ransomware.pdf (дата обращения: 08.09.2023).

18. Cybersecurity threatscape: Q1 2023 [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q1/ (дата обращения: 08.09.2023).

19. Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model / L. Bekkers, S. van 't Hoff-de Goede, E. Misana-ter Huurne, Y. van Houten, R. Spithoven, E.R. Leukfeldt // Computers & Security. – 2023. – № 127. – P. 1–12.

20. Johns E. Cyber Security Breaches Survey 2021: Statistical Release. – 1 изд. – London: Department for Digital, Culture, Media and Sport. – 2021. – 66 p.

21. Rohn E. Explaining small business InfoSec posture using social theories / E. Rohn, G. Sabari, G. Leshem // Inform. Comput. Secur. – 2016. – No. 24 (5). – P. 434–556.

22. Osborn E. Risk and the small-scale cyber security decision making dialogue – a UK case study / E. Osborn, A. Simpson // Comput. J. – 2018. – No. 61 (4). – P. 472–495.

23. Van der Kleij R. Cyber resilient behavior: integrating human behavioral models and resilience engineering capabilities into cyber security / R. Van der Kleij, R. Leukfeldt // International Conference on Applied Human Factors and Ergono-

mics. – 2019. – P. 16–27 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/3336455 50_Cyber_Resilient_Behavior_Integrating_Human_Behavioral_Models_and_Resilience_Engineering_Capabilities_into_Cyber_Security (дата обращения: 12.10.2023)

24. Vashishtha L.K. An Ensemble approach for advance malware memory analysis using Image classification techniques / L.K. Vashishtha, K. Chatterjee, S.S. Rout // Journal of Information Security and Applications. – 2023. – No. 77. – P. 1–14.

25. Bozkir A.S. Utilization and comparision of convolutional neural networks in malware recognition / A.S. Bozkir, A.O. Cankaya, M. Aydos // 27th signal processing and communications applications conference. – 2019. – P. 1–4.

26. MaleVis dataset home page [Электронный ресурс]. – Режим доступа: https://web.cs.hacettepe.edu.tr/~selman/malevis/ (дата обращения: 12.10.2023).

27. A forensic analysis of android malware-how is malware written and how it could be detected? / K. Allix, Q. Jérome, T.F. Bissyandé, J. Klein, R. State, Y. Le Traon // IEEE 38th annual computer software and applications conference. – 2014. – P. 384–393.

28. Rathnayaka C. An efficient approach for advanced malware analysis using memory forensic technique / C. Rathnayaka, A. Jamdagni // IEEE Trustcom/BigDataSE/ICESS. – 2017. – P. 1145–1150.

29. Volatile memory analysis using the MinHash method for efficient and secured detection of malware in private cloud / N. Nissim, O. Lahav, A. Cohen, Y. Elovici, L. Rokach // Computers & Security. – 2019. – No. 87. – P. 1–20.

---

**Огнев Игорь Александрович**
Аспирант, ассистент каф. защиты информации (ЗИ)
Новосибирского государственного технического университета (НГТУ)
К. Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0003-3884-7170
Тел.: +7-999-465-77-31
Эл. почта: i.ognev.2016@corp.nstu.ru

**Никрошкин Иван Владимирович**
Аспирант, ассистент каф. защиты информации ЗИ НГТУ
К. Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0003-4824-7419
Тел.: +7-996-377-90-71
Эл. почта: i.nikroshkin@corp.nstu.ru

**Медведев Михаил Александрович**
Аспирант, ассистент каф. защиты информации ЗИ НГТУ
К. Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0001-7674-9964
Тел.: +7-923-148-20-85
Эл. почта: m.medvedev@corp.nstu.ru

**Красников Артем Дмитриевич**
Лаборант инжинирингового центра
«Информационная безопасность» (ИЦ ИБ) НГТУ
К. Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0009-0002-4437-9764
Тел.: +7-913-986 6199
Эл. почта: player7004@yandex.ru

Ognev I.A., Nikroshkin I.V.,
Medvedev M.A., Krasnikov A.D.

**Study of built-in information protection tools of Unix systems on the example of malware infection**

This article provides a comparative analysis of the built-in information protection tools of the Unix family operating systems using the example of malware infection of the operating system. The study involved open-source operating systems – Debian, and domestic operating systems – Alt Linux, RedOS, Astra Linux Special Edition. A ransomware virus was used as a malicious software. The presented results demonstrate the greatest ability of the Astra Linux operating system to resist malware infection.

**Keywords:** information security, information protection, malicious software, virus, ransomware, operating system, information protection tool.
**DOI:** 10.21293/1818-0442-2023-26-4-29-34

*References*

1. Maniriho P. API-MalDetect: Automated malware detection framework for windows based on API calls and deep learning techniques / P. Maniriho, A.N. Mahmood, M.J.M. Chowdhury // *Journal of Network and Computer Applications*. Amsterdam: Elsevier Ltd, 2023, pp. 1–18.

2. Jing C. Ensemble dynamic behavior detection method for adversarial malware / C. Jing, Y. Wu, C. Cui // *Future Generation Computer Systems*, 2022, no. 130, pp. 193–206.

3. Maniriho P. A study on malicious software behavior analysis and detection techniques: Taxonomy, current trends and challenges / P. Maniriho, A.N. Mahmood, M.J.M. Chowdhury // *Future Generation Computer Systems*, 2022, no. 130, pp. 1–18.

4. Labutin N.G. [Preventing ransomware from penetrating corporate information systems] // *Current trends in the development of science and technology*. Belgorod: Limited Liability Company «Agency for Advanced Scientific Research», 2017, pp. 113–115 (in Russ.)

5. Baizdrenko E.A. [Information Threats to Small Businesses: Ransomware] // *Topical Issues of Accounting and Management in the Information Economy*. Sevastopol: OOO «Ribest», 2018, pp. 270–274 (in Russ.)

6. Putivlskaya I.Y. [Market analysis of ransomware viruses] / I.Y. Putivlskaya, A.O. Tkach // *Science and Education: Domestic and Foreign Experience*. Belgorod: OOO GiK, 2018, pp. 37–41 (in Russ.)

7. Teplovodskikh A.D. [Aspects of protection against ransomware] / A.D. Teplovodskikh, S.S. Zotov // *Alley of Science*, 2017, no. 12, pp. 367–371 (in Russ.)

8. Dolmatov M.P. [Ransomware viruses] / M.P. Dolmatov, K.A. Yarmosh, V.L. Sklyaruk // *Modern Problems of Radio Electronics and Telecommunications*, 2018, no. 1, 209 p. (in Russ.)

9. Begovic K. Cryptographic ransomware encryption detection: Survey / K. Begovic, A. Al-Ali, Q. Malluhi // *Computers & Security*, 2023, no. 132, pp. 1–16.

10. Berrueta E. Survey on Detection Techniques for Cryptographic Ransomware / E. Berrueta, D. Morato, E. Magana, M.A. Izal // *IEEE Access*, 2016, no. 7, pp. 1–21.

11. Su D. Detecting Android locker-ransomware on Chinese social networks / D. Su, J. Liu, X. Wang, W. Wang // *IEEE Access*. 2017. pp. 20381–20393. Available at: https://www.researchgate.net/publication/329769980_Detecting_Android_Locker-Ransomware_on_Chinese_Social_Networks (Accessed: October 12, 2023).

12. Murali R. Evolving malware variants as antigens for antivirus systems / R. Murali, P. Thangavel, C. Sh. Velayutham // *Expert Systems with Applications*, 2023, no. 226, pp. 1–15.

13. Dwan B. The computer virus – From there to here: An historical perspective //*Computer Fraud & Security*, 2000, no. 12, pp. 13–16.

14. Mawgoud A.A. A malware obfuscation AI technique to evade antivirus detection in counter forensic domain Enabling AI applications in data science / A.A. Mawgoud, H.M. Rady, B.S. Tawfik // Springer, 2021, pp. 597–615. Available at: https://www.researchgate.net/publication/344349230_A_Malware_Obfuscation_AI_Technique_to_Evade_Antivirus_Detection_in_Counter_Forensic_Domain (Accessed: October 12, 2023)

15. The 2023 Global Ransomware Report. Available at: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf (Accessed: September 08, 2023).

16. 2023 Mid-year cyber security report: report reveals 48 ransomware groups have breached over 2,200 victims. Available at: https://research.checkpoint.com/2023/2023-mid-year-cyber-security-report-report-reveals-48-ransomware-groups-have-breached-over-2200-victims/ (Accessed: September 08, 2023).

17. Analyst Report: Techniques, Tactics, and Procedures (TTPs) of Ransomware Groups (in Russ.). Available at: https://go.kaspersky.com/rs/802-IJN-240/images/Report_Common%20TTPs%20of%20modern%20ransomware.pdf (Accessed: September 08, 2023).

18. Cybersecurity threatscape: Q1 2023 (in Russ.). Available at: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q1/ (Accessed: September 08, 2023).

19. Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model / L. Bekkers, S. van 't Hoff-de Goede, E. Misana-ter Huurne, Y. van Houten, R. Spithoven, E.R. Leukfeldt // *Computers & Security*, 2023, no. 127, pp. 1–12.

20. E. Johns Cyber Security Breaches Survey 2021: Statistical Release. 1 ed. London: Department for Digital, Culture, Media and Sport, 2021, 66 p.

21. Rohn E. Explaining small business InfoSec posture using social theories / E. Rohn, G. Sabari, G. Leshem // *Information and Computer Security*, 2016, no. 24, vol. 5, pp. 434–556.

22. Osborn E. Risk and the small-scale cyber security decision making dialogue – a UK case study / E. Osborn, A. Simpson // *Computer Journal*, 2018, no. 61, vol. 4, pp. 472–495.

23. R. Van der Kleij, R. Leukfeldt Cyber resilient behavior: integrating human behavioral models and resilience engineering capabilities into cyber security // *International Conference on Applied Human Factors and Ergonomics*, 2019, pp. 16–27. Available at: https://www.researchgate.net/publication/333645550_Cyber_Resilient_Behavior_Integrating_Human_Behavioral_Models_and_Resilience_Engineering_Capabilities_into_Cyber_Security (Accessed: October 12, 2023).

24. Vashishtha L.K. An Ensemble approach for advance malware memory analysis using Image classification techniques / L.K. Vashishtha, K. Chatterjee, S.S. Rout // *Journal of Information Security and Applications*, 2023, no. 77, pp. 1–14.

25. Bozkir A.S. Utilization and comparision of convolutional neural networks in malware recognition / A.S. Bozkir, A.O. Cankaya, M. Aydos // *27th Signal Processing and Communications Applications Conference*, 2019, pp. 1–4.

26. MaleVis dataset home page Available at: https://web.cs.hacettepe.edu.tr/~selman/malevis/ (Accessed: October 12, 2023).

27. A forensic analysis of android malware-how is malware written and how it could be detected? / K. Allix, Q. Jérome, T.F. Bissyandé, J. Klein, R. State, Y. Le Traon // *IEEE 38th Annual Computer Software and Applications Conference*, 2014, pp. 384–393.

28. Rathnayaka C. An efficient approach for advanced malware analysis using memory forensic technique / C. Rathnayaka, A. Jamdagni // *IEEE Trustcom/BigDataSE/ICESS*, 2017, pp. 1145–1150.

29. Volatile memory analysis using the MinHash method for efficient and secured detection of malware in private cloud / N. Nissim, O. Lahav, A. Cohen, Y. Elovici, L. Rokach // *Computers & Security*, 2019, no. 87, pp. 1–20.

---

**Igor A. Ognev**
Postgraduate student, assistant
Information Security Department (IS),
Novosibirsk State Technical University (NSTU)
20, K. Marks pr., Novosibirsk, Russia, 630073
ORCID: 0000-0003-3884-7170
Phone: +7-999-465-77-31
Email: i.ognev.2016@corp.nstu.ru

**Ivan V. Nikroshkin**
Postgraduate student, assistant IS NSTU
20, K. Marks pr., Novosibirsk, Russia, 630073
ORCID: 0000-0003-4824-7419
Phone: +7-996-377-90-71
Email: i.nikroshkin@corp.nstu.ru

**Mikhail A. Medvedev**
Postgraduate student, assistant IS NSTU
20, K. Marks pr., Novosibirsk, Russia, 630073
ORCID: 0000-0001-7674-9964
Phone: +7-923-148-20-85
Email: m.medvedev@corp.nstu.ru

**Artyom D. Krasnikov**
Laboratory Assistant, engineering Center
«Information Security» (IC IS), NSTU
20, K. Marks pr., Novosibirsk, Russia, 630073
ORCID: 0009-0002-4437-9764
Phone: +7-913-986-61-99
Email: player7004@yandex.ru

УДК 004.052.31

**В.Е. Гвоздев, М.Б. Гузаиров, А.С. Давлиева, Р.Р. Галимов**

# Оценка характеристик информационной безопасности радиосети MANET на основе анализа топологий связей

Топологические особенности распределенных инфокоммуникационных сетей относятся к ключевым факторам, определяющим их свойства: стабильность, надежность и устойчивость к отказам и атакам. Исследование влияния топологии связей в Mobile ad hoc network как составной части инфраструктуры вычислительно-коммуникационных систем относится к приоритетным задачам в рамках проблемы обеспечения эффективного и результативного сетецентрического управления. Показаны результаты исследования, целью которого было оценивание эффективности разных методов выявления характера тенденций в случае коротких временных рядов.

**Ключевые слова:** информационная безопасность, сетецентрическое управление, надежность, эффективность, тенденция, топология связей, компонент, статистические индексы.

**DOI:** 10.21293/1818-0442-2023-26-4-35-43

Результативность и эффективность сложных распределенных субъектоцентрических систем сетецентрического управления в значительной степени определяются функционированием объединений стационарных и мобильных информационных инфраструктур, производящих критически важные для потребителей продукты и услуги. Следствием сложных, часто не выявленных взаимосвязей явлений и процессов как внутри сложных систем, так и с внешней средой, отказов / сбоев аппаратных и программных компонентов, ошибок людей, дефектов в построении организационных систем, внешних злонамеренных воздействий является возникновение угроз и опасностей разной природы, возникновением в системах неожиданных уязвимостей [1–6]. Это стимулирует разработку и развитие методов повышения информационной безопасности систем информационной поддержки сетецентрического управления на основе разноаспектного рассмотрения свойств инфраструктурных компонент.

Mobile ad hoc network (MANET) есть совокупность двух либо более беспроводных устройств, способных взаимодействовать друг с другом в условиях отсутствия централизованного управления. Каждый из узлов в беспроводной ad hoc network является одновременно хостом и маршрутизатором. Топология сети в общем случае является динамической в силу изменчивости связей между узлами по причине мобильности узлов, покидания сети одними узлами и подключением к сети новых узлов. Узел можно рассматривать как абстрактную сущность, состоящую из маршрутизатора и набора связанных мобильных хостов. Узлы также способны реагировать на изменения в топологии и на сбои в аффилированных узлах посредством оперативного изменения маршрутов.

Топологические особенности распределенных инфокоммуникационных сетей относятся к ключевым факторам, определяющим их свойства: стабильность; надежность и устойчивость к отказам и атакам.

В силу отмеченных обстоятельств исследование влияния топологии связей в MANET как составной части инфраструктуры вычислительно-коммуникационных систем относится к приоритетным задачам в рамках проблемы обеспечения эффективного и результативного сетецентрического управления.

**Особенности MANET как объекта информационной безопасности**

Ad hoc NETwork (MANET) есть автономная система мобильных хостов, взаимодействующих через беспроводные связи, в совокупности формирующие коммуникационную сеть. Особенностями MANET являются следующие:

1. Все узлы способны перемещаться и могут образовывать без участия человека случайным образом динамические объединения (изменять топологию связей) как реакции на внешние и внутренние события.

2. В силу того, что связь является беспроводной, зоны распространения сигналов от узлов-отправителей ограничены. Поэтому возможна ситуация, когда узел назначения находится вне зоны непосредственного доступа узла-отправителя. В силу этого передача осуществляется через промежуточные узлы, т.е. по маршрутам. Особенностью маршрутизации в MANET является возможность присутствия в таблицах маршрутизации устаревшей информации, что обусловлено изменениями топологии сети вследствие перемещения узлов; возникновения новых связей / разрыва существующих связей.

3. Инфокоммуникационные компоненты MANET являются гетерогенными, что обусловлено составом и количеством ресурсов в разных узлах сети; асимметричностью связей между узлами; различиями в характеристиках связей передающих и принимающих узлов; изменением величины накладных расходов на обеспечение взаимодействия вследствие мобильности узлов.

4. Каждый из хостов способен производить, потреблять данные, направлять, отправлять и продвигать пакеты от других узлов, т.е. выполнять функции маршрутизатора. Узлы должны совместными усилиями создавать сети и управлять ими в условиях отсутствия централизованного органа управления.

5. Подходы к управлению состоянием MANET в отличие от стационарных сетей (infrastructure-based network) [7] зависят от текущих характеристик сети, в том числе от состояния источников питания (бата-

рей) узлов. Беспроводные каналы связи имеют значительно меньшую пропускную способность, чем сети с проводными соединениями. Реализованная пропускная способность беспроводной связи в условиях множественного доступа с учетом затухания, шумов и помех часто оказывается значительно ниже чем максимальная скорость передачи радиосигнала.

6. В силу динамического характера и заранее неопределенного состава сети к ней возможно подключение вредоносных узлов. Мобильные беспроводные сети обычно более подвержены физическим угрозам безопасности, чем стационарные кабельные сети. Возрастает возможность прослушивания и спуфинга (подмены), а также атак, следствием которых является отказ в обслуживании.

**Характеристики надежности MANET**

Надежность, наряду с устойчивостью, живучестью и уязвимостью, тесно связана с информационной безопасностью [8–10]. Надежность (reliability) является метрической характеристикой степени уверенности в том, что система реализует поставленную задачу [11]. Надежность является латентной системной характеристикой. Определение содержания этого понятия предполагает многоаспектное рассмотрение, во-первых, с точки зрения возможности обеспечения системой информационных потребностей пользователя. В рамках этой точки зрения предполагается соответствие свойств системы широкому диапазону требований пользователя. Во-вторых, с точки зрения возможности возникновения в системе отказов. В рамках этой точки зрения базовым вопросом является определение содержания понятия «отказ» на основе знаний о функциях системы.

Причинами, осложняющими определение понятия «отказ», являются следующие:

– содержание понятия в рамках исследования аппаратной инфраструктуры осложняется оценкой влияния нарушения работоспособности отдельных устройств на свойства сети в целом: нарушение работоспособности одного устройства может оказаться фатальным для системы; нарушение работоспособности другого приведет лишь к незначительной задержке в передаче сообщений;

– помимо точек зрения, ориентированных на исследование аппаратных компонентов, при оценке надежности инфокоммуникационных систем следует учитывать то, что ценность информационных сервисов с точки зрения пользователя в том числе определяется надежностью данных.

Динамическое изменение как внутреннего состояния MANET, так и внешней среды, в которой функционирует система, является не только причиной изменения содержания понятия «отказ», но и изменением состава и степени влияния разных факторов, приводящих к отказу аппаратных компонент и активизации латентных дефектов в программных продуктах, а также препятствующих доступности информации.

В [12] описан подход к оценке надежности сетевых структур на основе анализа топологии связей. Как упоминалось выше, надежность является системной характеристикой и, в зависимости от точки зрения на систему, допускает множество толкований (что является реализацией тезиса о множественности точек зрения на сложный объект, что соответствует архитектурному подходу, и предписывает учитывать многомерный характер отношений между компонентами сложной системы [13]).

В рамках сетецентрической концепции [14] повышение качества информационного взаимодействия между компонентами сети направлено в том числе на повышение плотности связности элементов, возможности интенсивного информационного обмена.

Связи в топологических структурах являются унифицированным инструментом описания физической и информационной областей сетецентрической среды, компонентой которой является MANET.

С формальной точки зрения MANET на *j*-м отрезке времени может быть поставлен в соответствие граф $(V_j, O_j)$, где $V_j$ – узлы графа; $O_j$ – связи между узлами на *j*-м отрезке времени. В рамках архитектурного подхода к исследованию сложным систем [13] MANET может характеризоваться множеством графов $\{(V_j^{(k)}, O_j^{(k)})\}$, где $k$ – идентификатор точки зрения на MANET.

Мобильные системы имеют возможность взаимодействовать с другими локальными информационными системами, а также с Internet. Считается, что в MANET в качестве точки сочленения в каждый момент времени выступает один из хостов. При этом сторонние информационные системы взаимодействуют со всеми хостами мобильной системы через хост, играющий роль точки сопряжения [15].

В настоящей работе постулируется положение о том, что надежность связей между хостами (при разном толковании содержания связей) определяет такие свойства безопасности мобильных систем, как доступность; уязвимость; доступность; конфиденциальность; устойчивость.

Следуя [12] в качестве метрики надежности, определяемой на основе топологии связей, используется

$$B = \frac{\sigma}{N(N-1)}, \qquad (1)$$

где $N$ – количество узлов графа; σ рассчитывается по правилу

$$\sigma = \sum_{i=1}^{N} k_i,$$

где $k_i = 0$, если *i*-й узел является точкой сочленения, $k_i = p_i$ – степень *i*-го узла.

В [12] показано, что использование упомянутой метрики позволяет поставить сетевой структуре метрическую характеристику, значения которой лежат в диапазоне $B \in (0;1]$, причем наибольшее значение B соответствует полносвязным графам. Там же отмечается, что существует прямая зависимость между характеристикой надежности сети и её устойчивостью

к сбоям и отказам узловых компьютеров и каналов связи.

Квантификация свойств системы на основе анализа топологии связей является формальным аппаратом представления свойств MANET, определяемых влиянием различных факторов: наличием физических каналов приема-передачи сведений; протоколами маршрутизации; состоянием батарей; работоспособностью аппаратных компонент хостов; наличием и доступностью в разных хостах требуемых данных и информации; злонамеренных внешних воздействий и внутренних нарушителей [16] и т.д. Использование оценок надежности связей, имеющих в рамках разных точек зрения различное толкование, обеспечивает сопоставимость свойств, получаемых в рамках разных точек зрения на MANET. Это, в свою очередь, делает возможным использование для построения оценок интегральных характеристик безопасности известных методов выявления тенденций; аппарата порядковых статистик; статистических индексов; лингвистических переменных.

**Оценка тенденций изменения информационной безопасности MANET на основе статистических индексов**

Мониторинг состояния компьютерных сетей является одной из задач обнаружения и противодействия нарушениям и компьютерным атакам [16]. Результатом внешних и внутренних негативных воздействий является, например, уменьшение пропускной способности канала ниже допустимого уровня, что формально может быть представлено как разрушение связей между хостами. Своевременная идентификация негативных изменений состояния мобильных систем создает основу для реализации деятельности, направленной на обнаружение актуальных источников угроз безопасности информации.

Считается, что сокращение времени выявления негативных тенденций изменения информационной безопасности является критически важным фактором с точки зрения обеспечения своевременных реакций на причины, влияющие на состояние системы. Это обусловливает выделение областей применимости методов оценивания характера тенденций, в том числе при малом числе компонент временного ряда. В рамках настоящего исследования полагается, что в значениях показателей надежности связей помимо систематической (обусловленной актуальными источниками опасности) составляющей присутствуют случайные, обусловленные особенностями рельефа, отказами и восстановлением оборудования.

**Формальная постановка задачи**

Имеются эмпирические исторические данные о наличии / отсутствии связей между хостами в различные моменты времени. По результатам оценки показателей надежности связей (например, характеризующих доступность информации), требуется оценить тенденцию изменения показателей. Дадим, следуя [16], содержательное толкование тенденциям разного вида.

Отрицательная тенденция сигнализирует о низком уровне защищенности системы, т.е. при появлении дополнительных угроз безопасности информации в отношении них не могут быть с высокой оперативностью приняты меры защиты информации, нейтрализующие эти угрозы.

Положительная тенденция соответствует высокому уровню защищенности, что означает: «…при появлении дополнительных угроз безопасности они с высокой степенью оперативности могут быть нейтрализованы…».

Отсутствие тенденции соответствует среднему уровню защищенности, что означает тому, что если в ходе эксплуатации информационной системы появились дополнительные угрозы безопасности информации, и в их отношении могут быть приняты меры защиты информации, нейтрализующие эти угрозы за время, приемлемое с точки зрения особенностей задач управления, поддерживаемых информационной системой.

Комплексный анализ информационной безопасности предполагает многоаспектное изучение свойств MANET. Каждой точке зрения ставится в соответствие топологическая структура. При этом единицы измерения разных характеристик различны.

Преобразование изначально несопоставимых характеристик к безразмерному виду на основании (1), постулируя взаимную независимость характеристик и полагая, что разные характеристики безопасности фиксируются в одни и те же интервалы времени, делает возможным формирование на основе временных рядов комплексных показателей информационной безопасности, например, в виде средних индексов.

Известны разные методы выявления тенденций, основанные на анализе качественных и количественных характеристик временных рядов. Особенностью задачи обеспечения информационной безопасности мобильных систем является необходимость оперативного реагирования на негативные изменения их состояния. Это обусловливает целесообразность использования методов, позволяющих объективно оценивать характер тенденции по малому числу измерений.

В ходе проведения исследований выполнялся следующий статистический эксперимент, целью которого было оценивание эффективности разных методов выявления характера тенденций в случае коротких временных рядов.

В случае оценки наличия отрицательной тенденции посредством датчиков случайных чисел в разных временных срезах генерировалось одно равномерно распределенное число

$$b(T_i) = 1 - a \cdot T_i, \quad (i = \overline{1;n}),$$

где $T_i$ – значение временного ряда; $a$ – характеристика скорости уменьшения показателя надежности.

Эксперимент повторялся 1 000 раз, причем в каждом из экспериментов оценивалась правильность идентификации наличия отрицательной тенденции, а также отсутствия тенденции. На рис. 1 показаны зависимости оценки эффективности разных методов в

виде доли правильных оценок характера тенденции от объема временного ряда *n* при различных *a*.

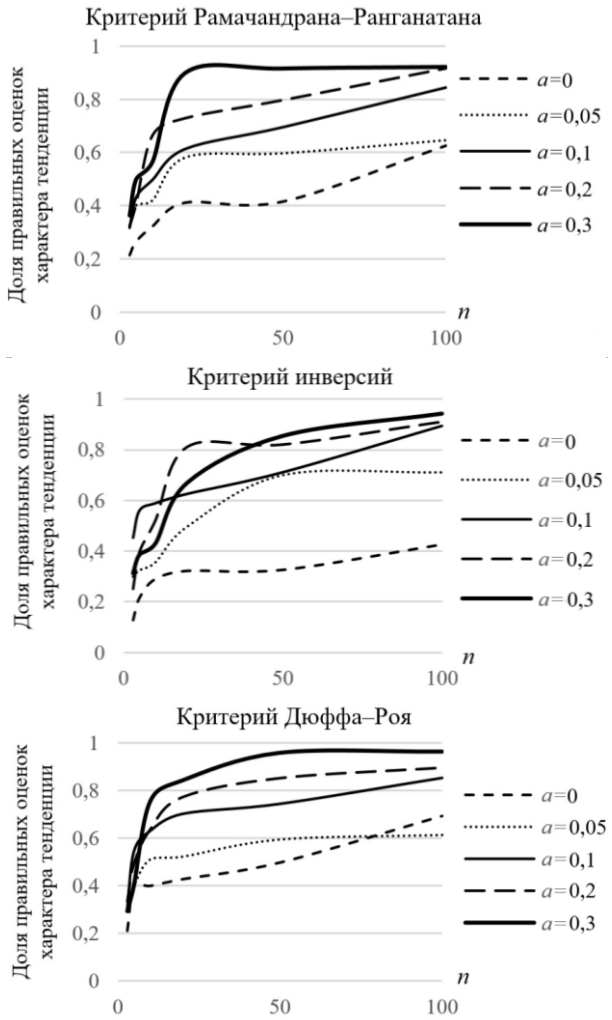



Рис. 1. Зависимости оценки эффективности разных методов в виде доли правильных оценок характера тенденции от объема временного ряда *n* при различных *a*

В работе рассматривались три критерия для выявления тенденции. Критерий Рамачандрана–Ранганатана является непараметрическим и учитывает не только количество серий временного ряда $T_1, T_2, .., T_n$, но и их длины, где одна серия – это ситуация $T_i \geq \tilde{T}$, а вторая – $T_i < \tilde{T}$. Особенность критерия состоит в том, что в случае больших объемах ряда гипотеза о случайности опровергается. Критерий инверсий предполагает наличие появления за значениями $T_i$ временного ряда таких значений, являющихся меньшими по величине, т.е. $T_i > T_j$, где $i < j \leq n$. Статистикой данного критерия является общее число инверсий во временном ряде, принимающее целое число [17]. Критерий Дюффа–Роя является модификацией критерия автокорреляции. При предположении о справедливости гипотезы о случайности и отсутствии тренда распределение статистики Дюффа–Роя быстро сходится к стандартному нормальному закону [17].

Таким образом, можно иметь более устойчивые результаты на уровне 70–80%, при условии, что чем сильнее тенденция, тем меньше данных необходимо, чтобы установить это.

Предлагаемый подход может составить основу принятия решений о периодичности контроля состояния MANET.

**Оценка устойчивости информационной безопасности на основе аппарата статистических индексов**

Анализ характера тенденций не позволяет оценить степень влияния разных факторов на изменение состояния системы. Поэтому в качестве самостоятельной задачи исследования, ориентированной на совершенствование свойств технических компонент информационной составляющей MANET, следует выделить задачи сопоставления характеристик информационной безопасности на основе данных, получаемых в разных условиях.

Ниже рассматривается использование аппарата статистических индексов для решения следующих задач:

а) оценка различия комплексных показателей информационной безопасности, полученных по результатам испытаний и данным эксплуатации;

б) оценка эффективности ресурсного обеспечения различных задач информационной безопасности;

в) оценка влияния структуры ресурсного обеспечения задач информационной безопасности на комплексный показатель информационной безопасности;

г) учета территориальных особенностей ситуаций, урегулирование которых обеспечивается мобильными системами различного состава и структуры.

Для решения выделенных задач используется аппарат статистических индексов, что позволяет сопоставлять свойства различных либо одинаковых по конструкции систем, соответствующих разным условиям исследования.

Рассмотрим способ обеспечения сопоставимости данных, получаемых в условиях динамично изменяющейся внешней среды. Изменчивость внешней среды проявляется как в различии длительности периодов наблюдения $T_j$, так и в числе регистрируемых значений разных характеристик информационной безопасности в течение *j*-го периода наблюдения $T_j$.

Основу формирования сопоставимых показателей составляет соотношение

$$Y_l(T_j) = \frac{1}{T_j} \int_{T_j} f(Y_l(t))dt,$$

где $f(Y_l(t))$ – оценка временной зависимости характеристики $Y_l(t)$, определяемая как кусочно-линейная аппроксимация по значениям узлов $\{t_q, Y_l(t_q)\}$, где $t_q$ – упорядоченные по возрастанию отметки вре-

мени $t_q \in T_j$, в которых регистрируются значения $l$-х характеристик $Y_l(t)$.

Такое преобразование позволяет сформировать таблицу вида

$$< j, Y_l(T_j) >, \quad l = \overline{1;L}, \quad j = \overline{1;J},$$

где $l$ – идентификатор характеристики информационной безопасности; $j$ – идентификатор временного интервала, которому соответствует $Y_l(t)$.

Построенная таблица служит исходными данными для расчета частных статистических индексов.

Рассмотрим содержание выделенных выше задач а–г.

а. Оценка показателей качества компонент распределенных систем информационного обеспечения предприятием-производителем осуществляется по данным специально организованных испытаний. Однако получение объективных оценок на основе специально организованных испытаний осложняется тем, что при испытаниях невозможно в полной мере воспроизвести условия реальной эксплуатации [18, 19]. Это осложняет вынесение обоснованных заключений практической пригодности физических компонент информационной подсистемы сетецентрической системы управления, а также о структуре ресурсного обеспечения различных видов работ, связанных с созданием физических компонент.

Тестирование соответствия является важным этапом жизненного цикла сложных инфокоммуникационных сетей. Важной составляющей тестирования соответствия свойств коммуникационных протоколов их спецификациям, а также других характеристик распределенных инфокоммуникационных систем является разработка и исполнение тестов.

Технологии испытания коммуникационных протоколов в MANET основаны на эмуляции и / или симуляции. При этом результаты симуляционного тестирования в ряде случаев оказываются достаточно далеки от результатов, получаемых в условиях эксплуатации [18–20].

В качестве инструмента решения задачи оценки степени различия комплексных показателей информационной безопасности, полученных по результатам испытаний и данным эксплуатации, предлагается использовать *индекс переменного состава* $I_{vc}$.

Индекс переменного состава рассчитывается по формуле

$$I_{vc} = \left( \frac{\sum_{j=1}^{m} y_1^{(j)} \cdot a_1^{(j)}}{\sum_{j=1}^{m} a_1^{(j)}} \right) / \left( \frac{\sum_{i=1}^{k} y_0^{(i)} \cdot a_0^{(i)}}{\sum_{i=1}^{k} a_0^{(i)}} \right). \qquad (2)$$

Здесь $y_0^{(i)}$ – значения $i$-х показателей информационной безопасности, определяемые по результатам специально организованных испытаний ($i$ = 1, ..., $k$); $y_1^{(j)}$ – значения $j$-х показателей информационной безопасности, определяемые в ходе эксплуатации ($j$ = 1, …, $m$); $a_0^{(i)}, a_1^{(j)}$ – весовые характеристики $i$-х и $j$-х показателей информационной безопасности, определяемые на основе топологий связей этих характеристик.

По сути (2) является средним индексом.

б. В [21] отмечается, что несбалансированность структуры бюджета проекта с требованиями к программному продукту является причиной низких потребительских свойств последних. В многочисленных литературных источниках (в частности, в [22]) подчеркивается, что свойства MANET в значительной степени определяются особенностями коммуникационных протоколов. В связи с этим можно выделить задачу сопоставления различных подходов к распределению ресурсов по видам работ проекта (WBS) по результатам испытания альтернативных вариантов протоколов.

В качестве инструмента решения задачи оценки эффективности ресурсного обеспечения решения разных классов задач информационной безопасности предлагается использовать *индекс постоянного состава* $I_{fc}$, характеризующий показатели информационной безопасности, полученные в результате испытаний, и соответствующие разным схемам распределения ресурсов. Рассчитывается по формуле

$$I_{fc} = \frac{\sum_{j=1}^{m} y_1^{(j)} \cdot a_1^{(j)}}{\sum_{j=1}^{m} y_0^{(j)} \cdot a_1^{(j)}}. \qquad (3)$$

Здесь $y_0^{(j)}$ – значения $j$-х показателей информационной безопасности в первом испытании ($j$ = 1, ..., $m$); $y_1^{(j)}$ – значения тех же показателей информационной безопасности, определяемые во втором испытании при измененной схеме распределения ресурсов; $a_1^{(j)}$ – весовые характеристики $j$-х показателей информационной безопасности, определяемые на основе топологий связей этих характеристик.

в. Управление информационной безопасностью предполагает решение взаимосвязанного комплекса задач на организационном, методическом, технологическом уровнях. В рамках ограниченных объемов ресурсов важной задачей является формирование сбалансированной структуры затрат на обеспечение информационной безопасности. В связи с этим в качестве самостоятельной задачи следует выделить оценку влияния структуры ресурсного обеспечения задач информационной безопасности на комплексный показатель информационной безопасности. В качестве инструмента решения задачи оценки влияния структуры ресурсного обеспечения задач информационной безопасности на комплексный показатель информационной безопасности может использоваться *индекс структурных сдвигов* $I_{ss}$, рассчитываемый по формуле

$$I_{ss} = \left( \frac{\sum_{j=1}^{m} y_0^{(j)} \cdot a_1^{(j)}}{\sum_{j=1}^{m} y_0^{(j)} \cdot a_0^{(j)}} \right) \Bigg/ \left( \frac{\sum_{j=1}^{m} a_1^{(j)}}{\sum_{j=1}^{m} a_0^{(j)}} \right), \qquad (4)$$

где $y_0^{(j)}$ – значения $j$-х показателей информационной безопасности в первой схеме распределения ресурсов ($j$ = 1, ..., $m$); $a_0^{(j)}, a_1^{(j)}$ – весовые характеристики $j$-х показателей информационной безопасности, определяемые на основе топологий связей этих характеристик при первой и второй схемах ресурсного обеспечения соответственно.

г. Устойчивость информационного сетевого взаимодействия в условиях динамически изменяющейся внешней среды является одним из базовых требований к системам информационного обеспечения сетецентрического управления [14]. MANET, при рассмотрении в рамках физической области, относится к классу технических систем с распределенными параметрами. В рамках этой точки зрения устойчивость является критически важным фактором безопасного функционирования MANET. Под устойчивостью понимается способность системы сопротивляться изменению своего состояния при различных воздействиях на нее [23, 24].

Особенностью сетецентрического управления является необходимость учета влияния территориальных особенностей ситуаций, урегулирование которых в том числе обеспечивается мобильными системами различного состава и структуры, при анализе информационной безопасности. Различие ситуаций и воздействий, испытываемых разными мобильными системами, находит отражение в топологических характеристиках показателей информационной безопасности. Для сопоставления уровней информационной безопасности, соответствующих разным участкам территории, могут использоваться индексы вида:

$$I_{A/B} = \frac{\sum_{j=1}^{m} y_1^{(j)} \cdot a_1^{(j)}}{\sum_{j=1}^{m} y_0^{(j)} \cdot a_1^{(j)}} \quad \text{и} \quad I_{fc} = \frac{\sum_{j=1}^{m} y_1^{(j)} \cdot a_0^{(j)}}{\sum_{j=1}^{m} y_0^{(j)} \cdot a_0^{(j)}}.$$

Здесь $I_{A/B}$ – индекс, в котором в качестве базы сравнения применяются данные за тот же период времени, соответствующие участку территории $A$; $I_{B/A}$ – индекс, используемый в качестве базы сравнения данных за тот же период времени соответствующие участку территории $B$; $y_0^{(j)}$ – значения $j$-х показателей информационной безопасности, определяемые на территории $A$; $y_1^{(j)}$ – значения $j$-х показателей информационной безопасности определяемые на территории $B$; $a_0^{(i)}, a_1^{(j)}$ – весовые характеристики показателей информационной безопасности, определяемые на основе топологий связей этих характеристик.

**Пример использования индекса структурных сдвигов**

В рамках проведения работ по обеспечению интероперабельности [25] инфокоммуникационных систем предложены две альтернативные архитектуры системы. В первой упор сделан на реактивный подход к обеспечению безопасности, основанный на выявлении и устранении латентных дефектов. Во второй – на превентивный подход, основанный на метафоре «Swiss Cheese Model» [26] и реализованный в рамках системной модели Anticipatory Failure Determination (AFD) [27].

По результатам испытания прототипов программных продуктов, в которых упор сделан на: эффективное восстановление работоспособности в случае проявления источников опасности (реактивный подход, AFD-1); предотвращение трансформации проявлений источника опасности в негативные последствия (превентивный подход, AFD-2), получены данные о характеристиках безопасности, соответствующие первой и второй архитектурам, при разном числе объектов в сети.

Требуется сформулировать предложения относительно направлений дальнейших работ по обеспечению функциональной безопасности программных компонент.

**Заключение**

В настоящей работе продемонстрировано использование аппарата статистических индексов применительно к задачам управления информационной безопасностью. Следует отметить, что идея использования статистических индексов в качестве интегральных характеристик сложных систем используется, например, в задачах экологической безопасности (индекс загрязнения атмосферы – ИЗА [28]; индекс загрязнения воды [29]). Ограничением рассмотренных выше формальных схем является линейная свертка индексов, соответствующих отдельным показателям информационной безопасности. Однако отмеченное ограничение не носит принципиального характера. В монографии [30] при описании метода обобщенного параметра приводится набор различных линейных и нелинейных сверток, предназначенных для формирования статистических индексов.

*Литература*

1. Baldwin K.J. Systems engineering guide for systems of systems. – Version 1.0. – Washington: Department of defense office of the deputy under secretary of defense for acquisition and technology, 2008. – 148 p.

2. Varshney U.S. Measuring the reliability and survivability of infrastructure-oriented wireless networks / U.S. Varshney, P.S. Andrew, A.D. Malloy // Local Computer Networks (LCN 2001), Florida, USA, 2001. – P. 611–618.

3. Bhaiji Y. Network security technologies and solutions // CCIE Professional Development, 2008. – 840 p.

4. Wireless local area network hits the public [Электронный ресурс]. – Режим доступа: http://www.touchbriefings.com/pdf/744/wire041_vis.pdf, свободный (дата обращения: 16.03.2011).

5. Westmark V.R. A definition for information system survivability // System Sciences. – 2004. – P. 1–10.

6. Сетецентрическое управление: современная парадигма развития систем управления в вооруженных силах ведущих держав мира / И.В. Сурма, В.И. Анненков, В.В. Карпов, А.В. Моисеев // Национальная безопасность. – 2014. – № 2(31). – С. 317–327.

7. Loo J. Mobile Ad hoc Networks: current status and future trends / J. Loo, J.L. Mauri, J.H. Ortiz // Auerbach publications, 2016. – 528 p.

8. ГОСТ 27.002–2015. Надежность в технике. Термины и определения. – 2016. – 23 с.

9. Ellison R.J. Survivable network systems: an emerging discipline / R.J. Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T. Longstaff, N.R. Mead // Technical report CMU/SEI-97-TR-013. – 1997 [Электронный ресурс]. – Режим доступа: https://resources.sei.cmu.edu/asset_files/TechnicalReport/1998_005_001_16598.pdf, свободный (дата обращения: 15.09.2023).

10. Mohsin Y. Communication and computer networks simulator (NS2) // Computer communications (Networks). – 2014. – 17 p.

11. Randell B. System reliability and structuring // Computing Systems Reliability. – Cambridge University Press, New York, USA. – 1979. – P. 1–18.

12. Тимофеев А.В. Адаптивное управление и интеллектуальный анализ информационных потоков в компьютерных сетях. – СПб.: ООО «Анатолия», 2012. – 280 с.

13. IEEE 1471–2000. Recommended Practice for Architecture Description of Software-Intensive Systems [Электронный ресурс]. – Режим доступа: http://cabibbo.dia.uniroma3.it/ids/altrui/ieee1471.pdf, свободный (дата обращения: 18.05.2021).

14. Макаренко С.И. Подавление сетецентрических систем управления радиоэлектронными информационно-техническими воздействиями // Системы управления, связи и безопасности. – 2017. – № 4. – С. 15–59.

15. Cordeiro C. Ad hoc & sensor networks: Theory and Applications / C. Cordeiro, D. Agrawal // World Scientific Publishing Co. Pte, 2006. – 663 p.

16. Методика определения угроз безопасности информации в информационных системах: метод. документ // ФСТЭК России. – 2021. – 43 с.

17. Лемешко Б.Ю. Критерии проверки гипотез о случайности и отсутствии тренда. Рук-во по применению: учеб. пособие / Б.Ю. Лемешко, И.В. Веретельникова. – Новосибирск, 2021. – 215 с.

18. Maag S. Model-Based Testing for MANETs // Труды ИСП РАН. – 2014. – Т. 26, вып. 6. – С. 31–44.

19. Lu Z. Unlocking the power of OPNET modeler / Z. Lu, H. Yang. – Cambridge University Press, 2012. – 238 p.

20. Salem A. Mobile Ad-hoc Network simulators, a survey and comparisons / A. Salem, H. Awwad // International journal of P2P network trends and technology (IJPTT). – 2014. – Vol. 4, Iss. 3. – P. 22–26.

21. Макконнелл С. Сколько стоит программный проект. – М.: Русская редакция; СПб.: Питер, 2007. – 297 с.

22. Bekmezci I. Flying Ad-Hoc Networks (FANETs): a survey / I. Bekmezci, O. Sahingoz, S. Temel // Ad Hoc Networks. – 2013. – Vol. 11. – P. 1254–1270.

23. Колесников А.А. Проблемы теории аналитического конструирования нелинейных регуляторов и синергетический подход // Синергетика и проблемы управления. – М.: ФИЗМАТЛИТ, 2004. – С. 35–129.

24. Gvozdev V.E. Ensuring the functional safety of the distributed dynamic systems components in the conditions of uncertainty of the environment use / V.E. Gvozdev, M.B. Guzairov, O.Ya. Bezhaeva, A.S. Davlieva, R.R. Galimov // Proceedings – ICOECS–2020: 2020 International Conference on Electrotechnical Complexes and Systems. – 2020. – P. 1–6.

25. ГОСТ 55062–2021. Информационные технологии. Интероперабельность. Основные положения. – 2021. – 12 с.

26. Revisiting the «Swiss Cheese» Model of Accidents // European Organization for the Safety of Air Navigation. – 2006. – No. 13/06. – 25 p.

27. Renan Favarão Da Silva, Marco Aurélio De Carvalho. Anticipatory Failure Determination (AFD) for product reliability analysis: A comparison between AFD and Failure Mode and Effects Analysis (FMEA) for identifying potential failure modes // Federal Technological University of Paraná (UTFPR). – Curitiba, Brazil, 2019. – 24 p.

28. Руководящий документ РД 52.04.6672005. Документы о состоянии загрязнения атмосферы в городах для информирования государственных органов, общественности и населения. Общие требования к разработке, построению, изложению и содержанию. – М.: Метеоагентство Росгидромета, 2006. – 50 с.

29. Глотова Н.В. Мониторинг среды обитания: учеб. пособие к практ. занятиям. – Челябинск: Изд-во ЮУрГУ, 2006. – 22 с.

30. Гаскаров Д.В. Прогнозирование технического состояния и надежности радиоэлектронной аппаратуры / Д.В. Гаскаров, Т.А. Голинкевич, А.В. Мозгалевский. – М.: Советское радио, 1974. – 224 с.

---

**Гвоздев Владимир Ефимович**
Д-р техн. наук, проф. каф. технической кибернетики
Уфимского университета науки и технологий (УУНиТ)
К. Маркса ул., 12, г. Уфа, Россия, 450008
ORCID: 0009-0004-8557-3445
Тел.: +7-908-350-35-63
Эл. почта: wega55@mail.ru

**Гузаиров Мурат Бакеевич**
Д-р техн. наук, проф.каф. управления информационной безопасностью УУНиТ
З. Валиди ул., 32, г. Уфа, Россия, 450076
Тел.: +7 (347-2) 29-97-51
Эл. почта: guzairovmb@uust.ru

**Давлиева Алия Салаватовна**
Канд. техн. наук, доцент
каф. технической кибернетики УУНиТ
К. Маркса ул., 12, г. Уфа, Россия, 450008
ORCID: 0000-0002-7548-2134
Тел.: +7-908-350-35-63
Эл. почта: davlieva.as@ugatu.su

**Галимов Роберт Ришатович**
Аспирант каф. технической кибернетики УУНиТ
К. Маркса ул., 12, г. Уфа, Россия, 450008
Тел.: +7-908-350-35-63
Эл. почта: rrgalimov@gmail.com

Gvozdev V.E., Guzairov M.B., Davlieva A.S., Galimov R.R.
**Evaluation of MANET information safety characteristics based on the analysis of link topologies**

Topological features of distributed infocommunication networks are among the key factors that determine their properties: stability, reliability and resistance to failures and attacks. The study of the communications topology influence in the Wireless Mobile ad hoc network, as an integral part of the infrastructure

of computing and communication systems, is one of the priority tasks when it comes to ensure the effective and efficient network-centric control. The paper presents the results of a study aiming to evaluate the efficiency of various methods used to identify the nature of trends in the case short time series.

**Keywords:** information safety, network-centric control, reliability, efficiency, trend, link topology, component, statistical indices.

**DOI:** 10.21293/1818-0442-2023-26-4-35-43

*References*

1. Baldwin K.J. *Systems engineering guide for systems of systems. Version* 1.0. Washington. Department of defense office of the deputy undersecretary of defense for acquisition and technology, 2008, 148 p.

2. Varshney U.S. Andrew P.S., Malloy A.D. Measuring the reliability and survivability of infrastructure-oriented wireless networks, Florida, USA. *Local Computer Networks (LCN 2001)*, 2001, pp. 611–618.

3. Bhaiji Y. Network security technologies and solutions. *CCIE Professional Development*, 2008. 840 p.

4. Wireless local area network hits the public. Available at http://www.touchbriefings.com/pdf/744/wire041_vis.pdf, free. (Accessed: March 16, 2011).

5. Westmark V.R. A definition for information system survivability. *System Sciences*, 2004, pp. 1–10.

6. Surma I.V., Annenkov V.I., Karpov V.V., Moiseev A.V. *Setecentricheskoe upravlenie: sovremennaya paradigma razvitiya sistem upravleniya v vooruzhennyh silah vedushchih derzhav mira* [Network-centric control: a modern paradigm for the development of control systems in the armed forces of the leading powers of the world]. *National Security*, 2014, no. 2 (31), pp. 317–327. (In Russ.).

7. Loo J. Mauri J.L., Ortiz J.H. Mobile Ad hoc Networks: current status and future trends. *Auerbach publications*, 2016, 528 p.

8. GOST 27.002-2015 *Nadezhnost' v tekhnike. Terminy i opredeleniya* [Reliability in engineering. Terms and definitions], 2016. 23 p. (In Russ.).

9. Ellison R.J., Fisher D.A., Linger R.C., Lipson H.F., Longstaff T., Mead N.R. Survivable network systems: an emerging discipline. *Technical report CMU/SEI-97-TR-013* 1997 Available at: https://resources.sei.cmu.edu/asset_files/TechnicalReport/1998_005_001_16598.pdf, free (Accessed: May 15, 1999).

10. Mohsin Y. Communication and computer networks simulator (NS2). *Computer Communications (Networks)*, 2014. 17 p.

11. Randell B. System reliability and structuring. Cambridge University Press. New York, USA. *Computing Systems Reliability*, 1979, pp. 1–18.

12. Timofeev A.V. *Adaptivnoye upravleniye i intellektualnyy analiz informatsionnykh potokov v kompyuternykh setyakh* [Adaptive control and intelligent analysis of information flows in computer networks]. St. Petersburg, LLC «Anatolia», 2012, 280 p. (in Russ.).

13. IEEE 1471–2000. Recommended Practice for Architecture Description of Software-Intensive Systems. Available at: http://cabibbo.dia.uniroma3.it/ids/altrui/ieee1471.pdf, free (Accessed: May 18, 2021).

14. Makarenko S.I. [Suppression of network-centric control systems by radio-electronic information and technical influences]. *Control Systems, Communications and Security*, 2017, no. 4, pp. 15–59 (in Russ.).

15. Cordeiro C. Agrawal D. Ad hoc & sensor networks: Theory and Applications. *World Scientific Publishing Co. Pte*, 2006, 663 p.

16. *Metodika opredeleniya ugroz bezopasnosti informatsii v informatsionnykh sistemakh: metodicheskiy dokument* [Methodology for determining information security threats in information systems: a methodological document]. FSTEC, Russia, 2021, 43 p. (in Russ.).

17. Lemeshko B.Yu., Veretelnikova I.V. *Kriterii proverki gipotez o sluchaynosti i otsutstvii trenda. Rukovodstvo po primeneniyu* [Criteria for testing hypotheses about randomness and the absence of a trend. Application guide: textbook]. Novosibirsk, 2021, 215 p. (in Russ.).

18. Maag S. Model-Based Testing for MANETs. *Russian Journal of Proceedings of the Institute for System Programming of the Russian Academy of Sciences*, 2014, vol. 26, iss. 6, pp. 31–44.

19. Lu Z., Yang H. Unlocking the power of OPNET modeler. *Cambridge University Press*, 2012, 238 p.

20. Salem A., Awwad H. Mobile Ad-hoc Network simulators, a survey and comparisons. *International journal of P2P network trends and technology (IJPTT)*, 2014, vol. 4, iss. 3, pp. 22–26.

21. McConnell C. *Skolko stoit programmnyy proyekt* [How much does a software project cost]. St. Petersburg: Peter, 2007, 297 p. (in Russ.).

22. Bekmezci I., Sahingoz O., Temel S. Flying Ad-Hoc Networks (FANETs): a survey. *Ad Hoc Networks*, 2013, vol. 11, pp. 1254–1270.

23. Kolesnikov A.A. *Problemy teorii analiticheskogo konstruirovaniya nelinejnyh regulyatorov i sinergeticheskij podhod* [Problems of the Theory of Analytical Design of Nonlinear Regulators and the Synergetic Approach]. *Synergetics and Control Problems*, 2004, pp. 35–129 (in Russ.).

24. Gvozdev V.E., Guzairov M.B., Bezhaeva O.Ya. Davlieva A.S., Galimov R.R. Ensuring the functional safety of the distributed dynamic systems components in the conditions of uncertainty of the environment use. *Proceedings – ICOECS 2020: 2020 International Conference on Electrotechnical Complexes and Systems*, 2020, pp. 1–6.

25. GOST 55062–202.1 *Informacionnye tekhnologii Interoperabel'nost'* [Osnovnye polozheniya Information technology Interoperability. Basic provisions], 2021, 12 p. (in Russ.).

26. Revisiting the «Swiss Cheese» Model of Accidents. *European Organization for the Safety of Air Navigation*, 2006, no. 13/06, pp. 1–25.

27. Renan Favarão Da Silva, Marco Aurélio De Carvalho. Anticipatory Failure Determination (AFD) for product reliability analysis: A comparison between AFD and Failure Mode and Effects Analysis (FMEA) for identifying potential failure modes. Curitiba, Brazil. *Federal Technological University of Paraná (UTFPR)*, 2019, 24 p.

28. Document RD 52.04.6672005. *Dokumenty o sostoyanii zagryazneniya atmosfery v gorodakh dlya informirovaniya gosudarstvennykh organov. obshchestvennosti i naseleniya. Obshchiye trebovaniya k razrabotke. postroyeniyu. izlozheniyu i soderzhaniyu* [Documents on the state of air pollution in cities to inform government agencies, the public and the population. General requirements for development, construction, presentation and content]. Meteo agency of Roshydromet, 2006, 50 p. (in Russ.)

29. Glotova N.V. *Monitoring sredy obitaniya* [Monitoring of the habitat: a textbook for practical exercises]. Chelyabinsk: Publishing house of YuUrGU, 2006, 22 p. (in Russ.).

30. Gaskarov D.V., Golinkevich T.A., Mozgalevsky A.V. *Prognozirovaniye tekhnicheskogo sostoyaniya i nadezhnosti radioelektronnoy apparatury* [Forecasting the technical condition and reliability of radio electronic equipment] Moscow. Soviet radio, 1974, 224 p. (in Russ.).

**Vladimir E. Gvozdev**
Doctor of Science in Engineering, Professor,
Department of Technical Cybernetics,
Ufa University of Science and Technology
12, K. Marx st., Ufa, Russia, 450008
ORCID: 0009-0004-8557-3445
Phone: +7-908-350-35-63
Email: wega55@mail.ru

**Murat B. Guzairov**
Doctor of Science in Engineering, Professor,
Department of Information Security Management
Ufa University of Science and Technology
12, K. Marx st., Ufa, Russia, 450008
Phone: +7 (347-2) 29-97-51
Email: guzairovmb@uust.ru

**Aliya S. Davlieva**
Candidate of Sciences in Engineering, Assistant Professor,
Department of Technical Cybernetics,
Ufa University of Science and Technology
32, Z. Validi st., Ufa, Russia, 450076
ORCID: 0000-0002-7548-2134
Phone: +7-908-350-35-63
Email: davlieva.as@ugatu.su

**Robert R. Galimov**
Postgraduate student, Department of Technical Cybernetics,
Ufa University of Science and Technology
12, K. Marx st., Ufa, Russia, 450008
Phone: +7-908-350-35-63
Email: rrgalimov@gmail.com

УДК 004.056

**А.А. Воробьева**

# Способ исследования устойчивости систем со встроенным искусственным интеллектом, использующихся на промышленных объектах, к состязательным атакам

Представлен способ исследования устойчивости систем со встроенным искусственным интеллектом (ИИ), использующихся на промышленных объектах, к состязательным атакам. Исследовано влияние состязательных атак на показатели работы систем, использующих модели машинного обучения (МО). Представлена разработанная обобщенная схема и определены сценарии реализации атак на системы со встроенным ИИ, использующиеся на промышленных объектах. Сформирован комплексный набор показателей, используемых для исследования устойчивости моделей МО, включающий показатели качества набора тестовых данных (MDQ), показатели качества модели МО (MMQ), показатели устойчивости модели к состязательным атакам (MSQ). Способ основан на применении данного комплекса показателей и включает следующие шаги: формирование набора тестовых данных, содержащего чистые образцы; оценка качества набора тестовых данных с использованием показателей MMQ; определение актуальных методов реализации состязательных атак; генерация состязательных примеров и формирование набора тестовых данных для оценки устойчивости модели, содержащего сгенерированные состязательные образцы; оценка качества сформированного набора тестовых данных с использованием показателей MDQ; оценка качества модели МО с использованием показателей MMQ; оценка устойчивости модели с использованием показателей MSQ.

**Ключевые слова:** кибербезопасность, методы искусственного интеллекта, интеллектуальные производственные системы, состязательные атаки.
**DOI:** 10.21293/1818-0442-2023-26-4-44-52

Под системой, использующейся на распределенных промышленных объектах, понимается распределённая система ввода-вывода с децентрализованной обработкой данных [1]. Как правило, такая система включает множество различного рода оборудования, создающего инфраструктуру для реализации определенного алгоритма управления [2]. Подобные объекты могут включать множество различных датчиков, сигналы от которых передаются на систему управления.

В настоящее время промышленные системы развиваются в соответствии с концепцией «Индустрии 4.0», подразумевающей полную автоматизацию всех процессов, ключевая роль в которой отводится методам машинного обучения (МО) и искусственного интеллекта (ИИ) [3, 4]. В настоящее время многие прикладные задачи решаются при помощи искусственных нейронных сетей (ИНС), например: визуальный контроль качества продукции и ее учет, мониторинг качества работы персонала или автоматизированных линий, определение объектов при позиционировании оборудования и манипуляторов, обнаружение опасных зон и контроль соблюдения персоналом правил безопасности [5].

Также на промышленных объектах могут использоваться различные биометрические системы для разграничения доступа, детекторы объектов (людей, автомобилей и др.), также основанные на методах ИИ. При этом эксперты отмечают, что эти технологии создают серьезные проблемы, связанные с кибербезопасностью (англ. cybersecurity) и функциональной безопасностью (англ. safety). В реальных промышленных системах должен обеспечиваться необходимый уровень доверия и надежности используемых моделей и алгоритмов МО. На передний план выходят отказоустойчивость и функциональная безопасность подобных систем, так как технологические процессы требуют непрерывного выполнения. Важно гарантировать, что их использование не приведет к возникновению сбоев и ошибок, вызванных как внутренними проблемами, так и действиями злоумышленников [6].

**Анализ состязательных атак на системы со встроенным искусственным интеллектом**

Обобщенно представляется возможным разделить жизненный цикл применения алгоритмов МО на два этапа: этап подготовки (обучения) модели и этап эксплуатации (рис. 1).

Отметим, что на промышленных объектах может применяться не одна, а несколько моделей (A, B, …, N), предназначенных для решения разных задач. Система управления превращает ответы моделей МО на поступающие входные данные в реальные действия.

Данные могут поступать с видеокамер и звукозаписывающих устройств, разнообразных датчиков (температуры, давления, уровня, частиц и пр.). Так, модель «A» может анализировать видеопоток, модель «B» – анализировать данные различных датчиков. Система управления использует их для принятия решения по выполнению какого-либо действия (в том числе полной остановки или возобновления производства, остановки одного из узлов и пр.). По сути система использует модели МО для преобразования входных данных реального мира в решения, а затем в действия.

Системы со встроенным ИИ, использующиеся на промышленных объектах, также уязвимы перед атаками [7, 8], которые могут выполняться как на

этапе подготовки и обучения модели, так и на этапе ее эксплуатации [9].

Состязательная атака (англ. adversarial attack) – это обобщенное наименование атак на системы ИИ, в том числе способы обмана ИНС с целью изменения «ответа» системы на необходимый злоумышленнику и нарушения ее производительности. Данные атаки могут выполняться на системы распознавания образов (фото, видео, аудио) и реализуются с использованием состязательных примеров (англ. adversarial samples) – образцов данных (англ. data sample), в которые внесены незначительные искажения, приводящие к некорректному распознаванию [10]. Такими искажениями, в частности, могут служить добавление шума или изменение нескольких пикселей на изображении. Важным является тот факт, что искажения незаметны для человека.

На этапе подготовки и обучения модели могут выполняться различные действия с обучающими данными, начиная от атак на получение несанкционированного доступа (НСД) к данным, заканчивая различными манипуляциями – отравлением обучающих данных.

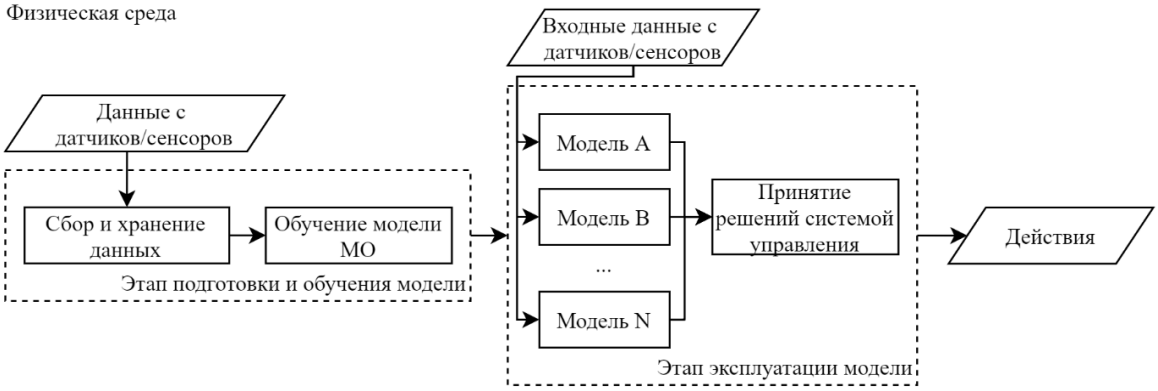



Рис. 1. Этапы применения алгоритмов МО на промышленных объектах

Атаки на доступ к данным имеют одну основную цель – кража набора данных для создания злоумышленником модели, которая будет использована для создания состязательных примеров для последующего выполнения атаки уклонения.

Отравление нацелено на смещение границы принятия решения и может выполняться как путем внедрения в набор новых вредоносных образцов, так и модификацией имеющихся данных (изменение значений признаков, изменение меток классов).

Атаки на этапе эксплуатации модели МО имеют две основные цели [11]:

• получение информации о модели или наборе обучающих данных (разведывательные атаки);

• поиск уязвимостей в обученной модели для нахождения образцов данных, на которых модель ошибается (атаки на обход модели МО).

В системах со встроенным ИИ защите подлежат:

1) данные (результаты измерений), из которых получены признаки для обучения;

2) алгоритмы получения признаков из результатов измерений;

3) алгоритмы обучения модели МО;

4) значения гиперпараметров модели МО;

5) значения параметров обученной модели МО;

6) доверительные вероятности принимаемых решений;

7) сами принимаемые решения;

8) граница принятия решений моделью (или гиперплоскость в $n$-мерном пространстве признаков).

**Этапы реализации атак на системы со встроенным ИИ, использующиеся на промышленных объектах**

В общем виде все сценарии выполнения атак на системы со встроенным ИИ, использующиеся на промышленных объектах, могут быть сведены к представленной на рис. 2 схеме.

Также выделяются два этапа выполнения атаки: подготовка и воздействие. Конкретные сценарии формируются путем пересечения техник этапа подготовки (ЭП) и этапа воздействия (ЭВ).

*ЭП.1–ЭП.2. Отравляющие атаки: внедрение данных в набор обучающих данных, модификация образцов в наборе обучающих данных*

Злоумышленник, имея доступ к обучающему набору данных, может осуществить его отравление путем изменения самих данных или меток классов. Это позволяет злоумышленнику встроить в модель МО уязвимость, которую достаточно сложно обнаружить. В стандартных условиях модель работает в соответствии с ожидаемым поведением, однако при наличии специального триггера во входных данных будет производить необходимый злоумышленнику результат.

Данная уязвимость может быть активирована путем передачи в модель МО образца данных, содержащего необходимый триггер. Примером может служить размещение специально подготовленного изображения в физической среде, где оно фиксируется камерой (см. ЭР.1, ЭР.3–ЭР.4).

*ЭП.3–ЭП.4. Атаки на доступ к данным или модели: кража набора обучающих данных, кража модели МО*

Злоумышленник, используя стандартные средства получения НСД, осуществляет кражу обучающего набора данных или модели.

С использованием набора данных он обучает собственную модель, повторяющую целевую модель, создает состязательные примеры и, используя свойство переносимости ИНС, осуществляет атаку целевой модели.

Если же злоумышленник имеет полный доступ к целевой модели, то он выполняет приведенные выше шаги, исключая этап обучения.

Далее выполняется атака по ЭР.1, ЭР.3–ЭР.4 путем передачи в модель вредоносного образца данных.

*ЭП.5–ЭП.6. Разведывательные атаки: восстановление модели МО, восстановление набора обучающих данных*

Разведывательные атаки могут как иметь целью кражу интеллектуальной собственности и получение конфиденциальной информации (ЭР.5–ЭР.6), так и являться вспомогательным этапом для реализации других атак (ЭР.1–ЭР.4).

Злоумышленник, используя различные виды санкционированного доступа (например, доступ по API) и ответы модели МО, осуществляет восстановление обучающего набора данных или модели.

Злоумышленник может восстановить данные, которые были использованы для обучения, направляя многократные запросы к модели и анализируя ответы (предсказанное значение и оценка уверенности в прогнозе). Корректируя подаваемые на вход данные и максимизируя уверенность в прогнозе, он имеет возможность восстановить обучающие данные или же убедиться, что конкретный образец содержался в обучающем наборе.

Также анализ ответов модели может быть использован для создания собственной модели, которая будет имитировать поведение целевой модели.

Атака выполняется по ЭР.1–ЭР.4 и по ЭР.5–ЭР.6.

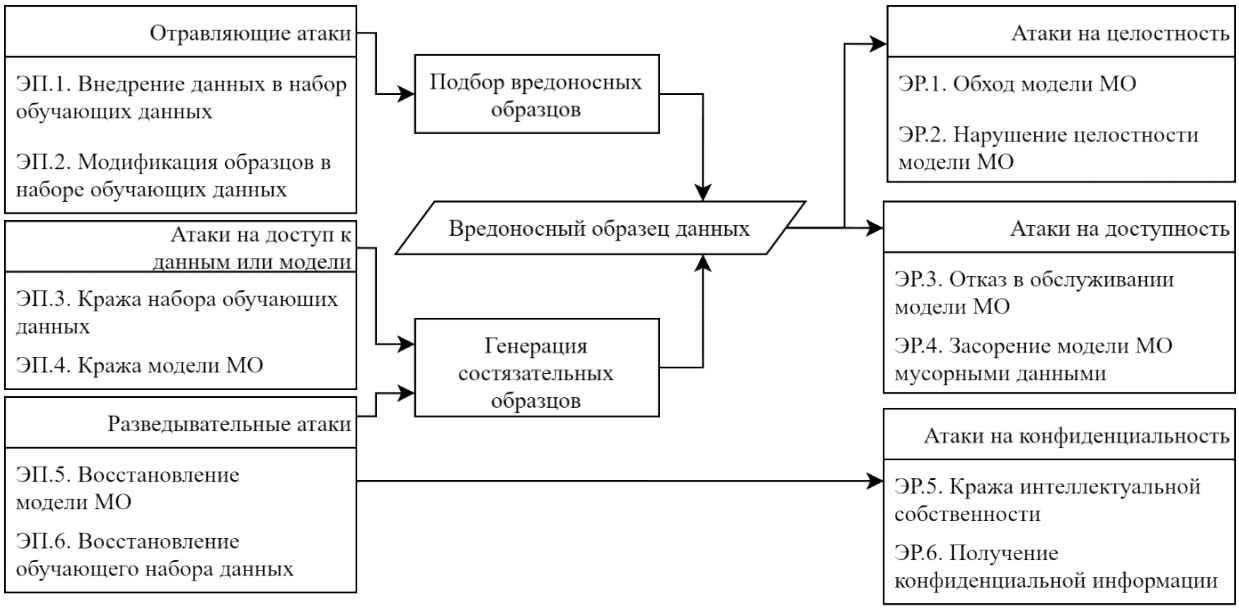



Рис. 2. Обобщенная схема реализации атак на системы со встроенным ИИ, использующиеся на промышленных объектах

*ЭР.1. Обход модели МО*

Злоумышленник создает состязательные образцы и, используя свойство переносимости ИНС, осуществляет атаку целевой модели путем передачи состязательного примера, например, изображения, размещая его в физической среде, где он фиксируется камерой.

*ЭР.2. Нарушение целостности модели МО*

Злоумышленники могут ухудшить качество работы целевой модели, если модель использует поступающие входные данные для дообучения. Ввод множества вредоносных данных постепенно изменит модель, нарушит ее целостность и снизит доверие к системе.

*ЭР.3–4. Отказ в обслуживании модели МО и засорение модели МО мусорными данными*

Злоумышленник генерирует поток запросов к модели МО с целью ухудшить, замедлить или остановить работу системы. Часто системы с МО требуют значительных вычислительных ресурсов, злоумышленник может создать такие входные данные, которые требуют больших объемов вычислений.

*ЭР.5–ЭР.6. Кража интеллектуальной собственности, получение конфиденциальной информации*

Злоумышленник осуществляет восстановление обучающего набора данных или модели, преследуя своей целью кражу интеллектуальной собственности или получение конфиденциальной информации.

**Сценарии реализации состязательных атак на системы со встроенным искусственным интеллектом, использующиеся на промышленных объектах**

Анализ литературы показал, что в настоящее время существует два основных способа применения состязательных атак к реальным промышленным объектам: использование состязательных заплаток (англ. adversarial patches) и состязательные атаки на виртуальные датчики (англ. soft sensors).

Состязательная заплатка – изображение меньшего размера (относительно объекта), которое создается с использованием состязательных атак и накладывается поверх объекта. Выделим три сценария использования состязательных заплаток для атак систем, применяющиеся на промышленных объектах.

*Сценарий 1.* Обман биометрических систем.

Состязательные заплатки, нанесенные на предметы одежды или медицинские маски, могут способствовать сокрытию субъекта или же неверной его идентификации. На рис. 3 приведен пример реализации такой атаки [12]. Точность идентификации субъекта без использования маски составляет 74,83%, с использованием обычной медицинской маски – 53,04%, с использованием маски с состязательным изображением – 5,17%.

Подобные атаки могут применяться для обмана систем биометрической идентификации разграничения доступа, мониторинга качества работы персонала, контроля соблюдения персоналом правил безопасности.


Рис. 3. Сценарий использования состязательных заплаток для обмана биометрических систем (неверная идентификация субъекта)

*Сценарий 2.* Обман систем детектирования и распознавания объектов.

Подобные подходы могут использоваться для обмана систем детектирования и распознавания объектов, таких как автомобили, упаковки с готовой продукцией. Рисунок 4 иллюстрирует нанесение состязательных заплаток на системы распознавания автомобилей, что позволяет скрыть присутствие данного объекта на территории [13, 14].

Данные атаки могут применяться для обмана систем визуального контроля качества продукции и ее учета, мониторинга качества работы автоматизированных линий, контроля опасных для человека зон, контроля пересечения объектами защищаемого периметра.


Рис. 4. Сценарий использования состязательных заплаток для обмана систем детектирования объектов (сокрытие объекта)

*Сценарий 3.* Обман систем позиционирования манипуляторов

Роботизированные производственные системы также используют системы распознавания образов, основанные на ИНС.

В работе [15] продемонстрирована атака на детектор объектов и позиционирования манипулятора, роботизированной руки. На карту нанесена состязательная заплатка, что создает некоторую оптическую иллюзию относительно позиции центра карты (рис. 5). Данная заплатка позволяет сместить предсказанное местоположение центра на область руки человека-оператора, что приводит к захвату ее манипулятором.

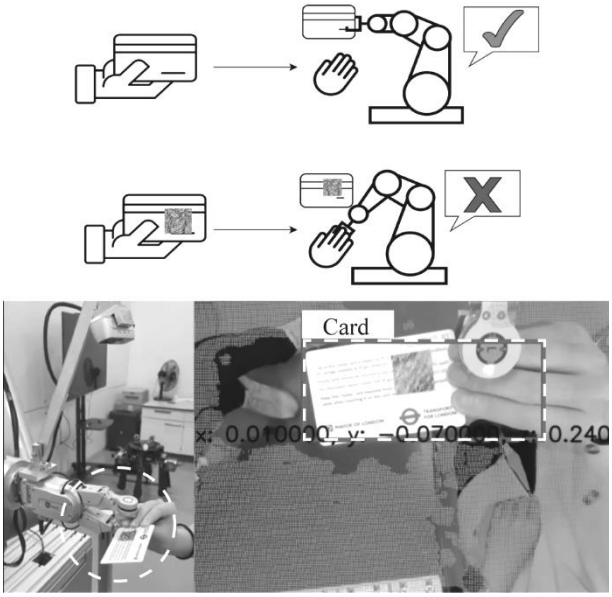



Рис. 5. Сценарий использования состязательных заплаток для обмана детектора объектов и позиционирования манипулятора (роботизированной руки)

*Сценарий 4.* Состязательные атаки на виртуальные датчики.

Виртуальные датчики представляют собой модели прогнозирования. На датчик в реальном времени поступают значения независимых переменных, на основании которых он прогнозирует зависимую переменную с использованием ИНС: в том числе глубоких нейронных сетей (DNN), автоэнкодеров, рекуррентных нейронных сетей (RNN), сетей с долгой краткосрочной памятью (LSTM), сверточных нейронных сетей (CNN).

Все из приведенных архитектур ИНС уязвимы к состязательным атакам. Созданные состязательные примеры могут привести к некорректным прогнозам этих моделей. При этом состязательные примеры создаются таким образом, чтобы выходные данные и прогнозы оставались похожими на допустимые.

В работе [16] продемонстрирована атака на виртуальные датчики, использующиеся в печи первичного риформинга (производство аммиака). Авторы проанализировали механизм, лежащий в основе работы виртуальных датчиков, и предложили два новых алгоритма для проведения атак: прямая атака на вывод (англ. directly attack output, DAO) и итеративная прямая атака на вывод (англ. iterative directly attack output, IDAO). В экспериментах была выполнена оценка коэффициента детерминации ($R^2$) модели до выполнения атак (методом быстрого градиента, базо-

вым итеративным методом, DAO и IDAO). До проведения атак $R^2$ составлял 0,821, а после в среднем по приведенным всем видам атак снизился до –4,184.

**Влияние состязательных атак на показатели работы систем со встроенным искусственным интеллектом**

Злоумышленник, реализующий состязательные атаки, может действовать так, чтобы получить необходимое ему поведение системы; нарушить корректность ее работы; сделать систему недоступной; получить конфиденциальную информацию о системе в целом, модели МО и/или обучающих данных.

В табл. 1 отражено влияние состязательных атак на основные показатели работы систем со встроенным ИИ.

Таблица 1

**Оценка показателей работы систем со встроенным ИИ, находящихся в условиях реализации состязательных атак**

| Вид атаки | Этапы использования МО | Показатель работы системы со встроенным ИИ | Влияние атаки на показатель |
|---|---|---|---|
| Атаки на конфиденциальность | Подготовка и обучение модели<br>Эксплуатация модели | Риск нарушения приватности | Повышение |
| | | Риск утечки конфиденциальных данных | Повышение |
| Атаки на целостность | Подготовка и обучение модели<br>Эксплуатация модели | Уверенность в прогнозе (confidence) | Снижение уверенности в прогнозе |
| | | Показатели качества работы модели МО | Снижение показателей качества |
| Атаки на доступность | Эксплуатация модели | Время получения ответа от системы | Повышение |

Уязвимости систем со встроенным ИИ позволяют злоумышленникам манипулировать целостностью систем машинного обучения (заставляя их совершать ошибки), конфиденциальностью (что приводит к утечке информации) и доступностью (нарушая или прекращая работу систем в целом или моделей).

**Разработка способа исследования устойчивости систем со встроенным искусственным интеллектом к состязательным атакам**

Под устойчивостью принято понимать свойство системы функционировать с заданными качественными показателями, находясь в условиях реализации атак [17]. С формальной точки зрения устойчивость к состязательным атакам определяется ее нечувствительностью к изменениям во входных данных. Устойчивость модели ($F$) оценивается на основе набора данных, включающего сгенерированные состязательные примеры. При этом качество полученного набора играет решающую роль в оценке показателей устойчивости.

Модель $F$: $X \to Y$ представляет собой отображение входного пространства $X$ в выходное пространство меток классов $Y$. Входное пространство $X = \{x_1, \ldots, x_n\}$ содержит $n$ образцов данных, а выходное пространство $Y = \{y_1, \ldots, y_m\}$ содержит $m$ возможных предсказаний метки класса. Модель $F$ построена таким образом, что для образца данных $x_i$ способна отнести его к истинному классу $y_j$.

Множество состязательных образцов $X' = \{x'_1, \ldots, x'_n\}$ образуется путем добавления искажений $p$ к исходным образцам $X$. $\Omega(x_i)$ представляет множество всех возможных измененных образцов $x_i$.

Модель $F$ является устойчивой к состязательным атакам, если никакое искажение $p$, внесенное в $x_i$, не может изменить выходные данные, т.е. $x'_i \in \Omega(x_i) \Rightarrow F(x_i) = y_j$.

*Показатели устойчивости систем со встроенным ИИ к состязательным атакам*

Существует ряд показателей, позволяющих оценить качество разработанной модели МО. Показатели качества набора тестовых данных играют решающую роль в оценке устойчивости.

Представляется возможным сгруппировать данные показатели в три основные категории, характеризующие:

- качество набора тестовых данных (MDQ);
- качество модели МО (MMQ);
- устойчивость модели к состязательным атакам (MSQ).

Выделим ряд показателей, характеризующих качество набора тестовых данных:

- покрытие нейронов [18];
- незаметность внесенных изменений [19].

Показатели устойчивости модели МО приведены в табл. 2.

На рис. 6 проиллюстрирована кривая устойчивости модели к состязательным образцам, она демонстрирует взаимосвязь между точностью работы на состязательных примерах и уровнем внесенных искажений. В данном примере под внесенными искажениями понимается добавление цифрового шума на изображения.

Плавная кривая устойчивости означает, что модель МО стабильна и последовательна (модель 1 на иллюстрации), а крутая – показывает, что она чувствительна и нестабильна (модель 2 на иллюстрации). Значение радиуса устойчивости (отмечен вертикальной штриховой линией) для модели 1 и 2 в данном примере составляет 0,25 и 0,03 соответственно. Радиус устойчивости вычисляется, исходя из имеющихся требований к значению показателя точности работы модели, и отражает максимальное количество искажений, которые могут быть корректно обработаны моделью.

Высокая точность $A_{\text{clear}}$ и большой радиус устойчивости указывают на то, что модель устойчива к состязательным атакам, тогда как низкая точность $A_{\text{clear}}$ и небольшой радиус устойчивости предполагают, что она уязвима для них.

Таблица 2

**Показатели качества модели МО и устойчивости модели к состязательным атакам**

| | | |
|---|---|---|
| Характеризующие качество модели МО | | |
| $A_{clear}$ | Точность (accuracy) работы модели на чистых данных | Доля чистых образцов данных $X$, отнесенных моделью к истинному классу относительно общего числа образов $n$ |
| $Perf_{clear}$ | Производительность модели на чистых данных | Количество чистых образцов данных, обработанных моделью в единицу времени |
| Характеризующие устойчивость модели МО к состязательным атакам | | |
| $A_{adv}$ | Точность работы модели на состязательных данных | Доля состязательных образцов данных $X'$, отнесенных моделью к истинному классу относительно общего числа образов |
| $R$ | Радиус устойчивости | Оценка максимального количество искажений $p$, которые могут быть внесены в образец данных $x_i$, так чтобы $F(x'_i) = y_j$ [20] |
| $S$-curve | Кривая устойчивости | График, позволяющий оценить зависимость точности $A_{adv}$ от $p$ (рис. 7) |
| $AVF_{conf}$ | Средняя уверенность (confidence) модели в прогнозе относительно ложного класса | Среднее арифметическое вероятностной оценки уверенности в прогнозах относительно ложного класса по всем состязательным примерам, которые были успешны в обходе модели |
| $AVT_{conf}$ | Средняя уверенность модели в прогнозе относительно истинного класса | Среднее арифметическое вероятностной оценки уверенности в прогнозах относительно истинного класса по всем состязательным примерам, которые были успешны в обходе модели |
| $NTR$ | Толерантность к шуму | Оценка распределения вероятностей над множеством классов, среднее арифметическое разниц между вероятностью наиболее подходящего ложного класса и максимальной вероятностью других классов [21] |
| $Perf_{adv}$ | Производительность модели на состязательных данных | Количество состязательных образцов данных, обработанных моделью в единицу времени |

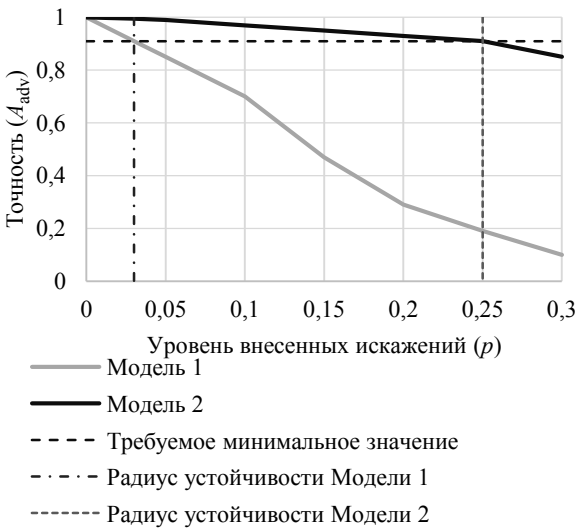



Рис. 6. Иллюстрация кривой и радиуса устойчивости модели к состязательным образцам

*Способ исследования устойчивости систем со встроенным искусственным интеллектом, использующихся на промышленных объектах, к состязательным атакам*

Оценка устойчивости систем со встроенным искусственным интеллектом к состязательным атакам сводится к оценке применяемой модели МО, что схематично отражено на рис. 7.

Приведем последовательность выполнения оценки устойчивости систем со встроенным искусственным интеллектом к состязательным атакам:

1. Формирование набора тестовых данных, содержащего чистые образцы ($Data_{clear}$).

2. Оценка качества набора тестовых данных $Data_{clear}$ с использованием показателей MDQ.

3. Определение актуальных методов реализации состязательных атак.

4. Генерация состязательных примеров на основании выделенных в п. 2 методов с использованием программных инструментов и библиотек (Adversarial Robustness Toolbox, Robustness Gym, Cleverhans, Alibi Detect).

5. Формирование набора тестовых данных для оценки устойчивости модели, содержащих сгенерированные состязательные образцы ($Data_{adv}$).

6. Оценка качества набора тестовых данных $Data_{adv}$ с использованием показателей MDQ.

7. Оценка качества модели МО с использованием $Data_{clear}$ и показателей MMQ.

8. Оценка устойчивости модели с использованием $Data_{adv}$ и показателей MSQ.

Дополнительно может выполняться оценка устойчивости модели к различного рода искажениям (различные виды шума, туман, снег, изменения яркости и контрастности, оптические искажения и пр.) [22].

Также после внедрения мер противодействия состязательным атакам рекомендуется выполнить оценку их качества (включая, но не ограничиваясь разницей Aclear до и после применённых мер).

**Заключение**

В статье представлен способ исследования устойчивости систем со встроенным ИИ к состязательным атакам. Установлено влияние состязательных атак на показатели конфиденциальности, целостности и доступности систем. На основе анализа литературных источников выделены показатели, характеризующие устойчивость систем перед состязательными атаками, в том числе точность работы модели на состязательных данных, радиус устойчивости, кривая устойчивости, средняя уверенность модели в прогнозе относительно ложного класса, оценка толерантности к шуму, производительность модели на состязательных данных. Способ основан на применении комплекса показателей, включающего показа-

тели качества набора тестовых данных, показатели качества модели МО, показатели устойчивости модели к состязательным атакам. Данный способ предназначен для специалистов по кибербезопасности, а также разработчиков программных систем со встроенным искусственным интеллектом. Способ позволяет оценить устойчивость систем со встроенным ИИ (в том числе применяющихся на промышленных объектах) к состязательным атакам.

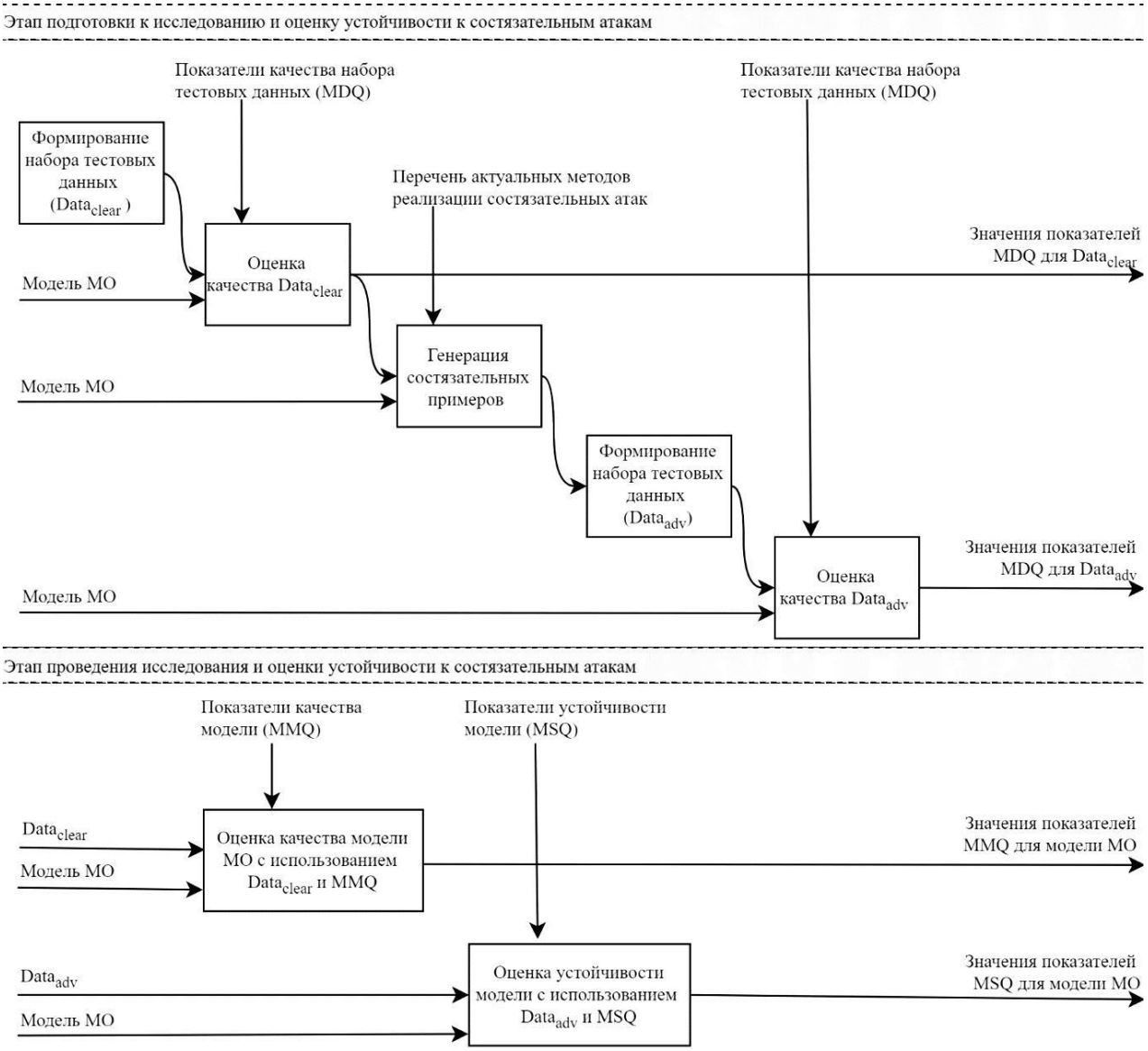



Рис. 7. Схема исследования и оценки устойчивости систем со встроенным искусственным интеллектом к состязательным атакам

Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации, № 2019-0898.

*Литература*

1. Обзор современного рынка распределенных систем управления в нефтяной и газовой промышленности / А.В. Окружнов, Р.Р. Хайбунасов, И.Р. Хасанов, М.М. Андреева // Вестник Казанского технологического ун-та. – 2015. – Т. 18, № 2. – С. 383–389.

2. Коекин В.А. Алгоритмы управления на территориально распределенных промышленных и бытовых объектах // Электротехнические и информационные комплексы и системы. – 2008. – № 51. – С. 59–65.

3. Воробьева А.А. Методы интеллектуального анализа данных и обработки естественного языка в управлении роботизированными производственными системами / А.А. Воробьева, М.Ю. Федосенко // Доклады ТУСУР. – 2023. – Т. 26, № 3. – С. 65–71.

4. Smart Factory Monitoring [Электронный ресурс]. – Режим доступа: https://www.procemex.com/smart-factory/, свободный (дата обращения: 05.12.2023).

5. AIoT для умных фабрик [Электронный ресурс]. – Режим доступа: https://www.cta.ru/articles/obzory/vstraivaemye-sistemy/165894/, свободный (дата обращения: 05.12.2023).

6. Adversarial/Robust AI Report development methodology [Электронный ресурс]. – Режим доступа: https://ec.eu-

ropa.eu/research/participants/documents/downloadPublic?documentIds=080166e5e1fdef06&appId=PPGMS, свободный (дата обращения: 05.12.2023).

7. A survey on adversarial attack in the age of artificial intelligence / Z. Kong, J. Xue, Y. Wang, L. Huang, Z. Niu, F. Li // Wireless Communications and Mobile Computing. – 2021. – Vol. 2021. – P. 1–22.

8. A review on ai for smart manufacturing: Deep learning challenges and solutions / J. Xu, M. Kovatsch, D. Mattern, F. Mazza, M. Harasic, A. Paschke, S. Lucia // Applied Sciences. – 2022. – Vol. 12, No. 16. – P. 8239.

9. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/pubs/ai/100/2/e2023/ipd, свободный (дата обращения: 05.12.2023).

10. Goodfellow I.J. Explaining and harnessing adversarial examples / I.J. Goodfellow, J. Shlens, C. Szegedy [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/1412.6572, свободный (дата обращения: 05.12.2023).

11. Tuptuk N. Security of smart manufacturing systems / N. Tuptuk, S. Hailes // Journal of manufacturing systems. – 2018. – Vol. 47. – P. 93–106.

12. Adversarial Mask: Real-World Universal Adversarial Attack on Face Recognition Models / A. Zolfi, S. Avidan, Y. Elovici, A. Shabtai // Joint European Conference on Machine Learning and Knowledge Discovery in Databases. – 2022. – P. 304–320.

13. Adversarial patch attack on multi-scale object detection for UAV remote sensing images / Y. Zhang, J. Qi, K. Bin, H. Wen, X. Tong // Remote Sensing. – 2022. – Vol. 14, No. 21. – P. 5298.

14. {CAPatch}: Physical Adversarial Patch against Image Captioning Systems / S. Zhang, Y. Cheng, W. Zhu, X. Ji, W. Xu // 32nd USENIX Security Symposium (USENIX Security 23). – 2023. – P. 679–696.

15. Physical Adversarial Attack on a Robotic Arm / Y. Jia, C.M. Poskitt, J. Sun, S. Chattopadhyay // IEEE Robotics and Automation Letters. – 2022. – Vol. 7, No. 4. – P. 9334–9341.

16. Kong X. Adversarial attacks on neural-network-based soft sensors: Directly attack output / X. Kong, Z. Ge // IEEE Transactions on Industrial Informatics. – 2021. – Vol. 18, No. 4. – P. 2443–2451.

17. Дорф Р. Современные системы управления / Р. Дорф, Р. Бишоп. – М.: Лаборатория базовых знаний, 2002. – 832 с.

18. Deepgauge: Multi-granularity testing criteria for deep learning systems / L. Ma, F. Juefei-Xu, F. Zhang, J. Sun, M. Xue, B. Li, C. Chen // Proceedings of the 33rd ACM/IEEE international conference on automated software engineering. – 2018. – P. 120–131.

19. A comprehensive evaluation framework for deep model robustness / J. Guo, W. Bao, J. Wang, Y. Ma, X. Gao, G. Xiao, A. Liu // Pattern Recognition. – 2023. – Vol. 137. – P. 109308.

20. Quantifying Robustness to Adversarial Word Substitutions / Y. Yang, P. Huang, J. Cao, F. Ma, J. Zhang, J. Li // Joint European Conference on Machine Learning and Knowledge Discovery in Databases. – 2023. – P. 95–112.

21. Towards imperceptible and robust adversarial example attacks against neural networks / B. Luo, Y. Liu, L. Wei, Q. Xu // Proceedings of the AAAI Conference on Artificial Intelligence. – 2018. – Vol. 32, No. 1. – P. 1–8.

22. Hendrycks D. Benchmarking neural network robustness to common corruptions and perturbations / D. Hendrycks, T. Dietterich [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/1903.12261, свободный (дата обращения: 05.12.2023).

**Воробьева Алиса Андреевна**
Канд. техн. наук, доцент ф-та безопасности информационных технологий (ФБИТ) Национального исследовательского университета ИТМО (Университет ИТМО)
Кронверкский пр-т, 49, А,
г. Санкт-Петербург, Россия, 197101
ORCID: 0000-0001-6691-6167
Тел.: +7-921-947-21-14
Эл. почта: vorobeva@itmo.ru

Vorobeva A.A.

**Method for evaluating the industrial systems with built-in artificial intelligence robustness to adversarial attacks**

The paper presents a method for evaluating the industrial systems with built-in artificial intelligence (AI) robustness to adversarial attacks. The influence of adversarial attacks on the systems performance has been studied. The scheme and the scenarios to implement attacks on industrial systems with built-in AI were presented. A comprehensive set of metrics used to study the robustness of ML models has been proposed, including test data set quality metrics (MDQ), ML model quality metrics (MMQ), and model robustness to adversarial attacks metrics (MSQ). The method is based on the use of this metrics set and includes the following steps: generating a set of test data containing clean samples; assessing the quality of a test data set using MMQ metrics; identification of relevant adversarial attacks methods; generating adversarial examples and a test data set, containing the adversarial samples, to evaluate the robustness of the ML model; assessing the quality of the generated adversarial test data set using MDQ indicators; evaluating the quality of a ML model using MMQ indicators; evaluating model robustness using MSQ scores.

**Keywords:** cybersecurity, artificial intelligence methods, intelligent production systems, adversarial attacks.
**DOI:** 10.21293/1818-0442-2023-26-4-44-52

*References*

1. Okruzhnov A.V, Khaibunasov R.R., Khasanov I.R., Andreeva M.M. [Overview of the modern market for distributed control systems in the oil and gas industry]. *Bulletin of the Technological University*, 2015, vol. 18, no. 1, pp. 383–389 (in Russ.).

2. Koekin V.A. Control algorithms for geographically distributed industrial and domestic facilities. *Electrical Engineering and Information Complexes and Systems*, 2008, no. S1, pp. 59–65 (in Russ.).

3. Vorobeva A.A., Fedosenko M.Yu. Methods for data mining and natural language processing in the management of robotic production systems. *Proceedings of TUSUR University*, 2023, vol. 26, no. 3, pp. 65-71.

4. *Smart Factory Monitoring*. Available at: https://www.procemex.com/smart-factory/, free (Accessed: December 02, 2023).

5. *AIoT for smart factories*. Available at: https://www.cta.ru/articles/obzory/vstraivaemye-sistemy/165894/, free (Accessed: December 02, 2023).

6. *Adversarial/Robust AI Report development methodology*. Available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5e1fdef06&appId=PPGMS, free (Accessed: December 02, 2023).

7. Kong Z., Xue J., Wang Y., Huang L., Niu Z., Li F. A survey on adversarial attack in the age of artificial intelligence, *Wireless Communications and Mobile Computing*, 2021, vol. 2021, pp. 1–22.

8. Xu J., Kovatsch M., Mattern D., Mazza F., Harasic M., Paschke A., Lucia S. A review on ai for smart manufacturing: Deep learning challenges and solutions, *Applied Sciences*, 2022, vol. 12, no. 16, pp. 8239.

9. *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*. Available at: https://csrc.nist.gov/pubs/ai/100/2/e2023/ipd, free (Accessed: December 02, 2023).

10. Goodfellow I.J., Shlens J., Szegedy C. Explaining and harnessing adversarial examples. Available at: https://arxiv.org/abs/1412.6572, free (Accessed: December 02, 2023).

11. Tuptuk N., Hailes S. Security of smart manufacturing systems, *Journal of Manufacturing Systems*, 2018, vol. 47, pp. 93–106.

12. Zolfi A., Avidan S., Elovici Y., Shabtai A. Adversarial Mask: Real-World Universal Adversarial Attack on Face Recognition Model, *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, 2022, pp. 304–320.

13. Zhang Y., Zhang Yi., Qi J., Bin K., Wen H., Tong X. Adversarial patch attack on multi-scale object detection for UAV remote sensing images, *Remote Sensing*, 2022, vol. 14, no. 21, pp. 5298.

14. Zhang S., Cheng Y., Zhu W., Ji X., Xu W. {CAPatch}: Physical Adversarial Patch against Image Captioning Systems, *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 679–696.

15. Jia Y., Poskitt C.M., Sun J., Chattopadhyay S. Physical Adversarial Attack on a Robotic Arm, *IEEE Robotics and Automation Letters*, 2022, vol. 7, no. 4, pp. 9334–9341.

16. Kong X., Ge Z. Adversarial attacks on neural-network-based soft sensors: Directly attack output, *IEEE Transactions on Industrial Informatics*, 2021, vol. 18, no. 4, pp. 2443–2451.

17. Dorf R., Bishop R. *Sovremennye sistemy upravleniya* [Modern control systems]. Moskva, Laboratoriya Bazovyh Znanij, 2002, 832 p. (in Russ.).

18. Ma L., Juefei-Xu F., Zhang F., Sun J., Xue M., Li B., Chen C. Deepgauge: Multi-granularity testing criteria for deep learning systems, *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering*, 2018, pp. 120–131.

19. Guo J., Bao W., Wang J., Ma Y., Gao X., Xiao G., Liu A. A comprehensive evaluation framework for deep model robustness, *Pattern Recognition*, 2023, vol. 137, pp. 109308.

20. Yang Y., Huang P., Cao J., Ma F., Zhang J., Li J. Quantifying Robustness to Adversarial Word Substitutions, *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, 2023, pp. 95–112.

21. Luo B., Liu Y., Wei L., Xu Q. Towards imperceptible and robust adversarial example attacks against neural networks, *Proceedings of the AAAI Conference on Artificial Intelligence*, 2018, vol. 32, no. 1, pp 1–8.

22. Hendrycks D., Dietterich T. Benchmarking neural network robustness to common corruptions and perturbations. Available at: https://arxiv.org/abs/1903.12261, free (Accessed: December 02, 2023).

**Alisa A. Vorobeva**
Candidate of Sciences in Engineering, Associate professor,
Faculty of Secure Information Technologies,
ITMO University
49, Kronverksky pr., bldg. A, St. Petersburg, Russia, 197101
ORCID: 0000-0001-6691-6167
Phone: +7-921-947-21-14
Email: vorobeva@itmo.ru

УДК 004.89

**А.В. Куртукова, А.С. Романов, А.А. Шелупанов**

# Разработка методики идентификации авторства бинарных и дизассемблированных кодов программы на основе ансамбля современных методов обработки естественного языка

Данная статья является частью цикла исследований, направленных на решение проблем идентификации авторства программного кода. Анализ бинарного или дизассемблированного кода является важнейшей задачей информационной безопасности, разработки программного обеспечения и компьютерной криминалистики ввиду необходимости защиты результатов интеллектуальной деятельности и авторского права, а также определения авторов вредоносных программ. Любая программа представляет собой машинный код, который может быть дизассемблирован (преобразован в текст на языке ассемблера) при помощи специализированных инструментов и проанализирован на предмет авторства по аналогии с текстом на естественном языке. Для решения обозначенной проблемы в статье предлагается методика на основе ансамбля fastText, метода опорных векторов (SVM) и авторской гибридной нейронной сети. Предложенная методика оценивалась на исходных кодах на языках C и C++, собранных с платформ GitHub и Google Code Jam, скомпилированных в исполняемые файлы и дизассемблированных инструментами реверс-инжиниринга. Средняя точность идентификации автора дизассемблированного кода предложенной методикой составила более 0,9. Методика также была апробирована на исходных кодах, в результате чего средняя точность составила 0,96 для простых случаев и более 0,85 для сложных (обфускация, стандарты кодирования и др.).

**Ключевые слова:** исходный код, машинное обучение, автор, нейронные сети, ансамбль, дизассемблер.
**DOI:** 10.21293/1818-0442-2023-26-4-53-60

Идентификация автора программного кода является важнейшей задачей в цифровой криминалистике [1] и обнаружении плагиата [2]. Решения этой задачи особенно полезны при судебных разбирательствах, связанных с вопросами интеллектуальной собственности и авторских прав, а также при расследованиях случаев разработки и распространения вредоносного программного обеспечения. Существующие методы идентификации автора компьютерной программы можно разделить на три группы: анализирующие исходный код [3–7], ассемблерный код дизассемблированной программы [8–12] и универсальные методы, применимые в обоих случаях [13, 14]. Хотя эти методы основаны на разных алгоритмах и подходах, все они имеют общий принцип работы: определение уникального стиля кодирования автора-программиста.

Уникальный стиль программиста характеризуется шаблонами проектирования, языковыми конструкциями, форматированием блоков кода, стилем комментариев к коду, идентификаторами, переменными, наименованиями функций, «запахами кода» [15] – фрагментами кода, не соответствующими правилам написания кода на языке, используемом автором программы. Перечисленные характеристики представляют исходный код программы, а не дизассемблированный. Однако некоторые из них остаются распознаваемыми даже после компиляции и дизассемблирования программы. Таким образом, определение авторства на основе дизассемблированного кода является более методологически сложным и требует более современных решений, адаптированных к этому виду анализа.

Целью данного исследования является разработка комплексного решения на основе алгоритмов обработки естественного языка, позволяющего с высокой точностью идентифицировать автора программы, используя как исходные, так и дизассемблированные коды.

**Обзор литературы**

При разработке и совершенствовании методики идентификации автора программного кода важно учитывать опыт, полученный исследователями ранее, и принимать во внимание преимущества, недостатки и ограничения тех или иных подходов.

Задача анализа программного кода с целью установления авторства имеет несколько фундаментальных решений, обеспечивающих приемлемый для их использования в прикладных задачах результат.

Большая часть методов [12–14], помимо основанных на глубоких нейронных сетях (НС) [16], оперирует множеством признаков, предложенным в исследовании [9]. Идея состоит в применении графов семантического потока (SFG) и потока управления (CFG), полученных путем реверс-инжиниринга, с целью получения из них последовательной трассировки операций. Итоговое множество признаков, полученное таким образом, включает вызовы библиотек, идиомы, графлеты, *n*-граммы и шаблоны функций.

Согласно результатам анализа аналогов разрабатываемой методики, такое множество является достаточным для получения высокой точности (более 0,7 для наборов данных Google Code Jam (GCJ) [17] и Codeforces [18]) простыми статистическими моделями, такими как метод опорных векторов (SVM) и абстрактные синтаксические деревья (АСД).

Исходя из анализа трудов [3–15], можно сделать вывод о том, что при решении задачи идентификации автора программного кода следует учитывать ряд факторов:

1. Большинство признаков, которые используются для определения авторства программы, описывают ее функциональность, а не авторский стиль, что может негативно сказаться на обобщающей способности классификатора.

2. При формировании признакового пространства важно предусмотреть фильтрацию для повышения информативности отдельно взятых признаков и их отделения от шума.

3. Большое влияние на оценку эффективности подхода оказывает домен данных. Зачастую исследователи используют программные коды с соревнований либо устаревшие наборы данных, находящиеся в открытом доступе, что негативно сказывается на объективности оценки и не позволяет оценить обобщающую способность подходов.

Следует отметить, что несмотря на безусловную эффективность подходов на основе CFG и SFG совместно с классическими алгоритмами машинного обучения, их использование в качестве основы для универсальной методики идентификации автора программного кода недопустимо. Это обусловлено двумя аспектами:

1. Подходы адаптированы под анализ дизассемблированных кодов и не применимы к исходным кодам.

2. Трудоемкость процесса и необходимость экспертных знаний низкоуровневых языков для его осуществления.

Нейросетевые подходы и ансамбли на их основе могут стать эффективной и универсальной альтернативой, не требующей дополнительных временных затрат на формирование релевантного множества признаков.

**Набор данных**

Для объективной оценки эффективности реализуемых подходов был необходим объемный и репрезентативный набор данных. При формировании набора обязательным было условие, что он не должен содержать данные, принадлежащие одному домену (как соревновательные данные GCJ). Это обусловлено, во-первых, необходимостью получить точную оценку и избежать ее искусственного завышения за счет решения одинаковых задач одними и теми же авторами-программистами, во-вторых, важностью реализации подхода с высокой обобщающей способностью без привязки к специфике данных. Так было решено сформировать собственный набор бинарных кодов программ.

Набор данных был собран при помощи интерфейса программирования приложения (API) открытого хостинга IT-проектов GitHub. В его состав вошли исходные коды, соответствующие требованиям:

– язык программирования – C и C++;

– длина кода не менее 5 строк;

– не менее 20 файлов с исходным кодом в репозиториях автора;

– возможность компиляции с помощью GCC;

– наличие сопроводительного файла с информацией о настройках компиляции.

Отобранные исходные коды были скомпилированы при помощи коллекции компиляторов GNU (GCC) [19], а затем дизассемблированы интерактивным дизассемблером (IDA) Pro [20]. Подробная информация об исходных и дизассемблированных кодах представлена в табл. 1.

Таблица 1

**Набор данных GitHub**

| Характеристика | Исходные коды | Дизассемблированные коды |
|---|---|---|
| Общее число авторов | 167 | |
| Общее число файлов | 12 779 | 5 661 |
| Ср. число файлов автора | 63 | 25 |
| Макс. число файлов автора | 132 | 51 |
| Мин. число файлов автора | 20 | 20 |
| Ср. число строк кода | 146 | 1 677 |

Так как целевым направлением применения методики является информационная безопасность, было решено сформировать релевантный этой тематике набор данных. В него вошли вредоносные исполняемые файлы известных хакерских группировок (рис. 1). Данные были получены на основании отчетов организаций, занимающихся обеспечением кибербезопасности, и дизассемблированы аналогично данным GitHub.

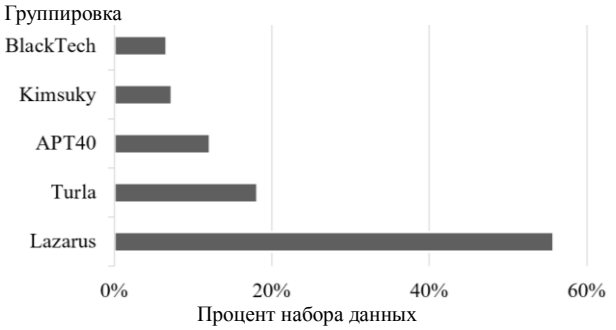



Рис. 1. Статистика набора данных вредоносных кодов

**Предварительные эксперименты**

Ранние исследования, посвященные решению задачи идентификации автора дизассемблированного кода программы, позволили оценить возможность применения наиболее эффективных моделей, исходя из смежных работ [21–23]: гибридной НС (HNN) на основе архитектур Inception-v1 и двунаправленных рекуррентных блоков, метода опорных векторов (SVM) и fastText.

В качестве метрики применялась точность, рассчитанная в результате процедуры 10-кратной перекрестной проверки. Обобщенные результаты эксперимента с дизассемблированными данными GitHub представлены в табл. 2.

Таблица 2

**Результаты экспериментов GitHub**

| Число авторов | HNN | SVM | fastText |
|---|---|---|---|
| 2 | 0,84 | 0,83 | 0,91 |
| 5 | 0,78 | 0,78 | 0,86 |
| 10 | 0,66 | 0,62 | 0,79 |

На основании полученных значений точности была рассчитана статистическая значимость результатов при помощи непараметрических апостериорных тестов Фридмана и Неменьи. Для оценки разницы между моделями использовался апостериорный тест Неменьи. Графическая интерпретация Дешмара представлена на рис. 2, где график *а* демонстрирует результаты для 2 авторов, *б* – для 5 и *в* – для 10 соответственно.

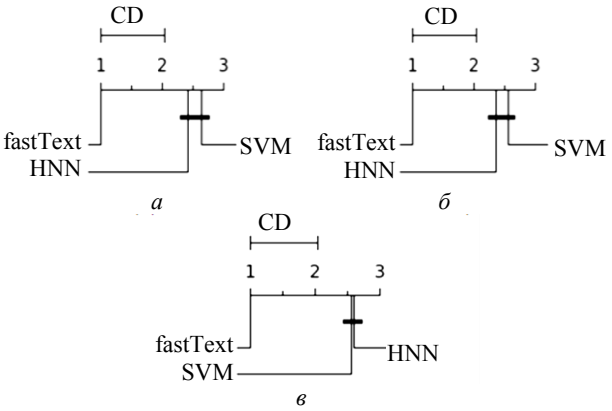



Рис. 2. Результаты для
2 авторов – *а*, 5 авторов – *б*, 10 авторов – *в*

Тесты показали, что эффективности HNN и SVM приблизительно равны, так как разница между их средними рангами меньше расчетного значения критической разницы (CD). Результат, полученный fastText, напротив, оказался значимым и несопоставимым с другими моделями.

Еще один эксперимент был выполнен на основе набора вредоносных исполняемых файлов, разработанных хакерскими группировками. Полученные результаты представлены в табл. 3.

Таблица 3

**Результаты экспериментов на вредоносных кодах**

| Число авторов | HNN | SVM | fastText |
|---|---|---|---|
| 2 | 0,89 | 0,9 | 0,94 |
| 3 | 0,85 | 0,87 | 0,9 |
| 4 | 0,82 | 0,8 | 0,85 |
| 5 | 0,76 | 0,74 | 0,79 |

Исходя из результатов предварительных экспериментов, был сделан вывод об особой эффективности fastText для идентификации автора дизассемблированного кода программы. Однако применение fastText в качестве универсального метода, исходя из ранних работ [21–23], не представлялось возможным из-за его низкой в сравнении с HNN эффективности для анализа исходных кодов программ.

Предварительные эксперименты позволили выдвинуть гипотезу об эффективности ансамбля классификаторов, состоящего из HNN, SVM и fastText, как универсального метода решения задачи идентификации автора программы на основе исходного или дизассемблированного кода.

**Универсальная методика идентификации автора программы по его исходным или дизассемблированным кодам**

Исходя из выдвинутой на основе предварительных экспериментов гипотезы об эффективности ансамбля классификаторов, была предложена усовершенствованная методика идентификации автора программы (рис. 3).

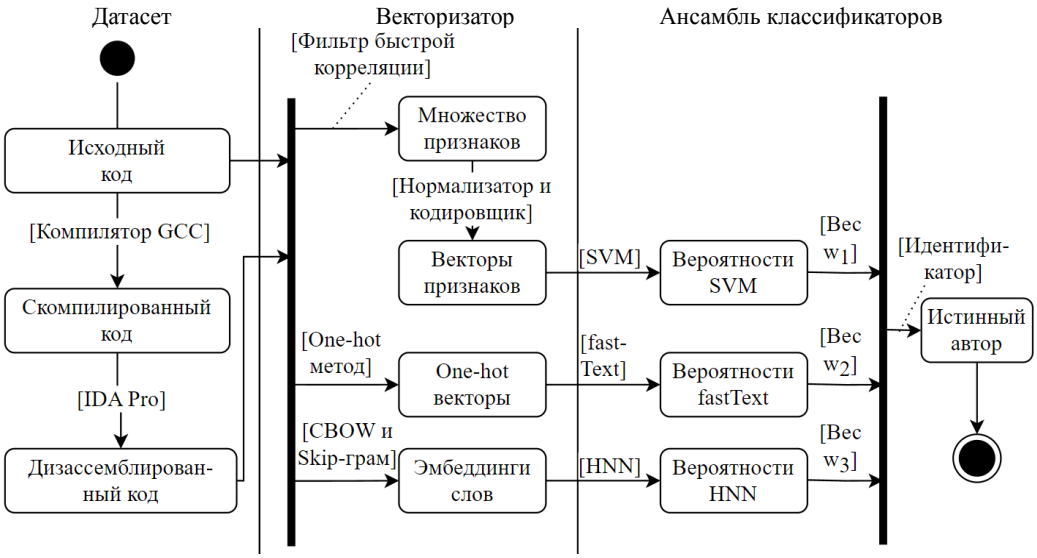



Рис. 3. Методика идентификации автора программы на основе ансамбля SVM, fastText, HNN

Первый этап посвящен подготовке обучающих данных к векторизации. Для случая идентификации автора по исходному коду файл сразу передается в модуль векторизации и не подлежит предобработке. Для случая идентификации автора по дизассемблированному коду исходный код компилируется с помощью GCC, а затем дизассемблируется IDA Pro.

Полученный в результате реверс-инжиниринга файл передается в модуль векторизации.

Второй этап заключается в преобразовании обучающих данных в векторный вид. Каждый из классификаторов требует соответствующий ему формат входных данных:

– SVM принимает на вход множество нормализованных и векторизованных признаков. В качестве признакового пространства для SVM использовались паттерны, описанные в исследовании [9].

– HNN работает с текстом как исходного, так и дизассемблированного кода без какой-либо предварительной обработки. Текст в его первоначальном виде передается прямому посимвольному кодировщику. Прямое посимвольное кодирование создает вектор из 255 нулей и 1 единицы для каждого отдельно взятого символа текста. При этом единица устанавливается на позиции, соответствующей коду символа, согласно американскому стандартному коду обмена информацией (ASCII).

– fastText также принимает на вход исходные коды как текст. Представления слов (эмбеддинги) создаются fastText автоматически при помощи кодирования непрерывным мешком слов (CBOW).

Последний этап состоит в обучении ансамбля классификаторов для последующей идентификации автора программы. Оптимальные гиперпараметры для классификаторов SVM и HNN были определены экспериментально при помощи жадного поиска, а для fastText использовалась встроенная в инструмент функция автовалидации.

Для SVM использовались следующие параметры:

– тип – многоклассовая классификация;

– алгоритм обучения – метод последовательной оптимизации;

– ядро – сигмоидальное;

– параметр регуляризации C = 1;

– допустимый уровень ошибки = 0,00001.

В качестве параметров для HNN были выбраны:

– функция оптимизации – Adadelta;

– функция активации – Softmax;

– функция прореживания – Dropout(0,2);

– промежуточная функция активации – ReLU;

– leaning rate = $10^{-4}$;

– rho = 0,95;

– eps = $10^{-7}$.

Большинство параметров fastText по умолчанию оказались оптимальными:

– learning rate = 0,9;

– threads = 15;

– lrUpdateRate = 5.

Главный принцип работы ансамбля состоит в применении весовых коэффициентов, представленных на схеме как $w_1$, $w_2$ и $w_3$, к результатам работы отдельных классификаторов. Для анализа дизассемблированных кодов наибольший вес ($w_3$ = 0,4) присваивается решениям fastText как наиболее точного классификатора для данного случая. Для решений, принятых двумя другими классификаторами, устанавливаются равные веса: $w_1$ = 0,3 для SVM и $w_2$ = 0,3 для HNN соответственно. Таким образом, наибольшую ценность будут представлять вероятности, полученные от fastText. Единственный случай, когда решением fastText можно будет пренебречь, это совпадение в вероятностях HNN и SVM. Тогда их суммарный коэффициент составит 0,6 против коэффициента fastText 0,4.

Для анализа исходных кодов программ наибольший вес присваивается решениям HNN ($w_2$ = 0,4). А решениям классификаторов fastText и SVM как менее эффективным в сложных случаях присваиваются равные веса. Аналогично случаю с бинарными кодами: $w_3$ = 0,3 для fastText и $w_1$ = 0,3 для SVM соответственно. Принцип идентификации автора исходного кода таким ансамблем аналогичен анализу дизассемблированного кода.

**Апробация методики**

Разработанная методика была апробирована на исходных и дизассемблированных кодах программ. Эксперименты были проведены как для простых, так и для сложных случаев идентификации автора. Число спорных авторов для части экспериментов было повышено до 20. Результаты работы ансамбля классификаторов для анализа дизассемблированных кодов представлены в табл. 4. Для анализа исходных кодов в простых случаях – в табл. 5.

Таблица 4

**Результаты для дизассемблированных кодов**

| Число файлов | 10 | 20 | 30 |
|---|---|---|---|
| 5 авторов | 0,86 | 0,9 | 0,96 |
| 10 авторов | 0,85 | 0,87 | 0,93 |
| 20 авторов | 0,78 | 0,83 | 0,86 |

Таблица 5

**Результаты для простых исходных кодов**

| Число файлов | 10 | 20 | 30 |
|---|---|---|---|
| 5 авторов | 0,95 | 0,97 | 0,98 |
| 10 авторов | 0,93 | 0,95 | 0,96 |
| 20 авторов | 0,92 | 0,95 | 0,96 |

В результате применения ансамбля к дизассемблированным кодам был получен прирост в точности более 0,1 в сравнении с применением классификаторов по отдельности. При достаточном количестве обучающих файлов точность превышает 0,9.

Результаты, полученные ансамблем для исходных кодов, сопоставимы с полученными ранее [23], т.е. ансамбль негативного влияния на данный случай не оказывает.

Помимо простых случаев идентификации автора исходного кода программы, важно проверить и сложные, чтобы убедиться в устойчивости усовершенствованной методики. К таким случаям относятся обфускация, следование стандартам кодирования, командная разработка и добавление искусственно сгенерированных кодов.

В табл. 6 представлены результаты идентификации автора обфусцированного исходного кода. В качестве обфускатора использовался AnalyzeC [24]. Процесс обфускации AnalyzeC предполагает:

– полное удаление комментариев и пробелов;

– добавление псевдосложного кода, не изменяющего функциональность программы;

– директив препроцессора;

– замену строк шестнадцатеричным эквивалентом.

Результаты, полученные ансамблем, сопоставимы с полученными ранее [23], т.е. ансамбль негативного влияния на этот случай не оказывает.

Таблица 6

**Результаты для обфусцированных исходных кодов**

| Число файлов | 10 | 20 | 30 |
|---|---|---|---|
| 5 авторов | 0,85 | 0,9 | 0,91 |
| 10 авторов | 0,72 | 0,78 | 0,85 |
| 20 авторов | 0,64 | 0,72 | 0,75 |

Следующий случай – идентификация автора исходного кода, написанного командой разработчиков. В этом случае программисты используют систему управления версиями (GitLab, GitHub) и фиксируют изменения в репозитории проекта с помощью коммитов. Исходный код одной программы может содержать признаки сразу нескольких авторов. Поэтому возможность установления авторства на основании коммитов особенно важна.

Информация о коммитах, их содержимом и авторах была получена в процессе сбора данных при помощи API GitHub. В табл. 7 представлены результаты идентификации автора исходного кода, сформированного из коммитов. Прирост точности, полученный ансамблем классификаторов вместо отдельной HNN [23], составил в среднем 0,03.

Таблица 7

**Результаты для обфусцированных исходных кодов**

| Число файлов | 10 | 20 | 30 |
|---|---|---|---|
| 5 авторов | 0,89 | 0,94 | 0,97 |
| 10 авторов | 0,86 | 0,91 | 0,94 |
| 20 авторов | 0,83 | 0,87 | 0,91 |

Случай, вызвавший наибольшие сложности в ранних исследованиях, заключается в использовании исходного кода, написанного в соответствии со стандартами кодирования (табл. 8). Такой код пишется разработчиками с целью упрощения поддержки, а также улучшения читабельности кода, но сводит к минимуму уникальные признаки автора-программиста. Для оценки использовались исходные коды Linux Kernel [25], написанные на C/C++, в соответствии с общепринятыми стандартами. Для данного случая также был получен прирост, составивший в среднем 0,03, в сравнении с использованием HNN в отдельности [23].

Таблица 8

**Результаты для исходных кодов, написанных по стандартам кодирования**

| Наличие стандарта | Число файлов | 5 000 | 7 000 | 10 000 |
|---|---|---|---|---|
| Без стандартов | 10 | 0,76 | 0,83 | 0,89 |
| Со стандартами | | 0,42 | 0,48 | 0,62 |
| Без стандартов | 20 | 0,92 | 0,95 | 0,96 |
| Со стандартами | | 0,69 | 0,76 | 0,83 |
| Без стандартов | 30 | 0,95 | 0,97 | 0,98 |
| Со стандартами | | 0,75 | 0,84 | 0,89 |

Последний сложный случай вызван ростом популярности моделей семейства Generative Pre-trained Transformer (GPT) и их эффективностью для генерации исходных кодов программ. Эксперименты были проведены для наиболее сложного случая анализа искусственно сгенерированного кода – разграничение авторства между разными генеративными моделями – GPT-3, GPT-2 и RuGPT-3 (табл. 9). В данном случае использование ансамбля оказало положительное влияние и дало прирост в точности более 0,07 в сравнении с HNN по отдельности [23].

Таблица 9

**Результаты для искусственно-сгенерированных кодов**

| 10 файлов | 20 файлов | 30 файлов |
|---|---|---|
| 0,86 | 0,9 | 0,94 |

Для того чтобы убедиться в том, что усовершенствованная методика не вносит негативного эффекта в сложных случаях в сравнении с простыми, было решено провести T-тест для парных выборок. Его смысл заключается в попарном сравнении результатов перекрестной проверки в простых и сложных случаях и оценке *p*-значения для каждого из них в отдельности. Нулевая гипотеза, состоящая в том, что разница не является статистически значимой, принимается при *p*-значениях свыше 0,05. Альтернативная гипотеза предполагает критическую потерю в точности. Итак, для пары результатов «простой исходный код» – «обфусцированный исходный код» *p*-значение составило 2,35. Для пары «простой исходный код» – «коммит» – 0,06. Для пары «простой исходный код» – «искусственно сгенерированный исходный код» – 0,88. И для пары «простой исходный код» – «код, написанный по стандартам кодирования» – 1,83. Ни одна из пар не дала результата ниже границы в 0,05, т.е. разница в точности между простыми и сложными случаями критической не является.

Также был проведен ряд экспериментов, чтобы удостовериться, что усовершенствованная методика не уступает в точности аналогам, разработанным другими исследователями. Так как в большинстве работ для оценки своих подходов они использовали набор данных GCJ, было решено провести дополнительные эксперименты по анализу дизассемблированных кодов с помощью усовершенствованной методики. В набор были включены данные GCJ 2009 и 2010 для более объективного сравнения. Метрики и число авторов были взяты в соответствии с указанными в статьях. Следует отметить, что в одной из работ была использована отличная от точности метрика эффективности [15]. Метрика F0,5, применяемая авторами, рассчитывается как

$$F0{,}5=\frac{1{,}25\times(\text{precision}\times\text{recall})}{0{,}25\times(\text{precision}+\text{recall})}. \qquad (1)$$

Результаты данных экспериментов приведены в табл. 10. Из таблицы видно, что усовершенствованная методика на основе ансамбля классификаторов не уступает методам, предложенным другими исследователями ранее. В части случаев ансамбль проде-

монстрировал значительный прирост в точности. Кроме того, полученные ансамблем на GCJ результаты оказались лучше полученных на GitHub. Это объясняется тем, что оценка точности классификаторов на данных GCJ не является достаточно объективной из-за их специфики. Такие данные являются однородными и позволяют классификатору сосредоточиться только на авторских признаках, игнорируя функциональные отличия программ и их специфику. В отличие от GCJ, набор данных GitHub состоит из неоднородных данных (разный опыт программистов и многообразие решаемых задач), а эксперименты моделируют решение реальных задач. Это делает оценку более объективной.

Таблица 10

**Результаты для исходных кодов, написанных по стандартам кодирования**

| Работа | Число авторов | Метрика | Результат авторов | Наш результат | Разница в эффективности |
|---|---|---|---|---|---|
| Alrabaee S. [17] | 5 | F0,5 | 0,8 | 0,96 | + 0,16 |
| | 10 | F0,5 | 0,76 | 0,93 | + 0,17 |
| | 20 | F0,5 | 0,71 | 0,88 | + 0,17 |
| Rosenblum N. [9] | 5 | Точность | 0,93 | 0,97 | + 0,04 |
| | 20 | Точность | 0,77 | 0,87 | + 0,1 |
| Alrabaee S. [19] | 3 | Точность | 0,93 | 0,99 | + 0,06 |
| | 5 | Точность | 0,9 | 0,97 | + 0,07 |
| | 7 | Точность | 0,82 | 0,96 | + 0,14 |

**Заключение**

Согласно полученным результатам, исходную методику на основе HNN удалось усовершенствовать, адаптировав под анализ дизассемблированных кодов программ, и сделать универсальное решение на основе ансамбля классификаторов.

Исходя из проведенных исследований, можно выделить следующие преимущества методики:

1. Универсальность. Возможность определять автора как бинарного, так и исходного кода на основе текста программы и выделенных признаков.

2. Эффективность. Точность методики независимо от сложности задачи и специфики данных во всех экспериментах превышает 0,85. Этого достаточно для использования методики при решении практических задач.

3. Независимость от осложняющих факторов. Методика устойчива как к преднамеренным (обфускация, стандарты кодирования, командная разработка, искусственная генерация), так и к непреднамеренным (изменения в стиле, связанные с увеличением опыта и повышением квалификации программиста) искажениям кода программы.

К ограничениям методики, а также возможностям ее дальнейшего совершенствования можно отнести следующие аспекты. Во-первых, для достижения высокой точности идентификации автора дизассемблированного кода программа должна быть предварительно деобфусцирована, так как даже минимальная обфускация существенно снижает эффективность методики. Во-вторых, результаты напрямую зависят от количества авторов и обучающих данных на каждого автора. При увеличении числа авторов или нехватке числа обучающих экземпляров эффективность системы снижается.

Данная работа выполнена при финансовой поддержке Министерства науки и высшего образования РФ в рамках базовой части государственного задания ТУСУРа на 2023–2025 гг. (проект № FEWM-2023-0015).

*Литература*

1. A Forensic Traceability Index in Digital Forensic Investigation / S. Rahayu, S. Shahrin, N. Hafeizah, R. Yusof, M.F. Abdollah // Journal of Information Security. – 2013. – Vol. 4, No. 1. – P. 19–32.

2. Schleimer S. Winnowing: local algorithms for document fingerprinting / S. Schleimer, D.S. Wilkerson, A. Aiken // Proceedings of the 2003 ACM SIGMOD international conference on Management of data (SIGMOD '03). – Association for Computing Machinery, NewYork, NY, USA, 2003. – P. 76–85.

3. Large-Scale and Language-Oblivious Code Authorship Identification / M. Abuhamad, T. AbuHmed, A. Mohaisen, D. Nyang // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. – Toronto, ON, Canada, 2018. – P. 101–114.

4. RoPGen: Towards Robust Code Authorship Attribution via Automatic Coding Style Transformation / L. Zhen, G. Chen, C. Chen, Y. Zou, S. Xu // Proceedings of the 2022 IEEE 44th International Conference on Software Engineering (ICSE). – Pittsburgh, PA, USA, 2022. – P. 1906–1918.

5. Holland C. Code authorship identification via deep graph CNNs / C. Holland, N. Khoshavi, G. Jaimes // Proceedings of the 2022 ACM Southeast Conference (ACM SE '22). – 2022. – P. 144–150.

6. Bogomolov E. Authorship attribution of source code: A language-agnostic approach and applicability in software engineering / E. Bogomolov, V. Kovalenko, Y. Rebryk, A. Bacchelli, T. Bryksin // Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. – Athens, Greece, 2021. – P. 932–944.

7. Ullah F. Source code authorship attribution using hybrid approach of program dependence graph and deep learning model / F. Ullah, J. Wang, S. Jabbar, F. Al-Turjman, M. Alazab // IEEEAccess. – 2019. – Vol. 7. – P. 141987–141999.

8. Binary Authorship Verification with Flow-aware Mixture-of-Shared Language Model. – URL: https://arxiv.org/pdf/2203.04472, свободный (дата обращения: 18.11.2023).

9. Rosenblum N. Who Wrote This Code? Identifying the Authors of Program Binaries / N. Rosenblum, X. Zhu, B.P. Miller. – URL: https://pages.cs.wisc.edu/~jerryzhu/pub/Rosenblum11Authorship.pdf, свободный (дата обращения: 18.11.2023).

10. Alrabaee S. BinGold: Towards robust binary analysis by extracting the semantics of binary code as semantic flow graphs (SFGs) / S. Alrabaee, L. Wang, M. Debbabi // Dig. Investig. – 2016. – Vol. 18. – P. 11–22.

11. Caliskan-Islam A. When Coding Style Survives Compilation: De-anonymizing Programmers from Executable Binaries. – arXiv preprint. – arXiv:1512.08546. – 2017. – URL: https://arxiv.org/abs/1512.08546, свободный (дата обращения: 21.10.2023).

12. Alrabaee S. OBA2: An Onion Approach to Binary code Authorship Attribution / S. Alrabaee, N. Saleem, S. Preda, L. Wang, M. Debbabi // Dig. Investig. – 2014. – Vol. 11. – P. 94–103.

13. Caliskan-Islam A. Deanonymizing programmers via code stylometry // Proceedings of the 24th USENIX Security Symposium, Washington. – 2015. – P. 255–270. – URL: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-caliskanislam.pdf, свободный (дата обращения: 18.11.2023).

14. Alrabaee S. On the Feasibility of Malware Authorship Attribution / S. Alrabaee, P. Shirani, M. Debbabi, L. Wang // Dig. Investig. – 2016. – Vol. 28. – P. 3–11.

15. Zia T. Source Code Author Attribution Using Author's Programming Style and Code Smells / T. Zia, M.I.J. Ilyas // Intell. Syst. Appl. – 2017. – Vol. 5. – P. 27–33.

16. Google Code Jam. – URL: https://codingcompetitions.withgoogle.com/codejam, свободный (дата обращения: 18.11.2023).

17. Codeforces. – URL: https://codeforces.com, свободный (дата обращения: 18.11.2023).

18. GCC, the GNU Compiler Collection. – URL: https://gcc.gnu.org, свободный (дата обращения: 21.10.2023).

19. IDA Pro. – URL: https://hex-rays.com/ida-pro, свободный (дата обращения: 18.11.2023).

20. Куртукова А.В. Идентификация автора исходного кода методами машинного обучения / А.В. Куртукова, А.С. Романов // Труды СПИИРАН. – 2019. – № 18. – С. 741–765.

21. Kurtukova A. Source Code Authorship Identification Using Deep Neural Networks / A. Kurtukova, A. Romanov, A. Shelupanov // Symmetry. – 2020. – Vol. 12. – 2044. DOI:10.3390/sym12122044

22. Kurtukova A. Complex Cases of Source Code Authorship Identification Using a Hybrid Deep Neural Network / A. Kurtukova, A. Romanov, A. Shelupanov, A. Fedotova // Future Internet. – 2022. – Vol. 14. – P. 287. DOI: /10.3390/fi14100287

23. AnalyzeC. – URL: https://github.com/ryarnyah/AnalyseC, свободный (дата обращения: 18.11.2023).

24. Linux Kernel Coding Style. – URL: https://www.kernel.org/doc/html/v4.10/process/coding-style.html (дата обращения: 18.11.2023).

**Куртукова Анна Владимировна**
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.: +7-905-991-67-13
Эл. почта: av.kurtukova@gmail.com

**Романов Александр Сергеевич**
Канд. техн. наук, доцент каф. КИБЭВС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-34-26
Эл. почта: alexx.romanov@gmail.com

**Шелупанов Александр Александрович**
Д-р техн. наук, проф., президент ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 90-71-55
Эл. почта: saa@tusur.ru

Kurtukova A.V., Romanov A.S., Shelupanov A.A.
**Development of a methodology for identifying the authorship of binary and disassembled program codes based on an ensemble of modern natural language processing methods**

This article is part of a series of studies aimed at solving problems of identifying the authorship of source code. The analysis of binary or disassembled code is a critical task in information security, software development, and computer forensics due to the need to protect intellectual property and copyright, as well as to identify the authors of malware. Any program is a machine code that can be disassembled (converted into text in assembly language) using specialized tools and analyzed for authorship by analogy with text in natural language. To solve this problem, the article proposes a technique based on the fastText ensemble, support vector machine (SVM) and the author-developed hybrid neural network. The proposed methodology was evaluated on source codes in C and C++ languages, collected from the GitHub and Google Code Jam platforms, compiled into executable files and disassembled using reverse engineering tools. The average accuracy of identifying the author of disassembled code using the proposed method was more than 0.9. The technique was also tested on source codes, resulting in an average accuracy of 0.96 in simple cases and more than 0.85 in complex cases (obfuscation, coding standards, etc.).
**DOI:** 10.21293/1818-0442-2023-26-4-53-60

*References*

1. Rahayu S., Shahrin S., Hafeizah N., Yusof R., Abdollah M.F. A Forensic Traceability Index in Digital Forensic Investigation. *Journal of Information Security*, 2013, vol. 4., no. 1, pp. 19–32.

2. Schleimer S., Wilkerson D.S., Aiken A. Winnowing: local algorithms for document fingerprinting. *Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data (SIGMOD '03),* Association for Computing Machinery, New York, NY, USA, 2003, pp. 76–85.

3. Abuhamad M., AbuHmed T., Mohaisen A., Nyang D. Large-Scale and Language-Oblivious Code Authorship Identification. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Toronto, ON, Canada, 2018, pp. 101–114.

4. Zhen L., Chen G., Chen C., Zou Y., Xu S. RoPGen: Towards Robust Code Authorship Attribution via Automatic Coding Style Transformation. *Proceedings of the 2022 IEEE 44th International Conference on Software Engineering* (*ICSE*), Pittsburgh, PA, USA, 2022, pp. 1906–1918.

5. Holland C., Khoshavi N., Jaimes G. Code authorship identification via deep graph CNNs. *Proceedings of the 2022 ACM Southeast Conference (ACM SE '22),* 2022, pp. 144–150.

6. Bogomolov E., Kovalenko V., Rebryk Y., BacchelliA., Bryksin T. Authorship attribution of source code: A language-agnostic approach and applicability in software engineering.

*Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, Athens, Greece, 2021, pp. 932–944.

7. Ullah F., Wang J., Jabbar S., Al-Turjman F., Alazab M. Source code authorship attribution using hybrid approach of program dependence graph and deep learning model. *IEEEAccess*, 2019, vol. 7, pp. 141987–141999.

8. Song Q., Zhang Y., Ouyang L., Chen Y. BinMLM: Binary Authorship Verification with Flow-aware Mixture-of-Shared Language Model. Available at: https://arxiv.org/pdf/2203.04472, free (Accessed: November 18, 2023).

9. Rosenblum N., Zhu X., Miller B.P. Who Wrote This Code? Identifying the Authors of Program Binaries. Available at: https://pages.cs.wisc.edu/~jerryzhu/pub/Rosenblum11Authorship.pdf, free (Accessed: November 18, 2023).

10. Alrabaee S., Wang L., Debbabi M. BinGold: Towards robust binary analysis by extracting the semantics of binary code as semantic flow graphs (SFGs). *Digital Investigation*, 2016, vol.18, pp. 11–22.

11. Caliskan-Islam A. When Coding Style Survives Compilation: De-anonymizing Programmers from Executable Binaries. Available at: https://arxiv.org/abs/1512.08546, free (Accessed: November 18, 2023).

12. Alrabaee S., Saleem N., Preda S., Wang L., DebbabiM. OBA2: An Onion Approach to Binary code Authorship Attribution. *Digital Investigation*, 2014, vol. 11, pp. 94–103.

13. Caliskan-Islam A., Harang R., Liu A. Deanonymizing programmers via code stylometry. *Proceedings of the 24th USENIX Security Symposium*, 2015, pp. 255–270. Available at: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-caliskan-islam.pdf, free (Accessed: November 18, 2023).

14. Alrabaee S., Shirani P., Debbabi M., Wang L. On the Feasibility of Malware Authorship Attribution. *Digital Investigation,* 2016, vol. 28, pp. 3–11.

15. Zia T., Ilyas M.I.J. Source Code Author Attribution Using Author's Programming Style and Code Smells. *Intelligent SystemswithApplications*, 2017, vol. 5, pp. 27–33.

16. Google Code Jam. Available at: https://codingcompetitions.withgoogle.com/codejam, free (Accessed: November 18, 2023).

17. Codeforces. Available at: https://codeforces.com/, free. (Accessed: October 25, 2023).

18. GCC, the GNU Compiler Collection. Available at: https://gcc.gnu.org, free (Accessed: November 18, 2023).

19. IDA Pro. Available at: https://hex-rays.com/ida-pro/, free (Accessed: October 25, 2023).

20. Kurtukova A.V., Romanov A.S. [Identification author of source code by machine learning methods]. *SPIIRAS Proceedings*, 2019, vol. 18, no. 3, pp. 741–765 (in Russ.).

21. Kurtukova A., Romanov A., Shelupanov A. Source Code Authorship Identification Using Deep Neural Networks. *Symmetry,* 2020, Vol. 12, 2044. DOI: 10.3390/sym12122044.

22. Kurtukova A., Romanov A., Shelupanov A., Fedotova A. Complex Cases of Source Code Authorship Identification Using a Hybrid Deep Neural Network. *Future Internet*, 2022, vol. 14, 287. DOI: /10.3390/fi14100287.

23. AnalyzeC. Available at: https://github.com/ryarnyah/AnalyseC, free (Accessed: November 18, 2023).

24. Linux Kernel Coding Style. Available at: https://www.kernel.org/doc/html/v4.10/process/coding-style.html, free (Accessed: November 18, 2023).

---

**Anna V. Kurtukova**
Postgraduate student, Department of Complex Information Security of Electronic Computer Systems (KIBEVS),
Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-905-991-67-13
Email: av.kurtukova@gmail.com

**Aleksandr S. Romanov**
Candidate of Sciences in Engineering, Associate professor, KIBEVS TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 41-34-26
Email: alexx.romanov@gmail.com

**Alexandr A. Shelupanov**
Doctor of Science in Engineering, Professor, President TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 90-71-55
Email: saa@tusur.ru

УДК 004.023, 004.94, 316.3, 316.4

**В.М. Саклаков**

# Методология цифрового социологического исследования: общественная система как базовый инструмент моделирования

Проведен анализ существующих подходов к проведению социологического исследования, дана оценка системных разрывов в цикле моделирования объектов социологии. Предложена процедура моделирования сложных общественных взаимодействий, основанная на понятии «общественная система». Разработаны принципы ее моделирования, охватывающие уровни взаимодействия с внешней средой, состава и структуры. Представлены модель общественной системы, элементы которой обладают набором внутренних параметров, и алгоритм ее взаимодействия со средой. Для облегчения восприятия большого количества элементов, выделяемых из собранных эмпирических данных, финальный результат исследования предложено выводить на специальную карту. Первичная апробация, проводимая на основе сообщений из социальной сети, позволила выделить элементы сложной общественной системы и показать характер их взаимодействия. Сделан вывод о применимости методологии как инструмента мониторинга и прогнозирования сложных общественных взаимодействий.

**Ключевые слова:** общественная система, взаимодействие сложных субъектов общества, цифровая социология, общая теория систем, анализ данных, экстремизм, социальные сети.
**DOI:** 10.21293/1818-0442-2023-26-4-61-77

Процессы, в настоящее время протекающие как в российском, так и во многих зарубежных обществах, генерируют сильные пертурбационные эффекты. Эксперты из научной [1] и бизнес-среды [2], сферы государственного управления [3] трактуют их возникновение как следствие новой промышленной революции. В ответ на вызовы времени государства разрабатывают стратегии и программы развития: стратегия развития информационного общества Российской Федерации на 2017–2030 гг., индустрия 4.0 в Германии, цифровая экономика (Digital economy agenda) в США и др. Происходящая трансформация должна обеспечить рост производительности труда в отраслях, применяющих новые принципы разработки технологий и производства продуктовых линеек на их основе.

Одним из значимых результатов происходящего перехода станет, как и в предыдущих случаях [4], полное изменение пропорций, сложившихся в обществе экономических, социальных и других организационных систем, их структуры, методов взаимодействия. В уходящей формации они генерировали относительно небольшое количество данных и передавали их по малому количеству шлюзов: теле- и радиоканалам, газетам, сарафанному радио, статистическим сборникам и т.п. Мониторинг и прогнозирование таких систем проводился с помощью статистических и социологических исследований различного масштаба и глубины.

На сегодняшний момент ситуация меняется [5]: новые методы взаимодействия предполагают более интенсивный обмен данными, ведущийся огромным числом людей на ограниченном количестве крупных технологических платформ, таких как социальные сети, а также корпоративные ресурсы. Таким образом, количество шлюзов обмена данными выросло лавинообразно, а их мониторинг осуществляется на основе единой политики таких платформ.

В условиях активно формирующейся общественной формации традиционные методы социологической науки перестали показывать достаточную эффективность. Уже при выборке в 1 000 человек ими демонстрируются следующие узкие места [6, 7]:

1. Ограниченная география исследования.
2. Потенциальное выпадение значимых массивов данных из выборки случайным образом.
3. Низкая средняя скорость исследования – от 5–15 дней до 1 месяца.
4. Высокая трудоемкость, повышенные требования к квалификации социолога.
5. Усталость исследуемого поля после одной, максимум двух итераций.
6. Высокая скорость устаревания данных, низкая частота повторного использования.
7. Субъективная достоверность – респонденты часто дают ответы, совпадающие с социальными нормами, либо иным образом искажают данные.
8. Высокая средняя себестоимость исследования – в России от 75 до 500 тыс. руб.

К началу 2010-х гг. сложилось два значимых фактора: 1) многие организации активно проводили цифровизацию своей деятельности, 2) сформировалось ядро пользователей социальных сетей. Таким образом, появилась возможность накопления больших объемов данных и возник потенциал для вывода качества социологических исследований на новый уровень. На этой базе возник рынок анализа данных, предлагающий множество концепций и методов. Однако существовавшие на нем решения ориентированы на повышение эффективности внутренних процессов организаций-заказчиков их услуг [8, 9]. Лишь небольшое количество коммерческих компаний занимается аналитикой сложных взаимодействий в обществе, причем зачастую в виде побочной деятельности, но не системной и открытой междисциплинарной научной работы [10].

**Целями работы** являются:

1. Анализ современных подходов к описанию общественных взаимодействий методами: а) традиционной социологической науки, б) работы с цифровыми данными.

2. Разработка методологии цифрового социологического исследования.

3. Разработка средств автоматизации цифрового социологического исследования.

4. Апробация методологии с опорой на данные, генерируемые в цифровом пространстве.

Данный комплекс целей имеет системный характер и будет достигаться поэтапно, в рамках настоящей и будущих работ. В данной статье будут в достаточной мере достигнуты первая и вторая, а третья и четвертая – лишь частично – в качестве первичной апробации. Создание данной методологии, при будущем решении задач ее технического обеспечения, позволит добиться следующих параметров при проведении социологических исследований:

1. Размер и география выборки ограничены лишь доступом к цифровым массивам данных.

2. Автоматизация снижает время сбора, обработки и интерпретации данных, позволяя увеличить масштаб исследований. При этом уменьшится число исполнителей, а набор требований к их квалификации сместится в сторону позиции аналитика данных.

3. Бесконтактный сбор данных снимает эффект «усталости» исследуемого поля и увеличивает их репрезентативность.

4. Накопление данных о множестве элементов общества за длительный период позволит на первом этапе создать их цифровые тени, а затем – цифровых двойников [11].

5. Себестоимость исследования определяется главным образом программными и вычислительными возможностями, а также условиями доступа к программному интерфейсу пользователя (API) коммуникационных сервисов и базам данных.

Таким образом, разработка методологии показывает свою актуальность, она может быть использована при реализации «Стратегии развития информационного общества Российской Федерации на 2017–2030 гг.», программ «Национальная технологическая инициатива», «Цифровая экономика Российской Федерации», «Доктрины информационной безопасности». Однако необходимо учитывать и ограничения, существующие на текущем этапе:

1. Ориентация преимущественно на сферы с интенсивной генерацией и обменом данными между субъектами взаимодействия.

2. Цифровая фиксация данных и доступ к ним затруднены существующей инфраструктурой, а большое количество шумов затрудняет их анализ.

3. Исследование не обязательно должно опираться исключительно на данные, собранные в цифровом пространстве, – традиционные социологические методы также могут быть их источником, однако желательно проводить их интеграцию в едином хранилище.

## 1. Современное состояние предметной области

В настоящем разделе проводится классификация применяемых за последние восемь лет методов социологического исследования. Автор рассматривает опубликованные работы с позиции полноты применения инструментов в цикле социологического исследования существующих в обществе систем (табл. 1). Безусловно, объем публикаций гораздо шире представленного. В статье проводится анализ совокупности наиболее характерных для отрасли кластеров работ, подкрепленный ссылками на отдельные из них.

Таблица 1

**Инструменты цикла социологического исследования**

| Инструмент | Задача инструмента |
|---|---|
| Эмпирические данные | Полнота и достоверность процесса обработки данных |
| Методы обработки данных | Выделение признаков сущностей в объекте анализа |
| Общая теория систем | Анализ и синтез сущностей в единую модель |
| Диффузия моделей | Модификация систем |

### *1.1. Традиционные методы социологического исследования*

Выделим кластеры исследований, проводимых на принципах уходящей общественной формации:

1. Моделирование протекающих в обществе процессов на основе теоретического обобщения множества опубликованных исследований.

Одна из часто встречающаяся категорий работ не только в социологии, но и в общественных науках в целом. После проведения объективации некоторого процесса или явления происходит подборка публикаций по данной тематике. При этом возникает частичный или полный отрыв от эмпирических данных, представленных в них, либо данных из других источников. Результат таких исследований, опирающийся на набор модельных построений авторов, может обладать разной степенью правдоподобности, но зачастую недостаточно достоверен [12–15].

2. Узконаправленные прикладные социологические исследования.

Так же достаточно распространенная категория работ, проводимых для узкого круга стейкхолдеров* в рамках их отрасли или сферы деятельности. Масштаб и глубина таких исследований, как правило, жестко ограничены целями и организационными возможностями их заказчиков [16, 17]. Некоторым исключением тут может выступать аналитика, проводимая организациями с более гибкой структурой, имеющими механизмы самостоятельного предложения направления работ, например научные группы в профильных институтах [18–19].

В данной категории работ обрабатываются статистические данные, однако слабым местом зачастую

*Стейкхолдер – организационная система, являющаяся выгодоприобретателем от потенциального достижения определенных результатов.

является недостаточно проработанный этап объективации, что приводит к системным разрывам в описании комплексного явления или процесса. С другой стороны, узкая направленность позволяет, с учетом ограничений, увеличить их детализацию.

3. Исследование крупных общественных процессов или явлений.

Подобный класс исследований, как правило, требует больших, чем в предыдущем случае, временных, организационных и иных видов затрат. Объект анализа задается достаточно широко, что позволяет охватить процессы, явления и взаимодействующих в обществе субъектов большего масштаба. Зачастую применяются статистические или математические методы к лонгитюдным выборкам данных. Слабыми местами могут являться: 1) несоответствие поставленных целей и задач, а также применяемых методов сложности исследуемой системы; 2) ограниченная глубина получаемой модели; 3) центрированность на одной из частей определенной системы в отрыве от других взаимодействующих с ней элементов [20–22].

4. Методологические и методические подходы к социологическим исследованиям.

Авторы данной категории работ предлагают системы процедур моделирования протекающих в обществе процессов с определенной исследовательской позиции – прогнозной [23], познавательного моделирования [24] и т.д. Часть работ центрируется лишь на определенных процедурах, например объективации [25]. В отдельных работах, например [26–28], можно увидеть зачатки описания характеристик процесса социального взаимодействия. Однако заданный на начальном этапе объект анализа и вытекающие из него целевые ограничения позволяют получить лишь локальные результаты, обладающие недостаточным потенциалом для масштабирования. Одна из главных проблем данных работ – попытка описания комплексной модели с применением лишь инструментария высшего (методологического) уровня обобщения, не уделяя достаточного внимания уровням системному и (или) практическому. При этом применяемый инструментарий может не в полной мере соответствовать данному уровню или относится к другому, что приводит к ошибкам. Часть работ имеет связанность между уровнями обобщения и использует соответствующий им инструментарий, при этом опираясь на обработку статистических данных [29–31]. Также публикуются работы, рассматривающие применяемые группами социологов методы через заданную матрицу критериев [32].

5. Описание процесса развития социологической науки.

Самая малочисленная категория работ с точки зрения возможностей реального прогнозирования, что обусловлено недостаточной опорой на эмпирические данные (либо их слабой структуризацией) и ориентацией на ретроспективу. Аналитика в основном ведется методами обобщения множества ранее опубликованных работ и интервьюирования [33–36]. Лишь некоторые социологи применяют математический аппарат для обработки данных, что значимо увеличивает полезность извлекаемых данных и упрощает их анализ [37]. Авторы отдельных работ, рассматривающие современное состояние отрасли социологических исследований, замечают конкурентное взаимодействие сложившихся в обществе систем, однако не имеют комплексной методологии и целеполагания для проведения анализа с этой позиции [38].

**Итоги.** С точки зрения полноты цикла моделирования существующих в обществе систем (табл. 1) традиционные методы социологической науки все еще позволяют получать значимые результаты. С другой стороны, явными становятся и накопленные противоречия в виде недостаточной связанности применяемых инструментов в целом по отрасли, в том числе низкой степени их совокупной автоматизации. Возможности сбора данных, их обработки и моделирования систем на их основе ограничены техническими и организационными возможностями разрозненных исследовательских групп. При этом сами эмпирические данные, собранные традиционными методами, могут обладать большей или меньшей значимостью в общей выборке, однако явно уступают в динамике объема генерации, фиксации и сбора данных цифровым. На заключительном этапе диффузия полученных моделей и дальнейшая интеграция извлеченных знаний во множество систем-стейкхолдеров также затруднена, т.к. зачастую требует их сложной реконфигурации.

### *1.2. От традиционных социологических исследований к работе с цифровыми данными*

Новые возможности для моделирования социологических объектов открылись с развитием коммуникационных сетей, генерирующих огромное количество данных, ключевую роль которых отмечают эксперты из разных отраслей [39–40].

Внедрение информационных технологий в работу с ними позволило модифицировать инструменты в цикле моделирования систем и получать результаты, отличные от тех, что могли предоставить традиционные методы. При этом характер подобных модификаций разделился на два направления: 1) повышение эффективности отдельных вех в рамках инструментов цикла и 2) сквозное связывание всех инструментов. Выделены основные кластеры исследований:

1. Аналитика активности участников сообществ (от «Dark Web» до открытых).

По ключевым словам в социальных сетях отбираются сообщения, включающие в себя наборы метаданных, например геолокацию пользователя. В зависимости от масштаба исследуемого объекта и уровня автоматизации процесса их обработка может вестись на основе:

а) сопоставления сообщений групп пользователей с реальными событиями, такими как незаконный оборот запрещенных веществ и предметов [41], террористическая активность [42] или процессы радикализации сообществ [43];

б) инструментария математической науки и машинного обучения, позволяющего, к примеру, классифицировать семантическую тональность сообщений пользователей [44].

В предлагаемых моделях, как правило, не в полной мере проработан этап объективации, что отрицательно сказывается на дальнейшем применении инструментария общей теории систем, также применяемой на недостаточном уровне. Данный фактор накладывает критические ограничения на всю процедуру моделирования, снижая полезность извлекаемых данных.

2. Аналитика участников сообществ.

Работы, описанные в предыдущем пункте, ориентированы на рассмотрение *процессов* в отрыве от их участников, в настоящем – фокус на *составе* и *структуре* участников сообществ. Сбор данных осуществляется из социальных сетей, а обработка, как правило, является многомерной – применяется множество инструментов: от сложных математических моделей до синтеза связей пользователей посредством теории графов. Полезность извлекаемых данных зависит от целевых ограничений, заданных при объективации, – от описания определенной системы [45] до взаимодействия множества систем [46].

3. Аналитика акторов по закрытым базам данных.

Настоящий кластер работ во многом связан с предыдущими, однако стоит особняком из-за использования данных с ограниченным доступом. Сбор данных может вестись комбинированно из открытых (социальные сети) и закрытых источников (внутренние информационные ресурсы предприятий) либо только из последних. Для обработки применяются инструментарий системного анализа [47], математический аппарат и машинное обучение [48]. Среди узких мест выделяются значимые разрывы в цикле моделирования общественных процессов, их атомизация, а также получение локальных, слабо масштабируемых в иных средах результатов.

4. Цифровые социологические исследования.

Перспективный набор методик и методологий проведения социологических исследований и интерпретации их результатов [49–50]. В его основе лежат два принципиально новых фактора – возможность доступа к большому объему непрерывно генерируемых данных и возросший потенциал автоматизации их обработки при приемлемых затратах. Становление этого направления проходит в настоящее время, что обусловливает наличие работ разного охвата и глубины. Сам термин *цифровая социология* не является общепризнанным, а ряд авторов ошибочно ограничивает ее лишь «пониманием использования цифровых средств массовой информации как части повседневной жизни» [51]. Публикации не всегда позиционируются в рамках рассматриваемого направления, что существенно затрудняет их поиск и систематизацию [52, 53].

Другой проблемой может являться наличие значимых диспропорций в цикле моделирования. Например, в работе в достаточной мере применен инструментарий общей теории систем и математического обеспечения, но программное обеспечение имеет явно недостаточный потенциал, количество обработанных данных остается на уровне, достаточном лишь для уходящей общественной формации, а средства визуализации находятся на начальном стадии развития (или иные пропорции) [54–55]. При этом данный кластер работ является наиболее перспективным для модернизации, т.к., как правило, его методологическое ядро уже сформировано и нуждается в расширении, постоянном притоке новых данных, а также повышении эффективности программных средств. Вместе с тем нельзя не отметить существование работ, только маскирующихся под цифровое исследование [56].

**Итоги**. Основой для получения новых результатов в рассматриваемом кластере работ стала возможность ускоренной и регулярной фиксации огромного количества данных расширенным кругом специалистов. Их реакцией стали попытки модификации вех в каждом инструменте цикла моделирования систем.

Первые три кластера работ, рассмотренные в настоящем подразделе, идут по пути совершенствования лишь отдельных из них, что ограничивает эффекты от интеграции полученных знаний. Работы последнего кластера, напротив, с разной с степенью эффективности пытаются увязать между собой все четыре инструмента. Тем не менее на текущем этапе задача их сквозного связывания многими авторами задается скорее не напрямую, а на интуитивном уровне. Таким образом, накопленные противоречия между развитием коммуникационной инфраструктуры и возможностями существующих методов социологии позволяют, на основе цикла моделирования систем (см. табл. 1) сформулировать определение нового вида исследования:

*Цифровое социологическое исследование* – процесс динамического моделирования социологических объектов на основе устойчивых факторов: а) накопления данных из гетерогенных источников; б) выделения признаков сущностей в них, направленных на модификацию систем-стейкхолдеров.

### *1.3. Итоги раздела*

В современных условиях общество формирует огромные объемы фиксируемых данных. При этом отсутствует эффективный пакет технологий полного цикла моделирования сложных общественных взаимодействий, отвечающий требованиям новой общественной формации. Следствием проведения мониторинга недостаточно приспособленными инструментами становится принятие разрозненных, часто эклектичных стратегических решений и (или) управленческих мер по их реализации.

Многие агенты, сообщества и среды заинтересованы в разработке методологии социологического исследования, соответствующей новым условиям. На ее основе они смогут осуществлять мониторинг и прогнозирование на качественно новом уровне. С другой стороны, нужно понимать: методы работы с цифровыми данными не замещают собой методы традиционные, а наоборот – расширяют их потенциал.

**2. Общественная система как базовый инструмент моделирования сложных взаимодействий в социуме**

Во многих рассмотренных в предыдущем разделе работах фокус исследователя сосредоточен на аналитике *отдельных групп людей*, установок их поведения, социального состава, ценностей и т.д. Меньшая часть авторов в качестве объекта анализа выбирает *системы* различного уровня, имея при этом достаточный аналитический аппарат и набор эмпирических данных. Однако оба этих подхода имеют следующие узкие места.

Каждый человек принадлежит к некоторому конечному множеству сложившихся в обществе систем, а его действия обусловлены занимаемыми в них позициями. Их обособленный мониторинг вызывает разрывы в понимании как отдельных групп людей или организаций, так и систем, частью которых они являются. С одной стороны, прямой анализ огромного количества людей в отрыве от систем, агентами которых они являются, достаточно трудоемок и затратен, а в ряде случаев и в принципе не возможен даже бесконтактными методами цифровой социологии. С другой – методы выделения самих систем по определенным признакам также обладают ограниченным потенциалом без учета данных о деятельности их агентов.

Для расшивки обозначенных узких мест на первом этапе необходимо ввести ряд определений и понятий, описывающих применяемый инструментарий общей теории систем.

***2.1. Понятие общественной системы***

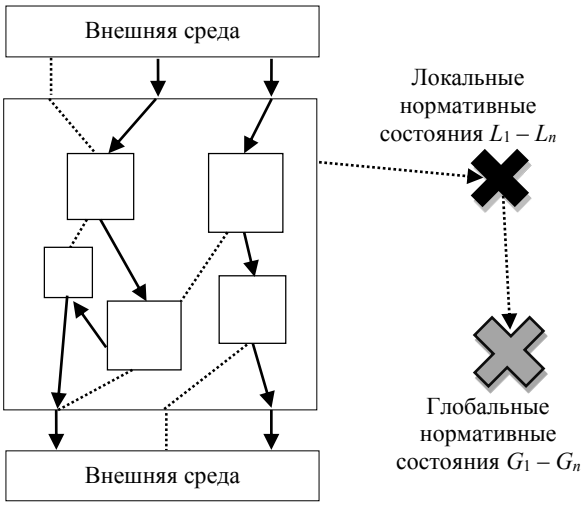
Понятие «общественная система» не является устоявшимся и в качестве прикладного инструмента, имеющего методологическую основу, применяется достаточно редко, особенно в цифровой социологии [57, 58]. Ряд научных работ, посвященных или близких к тематике исследования сложных общественных взаимодействий, описывает сущность, которую косвенно можно соотнести с рассматриваемой в настоящем разделе [59, 60]. Автор предлагает собственное понятие и вытекающую из него методологию как специализированный инструмент.

*Общественная система (ОС)* – целевое структурированное множество функционально, процессно и деятельностно обособленных от внешней среды элементов общества, взаимодействующих с ней как целое. С помощью теории систем [61] ОС можно описать как синтез моделей *состава*, *структуры*, *черного ящика*, формирующий модель *белого ящика*.

Основными свойствами любой ОС является ее *устойчивость* к воздействиям внешней среды, в том числе других систем, а также *целостность*. При этом последняя может обеспечиваться только до определенного порога, на котором она начинает критически сказываться на устойчивости. Подобная практика является традиционной и закреплена во многих нормативных документах ОС разного масштаба, например в [62]. Взаимодействия между ними может приводить к увеличению, снижению или полной утрате ими устойчивости и (или) целостности. Каждая система стремится к состояниям, в которых она с большей вероятностью по сравнению с альтернативами сможет сохранить устойчивость.

***2.2. Принципы моделирования ОС***

При анализе эмпирических данных о некоторых общественных системах появляется возможность обработки математическими и программными средствами наборов ее признаков в динамике. Непосредственно саму эмпирику может обеспечить сбор *цифровых следов* [63, 64], оставляемых агентами ОС в ходе взаимодействия. Такой инструмент уже используется аналитиками, однако зачастую они достаточно ограниченно вводят в общую картину модель «черного ящика», опираясь преимущественно на модели «состава» и «структуры». Для описания общественных систем, характера и методов их взаимодействия необходимо распределять получаемые данные по набору объектов в соответствии с выделенными признаками. Конечный набор признаков задается исследователем и зависит от качества и количества имеющихся данных. При этом для выделения объектов предлагается исходить из общих *принципов моделирования* – рис. 1. Их ядром является модель «белого ящика» [59], а в качестве приложений используются концепция целеустремленных систем [65] и алгоритм построения промежуточных моделей развития [66].




| Уровень | Обозначение |
|---|---|
| Взаимодействие с внешней средой | → |
| Состав | □ |
| Структура | - - - - - - - - - - - - - - |

Рис. 1. Принципы моделирования общественных систем

Любая общественная система имеет обособление от внешней среды, которое можно описать при помощи модели «черного ящика» как 1) *уровень взаимодействия с внешней средой.* Взаимодействие осуществляется двумя типами сущностей: первую можно представить при помощи модели состава как 2) *уровень состава*, вторую – при помощи модели структуры как 3) *уровень структуры*. Так, уровень 1

описывает *движение* к нормативному состоянию через взаимодействие с внешними объектами, 2 – *акторов* такого движения, 3 – их *коммуникацию*. Все множество таких элементов находится в постоянной динамике, однако воздействия каждого отдельного элемента являются дискретными, т.е. в конкретный временной отрезок могут не производиться.

Общественные системы имеют некоторое *базовое (фактическое)*, множество *локальных (промежуточных)* и *глобальное нормативное (желаемое) состояние*, к которому они стремятся для сохранения или увеличения параметров устойчивости и (или) целостности. Потребность их достижения приводит к взаимодействию ее элементов с внешней средой. Цифровые следы, позволяющие моделировать ОС, как правило, оставляются либо на уровне 1 в виде сообщений пользователей коммуникационных сервисов, либо на связке уровней 2 и 3 в виде таблиц активностей с набором переменных*.

Предложенные принципы моделирования имеют комплексный характер, т.е. распространяется на макро-, мезо- и микроуровни. Каждый субъект взаимодействия на своем уровне стремится к достижению нормативного состояния наиболее эффективным** из доступных способов. Для этого определяются необходимые, допустимые и неприемлемые элементы для собственной, а также общесистемной архитектуры, их пропорции и структура связей. Отклонение может возникать преимущественно в виде «выбросов», незначительно влияющих на систему в целом. Взаимодействие элементов общественных систем разного уровня возможно не напрямую, а только через создание условий на более высоком уровне для более низкого. Отдельные организации и люди включены в процесс взаимодействия через принадлежность ко множеству элементов ОС и не могут действовать вне таковых.

### *2.3. Модель общественной системы*

Первое, что необходимо сделать исследователю на подготовительном этапе работы, – провести базовое описание объекта анализа, т.е. рассматриваемых систем. Для их детализации предлагается использовать модель общественной системы: представим ее в виде матрицы, сущности которой описаны в подразд. 2.2 (табл. 2).

Таблица 2

**Модель общественной системы**

| Уровень ОС | Взаимодействия со средой | Состав | Структуры |
|---|---|---|---|
| Макро | Функции системы | Функциональные позиции | Институты |
| Мезо | Процессы, реализующие функции | Процессные позиции | Институциональные коммуникации |
| Микро | Профильная деятельность | «Облако» организаций | Организационные связи |

* Например – специальность, направление подготовки, данные об успеваемости и т.д.

** Эффективность может пониматься как результативность, отношение результатов и затрат, оптимальность [67].

На высшем уровне обобщения (макроуровень) выделяются *функции системы*, формирующиеся в ней в определенных пропорциях под воздействием внешней и внутренней среды. Вне зависимости от масштаба и сложности системы набор ее функций ориентирован на сохранение и увеличение показателей устойчивости и (или) целостности в процессе своего развития†. В отдельных случаях некоторые ОС могут снижать такие показатели, однако подобное стремление для них является девиантным. Для исполнения функций элементам уровня состава более низких уровней необходимо занять соответствующие *функциональные позиции*. При этом между ними возникают отношения взаимодействия, так называемые «правила игры» – *институты*††.

Для исполнения функций, на мезоуровне вырабатываются *реализующие их процессы*, образующие набор *процессных позиций* для элементов низшего уровня обобщения. Границы (принадлежность) таких позиций определяются позициями функциональными, которые они занимают. Институты на данном уровне детализируются до *институциональных коммуникаций* – их фактической реализации в виде совокупности связей между соответствующими процессными позициями.

Наконец на микроуровне складывается множество видов *профильной деятельности*. Она осуществляется целым *«облаком»* формальных и неформальных *организаций* в некотором смысле обособленно от конкретных исполнителей – юридических и физических лиц, общественных объединений и т.д. Их замена без модификации самой деятельности, либо элементов более высокого уровня не ведет к значимым изменениям на уровне всей ОС. Граница облака определяется занимаемой его элементами процессной позицией. При исполнении деятельности как между, так и внутри облаков возникают *организационные связи*.

Такая методика моделирования позволяет осуществлять комплексный мониторинг и прогноз существующих и потенциально формирующихся общественных явлений. При этом установление принадлежности к определенным общественным системам его участников не зависит от декларируемых ими целей и взглядов. Элементы, представленные в ячейках табл. 1, с математической и программной точек зрения являются многомерными массивами данных. При этом определение перечня классов для каждого элемента общественной системы остается открытой задачей, для решения которой необходимо обработать большое количество эмпирических данных – ей необходимо посвятить отдельную исследовательскую работу.

† Под термином «развитие» автор понимает переход ОС из базового состояния в нормативное.

†† Классическое понятие «институт», определяемое Д. Нортом как «нормы, правила и организации» [59], в текущем контексте необходимо сформулировать более четко: исключить из него элемент «организации», а также дополнить текстом: «…возникающие в процессе взаимодействия между функциональными позициями».

### *2.4. Взаимодействие общественной системы со средой*

Обобщенно процесс сохранения устойчивости и (или) целостности множеством общественных систем при ограниченности ресурсов вызывает явление, в науке определяемое термином «конкуренция». Подобный характер взаимодействия свойствен им вне зависимости от масштаба и сложности [68, 69]. Вступать в эффективное конкурентное взаимодействие с внешней средой для достижения нормативных состояний ОС может только при достаточной степени внутренней консолидации, также достигаемой в конкурентном процессе. При этом стремление общественных систем к нормативным состояниям, предполагающее взаимно пересекающиеся попытки использования ресурсов, приводит к двум типам взаимодействия на разных уровнях:

- Макроуровень: конструктивное / деструктивное.
- Мезоуровень: интеграция либо дезинтеграция.
- Микроуровень: кооперация либо санкции.

Конечный набор типов взаимодействия на каждом уровне может иметь разный характер. Например, деструктивное взаимодействие может вестись при стремлении к интеграции на мезоуровне и попеременно к кооперации и санкциям на микроуровне. При этом каждая ОС вырабатывает модель взаимодействия с внешней и внутренней средой не на основе объективной реальности, а исходя из выработанных механизмов сбора, накопления, обработки и аналитики данных. Таким образом для них формируется *внутренняя реальность*. В научном сообществе такое явление находится на ранней стадии исследования [70, 71] и часто ошибочно интерпретируется как «постреальность», «постправда» [72, 73].

Прежде чем описывать алгоритм взаимодействия ОС с внешней средой, необходимо сделать важное замечание – понятия «данные» и «информация» являются достаточно дискуссионными в науке [74]. Гипотеза автора настоящей работы заключается в том, что их определение является продуктом той системы деятельности [75], для которой оно разрабатывалось и не существует вне нее. Попытки выработки общенаучных определений могут приводить их частные вариации к общему подобию, однако при практическом применении они оказываются недостаточными или наоборот – избыточными.

Дадим описание алгоритма взаимодействия общественной системы с внешней средой (рис. 2). Он представляет собой цикл обработки наборов данных для выработки последовательности нормативных состояний и их достижения. В верхней части рисунка представлена стадия обработки, в нижней – метод обработки, в центре – ее результат.

1. **Фильтрация**. Модификация данных, собираемых в среде до состояния *информации** – множества распознанных по определенным признакам объектов.

* Такое понимание данных и информации не противоречит отечественному и международным стандартам [76, 77].

При этом одинаковые наборы данных, проходя стадию фильтрации в разных общественных системах, становятся уникальными, т.е. маркируются ими не одинаково.


Рис. 2. Цикл алгоритма взаимодействия общественной системы с внешней средой

2. **Интерпретация**. Модификация получаемой и накопленной информации до *концепции нормативного состояния* – определения текущего, множества локальных и глобального нормативных состояний. Проводится путем распределения информации по элементам ОС и ее отсеивания при несоответствии им. Подобное отсеивание может происходить и в случае затруднения достижения нормативного при ее прохождении на следующую стадию. При невозможности отсеивания информация может быть полностью или частично искажена.

3. **Организация**. Модификация концепции нормативного состояния до *плана нормативного состояния* – определения стратегии, методов и элементов-исполнителей, необходимых для его достижения. Проводится путем определения целеустремленности разных комбинаций элементов ОС – приоритета достижения ими нормативных состояний.

4. **Исполнение**. Модификация плана нормативного состояния до *фактического результата* – набора параметров общественной системы, которых фактически удалось достигнуть при стремлении к нормативным состояниям.

Для внедрения алгоритма необходимо учитывать его чувствительность к качеству данных. Преимущественно он ориентирован на их получение на уровне взаимодействия с внешней средой либо на его комбинации с уровнями состава и структуры.

### *2.5. Представление результатов и измерение в социологическом исследовании*

Финальным результатом обработки данных при проведении социологического исследования является их представление в виде *карты* – интерактивных

локаций для моделирования динамического позиционирования и взаимодействия общественных систем. Ввиду того, что общественные системы проявляют себя опосредованно – через влияние на параметры среды – их выделение становится возможным через мониторинг таких параметров.

Дадим базовое описание конверсии элементов ОС в программные объекты, необходимые для визуализации. Каждый такой элемент проходит классификацию и представляется в виде графического объекта, обладающего внутренними параметрами. Их вывод целесообразно разделить на две зоны: 1) карта, дающая общее представление об исследуемых системах и 2) интерфейс, в котором выводятся данные о параметрах конкретных объектов. При этом вычисления для большей наглядности могут сопровождаться разными визуальными эффектами, такими как *области видимости* для этапа фильтрации в цикле алгоритма взаимодействия с внешней средой. Рассмотрим основные параметры элементов ОС.

Начнем с уровня взаимодействия с внешней средой, характеризующегося векторными величинами: на микроуровне – *вектор* к нормативному состоянию, на мезоуровне их совокупность образует *процессную траекторию*, а при переходе на макроуровень такое движение приводит к *функциональной тенденции*. Уровень состава описывается скалярными величинами: *массой облака организаций, массой процессной позиции* и *массой функциональной позиции* как индикаторами вклада элементов ОС в нормативное состояние. Уровень структуры на микро-, мезо- и макроуровнях представляется также скалярными величинами: *масса организационной связи*, *масса институциональной коммуникации* и *масса института* как индикатор приоритета изменения внутренних параметров элементов ОС в ходе коммуникации с другими элементами.

Представленные в настоящем подразделе параметры элементов общественных систем являются базовыми и могут быть детализированы путем выведения параметров, производных от них. Объективным фактором является наличие большого количества пропусков в имеющихся у исследователя данных. Частично их можно заполнить, используя различные вычислительные методы, однако их достоверность требует достаточной доказательной базы.

***2.6. Итоги раздела***

Многими исследователями выдвигается критика возможностей прямого моделирования общественных явлений [78, 79] ввиду того, что центральным элементом в них является человеческая личность, которая не может быть обсчитана математически. Она подвержена рефлексии, зачастую демонстрирует иррациональное поведение, а также ориентацию не на конкретные цели, а на абстрактные ценности. Не отрицая подобное видение, автор предлагает иной подход, в котором объектом анализа являются общественные системы. Данные о людях и их поведении являются частью общего массива данных и рассматриваются в контексте взаимодействия в системах. Такой подход потенциально позволяет снизить количество системных ошибок в итоговых моделях, а также в определенной степени компенсировать вычислениями выпадение значимых массивов данных, в том числе ввиду эпизодичности присутствия современного человека в интернет-среде.

Методология цифрового социологического исследования содержит этапы:

1. Предварительное описание объекта анализа.
2. Сбор и агрегация массивов данных.
3. Выделение признаков элементов ОС.
4. Классификация их элементов.
5. Визуализация взаимодействия ОС на карте.
6. Создание модели объекта социологического исследования и ее детализированное описание.
7. Диффузия и интеграция извлеченных знаний в системы-стейкхолдеры.

Предложенная процедура моделирования позволяет существенно сократить временные и материальные издержки на проведение социологического исследования, а также получать принципиально новые результаты. Кроме того, при накоплении достаточного набора данных об определенной ОС можно переходить от ее простого мониторинга к прогнозированию характера ее внутреннего состояния и взаимодействия с внешней средой.

**3. Моделирование общественных систем на основе сообщений в социальных сетях**

Базовая проверка работоспособности методологии проводится на уровне взаимодействия с внешней средой, источник данных – социальная сеть микроблогов Twitter*[†]. Здесь необходимо сделать важное замечание: некоторые источники говорят о низкой ликвидности данных, генерируемых в социальных сетях [80, 81]. На этот фактор обращает внимание и большое количество исследователей, частично рассмотренных в подразд. 1.2 данной работы. Безусловно, формирующиеся методы коммуникации противоречивы: они имеют инфраструктурные ограничения, допускают наличие большого количества шумов в процессе генерации, распространения и использования данных. Однако даже первичная их аналитика демонстрирует системность и направленность деятельности множества акторов. Кроме того, перспектива роста охвата аудитории подобными платформами и углубление методов ее активности признаются специалистами [82].

Эмпирическим материалом для данного раздела стали 654 сообщения пользователей в социальной сети микроблогов Twitter, опубликованных в течение одной декады в сентябре 2018 г. с ключевым словом *«экстремизм»*. С одной стороны, социологический анализ такой тематики обладает очевидной актуальностью для общества [83, 84].

* По решению суда внесена в Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено.

[†] В настоящее время переименована в X.

С другой – рассмотрение данных пятилетней давности дополнительно снижает фактор остроты текущего момента при обсуждении финального результата исследования. В рамках данной работы сначала будет представлена демонстрация процедуры моделирования на примере одного сообщения, затем несколько сообщений будут объединены в единую карту. В последующий работах объем используемых эмпирических данных будет увеличен.

***Анализ единичного сообщения***

На данном этапе работы необходимо преобразовать слова-сообщения в определенные типы графических объектов и позиционировать их на одной из локаций карты. Необходимо учитывать – часть слов неизбежно не будет транслироваться самими авторами, поэтому недостающие объекты и их параметры необходимо вычислить, что не всегда возможно. Из собранных за обозначенный период сообщений выбрано обладающее наибольшей наглядностью для раздела (табл. 3). В тексте терминология автора полностью сохранена, однако в табл. 4 и на рис. 3–5 некоторые элементы ОС приведены в соответствие с официальными названиями. На его основе проведем первичную объективацию и выдвинем гипотезы о классах элементов ОС*.

Таблица 3

**Сообщение из социальной сети Twitter**

| |
|---|
| Sun Sep 09 19:29:52 +0000 2018<br>«Судя по сообщениям, вот такие ″вежливые человеки″ пытались сегодня провоцировать на ″экстремизм″ в Оренбурге. Рядом в темных очках оперативник ЦПЭ† в штатском. Странно, что нормальные менты ″в форме″ не привлекли их, ведь в масках митинговать запрещено. #9сентября #Оренбург https://t.co/SYZVlWdfHA Likes:7 Retweets: 0 |

Перейдем к детализации процесса обработки данных. На текущем этапе описывается только базовая логика методики перевода текстовых сущностей в графические объекты со значительным количеством экспертных (не машинных) обобщений. Ввиду того, что сообщение опубликовано представителем некоторой общественной системы, исходя из внутренней логики, его анализ необходимо разделить на два этапа:

А. *Системоцентричный*. Граница между элементами общественных систем интерпретируется ей по признаку принадлежности к *органам внутренних дел*, либо к группе *провоцируемых на экстремизм* и пролегает только на микроуровне. Входами и выходами являются попытки взаимного наложения санкций в заданных промежутке времени, локации и контексте. Также фиксируются организационные связи внутри первой группы.

Б. *Стратегический.* На данном этапе необходимо реконструировать общую картину произошедшего на всех уровнях (см. табл. 4). Здесь название общественной системы, по крайней мере на текущем этапе, является условным и может конструироваться на основе синтеза названий выделенных элементов [86].

На основе хештегов и даты публикации произведем привязку элементов общественной системы к контексту происходящего. Согласно хештегу #Оренбург и фразы «в Оренбурге» генерируется локация на карте с соответствующей идентификацией. Далее на основе хештега #9 сентября и даты публикации возникает возможность привязки к временной шкале и контексту событий: протестным акциям против повышения пенсионного возраста.

Таким образом, совокупность деятельности множества субъектов на мезоуровне можно классифицировать как *процесс социального обеспечения*, претерпевающий переход от базового состояния к нормативному [87]. Выделим наиболее очевидные элементы состава микроуровня: *Росгвардия, полиция, ЦПЭ*, а также *провоцируемые на экстремизм*. Последние, очевидно, были лишь частью облака вышедших на демонстрацию, другая его часть – *протестующие*.

Таким образом, можно выдвинуть гипотезу: границу первого облака можно определить исходя из занимаемой позиции *субъекта исполнительной власти*, второго – *субъекта законодательной власти*. Последний, будучи *непризнанным* в данной ОС и обладающий меньшей массой по сравнению с *признанным*, стремится, по крайней мере декларативно, к сохранению прежних параметров рассматриваемого процесса методом интеграции с элементом 2.2. Однако в результате это может привести только к передаче определенной массы между ними в пользу элемента 2.1, что и является фактическим нормативным состоянием. Признанный субъект законодательной власти стремится к сохранению своей массы, проводя дезинтеграцию с субъектом непризнанным путем увеличения массы институциональной коммуникации с субъектами исполнительной власти.

Вернемся на микроуровень и опишем нормативные состояния элементов ОС и методы их достижения. Росгвардия стремится к увеличению собственной массы за счет снижения силы вектора провоцируемых на экстремизм. Наиболее вероятно, но не точно, нормативное состояние ЦПЭ является идентичным, однако метод его достижения определить, исходя из сообщения, проблематично. То же касается как состояний, так и способов их достижения полицией. В свою очередь, второе облако с разной степенью интенсивности (силой вектора) пытается увеличить свою массу за счет Росгвардии. При этом автор сообщения, относящийся к провоцируемым на экстремизм, предложил метод достижения плана нормативного состояния: снизить массу связи полиции и Росгвардии, направив на последнюю вектор санкционного типа. Однако такой план был предложен пост-

* Как уже говорилось ранее, элементы ОС нуждаются в классификации, однако для ее релевантности необходимо провести отдельную исследовательскую работу. В работе настоящей представлены только гипотезы о классах с частичной опорой на инструментарий, ранее разработанный автором для смежного класса задач [85].

† Центр противодействия экстремизму.

фактум, не оказав влияния на деятельность в текущем этапе цикла взаимодействия ОС (см. подразд. 2.4) – такой опыт может быть ею учтен в следующих итерациях.

Переходя на макроуровень, выдвинем следующую гипотезу: социальное обеспечение можно определить как один из процессов, формирующих *функцию компенсации провалов рынка* [88]. В нем, что следует из данных более низкого уровня обобщения, участвуют *субъекты власти*. С другой стороны, *субъекты рынка*, как и *субъекты социума*, напрямую в тексте сообщения отсутствуют – их можно вычислить по принадлежности к данной функции. Причем признаки функциональной позиции *субъектов социума* можно дополнительно подтвердить по метаданным *#9сентября* и *#Оренбург*. Также обратим внимание: другие элементы более низкого уровня исходя только из этого сообщения определить невозможно.

При исполнении рассматриваемой функции субъекты рынка определили свою массу как недостаточную и, через субъектов власти модифицировали ее до таких параметров, отказавшись от части социальных обязательств. Перейдем к этапу визуализации взаимодействия ОС на локации «Оренбург» (см. рис. 3–5.)

Таблица 4

**Множество элементов общественных систем***

| Базовое и нормативное состояние ОС | Взаимодействия с внешней средой | Состава | Структуры |
|---|---|---|---|
| 2. Если $[m_2 < M] \rightarrow$ $\rightarrow [m_{2r} = m_2 + \Delta m]$ | Функция компенсации провалов рынка<br>1. Снижение массы 3<br>$v_1$: $[m_{3i} = m_3 - \Delta m_2, F_i]$.<br>2. Увеличение массы связи 1–2<br>$v_2$: $[w_{1-2r} = w_{1-2} + \Delta w_r, F_r]$.<br>3. Снижение массы<br>$v_3$: $[m_{3s} = m_3 - \Delta m_2, F_i]$ | [Россия] Субъекты<br>1. Власти.<br>2. Рынка.<br>3. Социума. | 1–2<br>1–3<br>2–3 |
| 1. Увеличение массы $[m_{1i} = m_1 + \Delta m_{2.1}]$.<br>2.1. Увеличение массы $[m_{2.1j} = m_{2.1} + \Delta m_{2.2}]$.<br>2.2 Сохранение массы $[m_{2.2i} = m_{2.2}]$ | Процесс социального обеспечения<br>1. Снижение силы траектории 2.1<br>$v_1$: $[v_{2.1}(w_{2.1-2.2}), F_j - \Delta F_i]$.<br>2.1. Увеличение массы коммуникации 2.1–2.2.<br>$v_{2.1}$: $[w_{2.1-2.2j} = w_{2.1-2.2} + \Delta w_j, F_j]$.<br>2.2. Увеличение массы коммуникации 1–2.2<br>$v_{2.2}$: $[w_{1-2.2i} = w_{1-2.2} + \Delta w_i, F_i]$ | [Оренбург] Субъекты<br>1. Исполнительной власти.<br>2. Законодательной власти.<br>2.1. Непризнанной.<br>2.2. Признанной | 1–2.1<br>1–2.2 |
| 1.1. Увеличение массы $[m_{1.1i} = m_{1.1} + \Delta m_2]$.<br>1.3. Увеличение массы $[m_{1.3i} = m_{1.3} + \Delta m_{2.1.2}]$.<br>2.1.2. Увеличение массы $[m_{2.1.2j} = m_{2.1.1} + \Delta m_{1.1}]$ | 1.1 Снижение силы вектора<br>$v_{1.1}$:$[v_2(m_{1.1j}), F_j - \Delta F_i]$.<br>2.1.2 Снижение массы связи (о)†<br>$v_{2.1.2}$: $[w_{1.1-1.2j} = w_{1.1-1.2j} - \Delta w_j, F_j]$.<br>Снижение массы (о)<br>$v_{1.2}$: $[m_{1.1j} = m_{1.1} - \Delta m_{1.2}, F_j]$ | 1.1. Росгвардия.<br>1.2. Полиция.<br>1.3. ЦПЭ.<br>2.1.1. Протестующие.<br>2.1.2. Провоцируемые на экстремизм | 1.1–1.2<br>1.1–1.3<br>1.2–1.3<br>2.1.1–2.1.2 |

* m – масса, w – масса связи, v – вектор.

Примеры синтаксиса записи:

• массы: $[m_{1i} = m_1 + \Delta m_{2.1}]$ – массе элемента 1 присвоить значение суммы его базовой (текущей) массы и приращения, пришедшего от иного элемента. Для краткости базовое состояние записывается как значение внутри нормативного;

• вектора: $v_{2.2}$: $[w_{1-2.1i} = w_{1-2.1} - \Delta w_i, F_i]$ – вектор от элемента 2.2 направлен на изменение массы связи 1–2.1 с силой $F_i$;

• контрвектора: $v_1$: $[v_{2.1}(m_{2.2}), F_j - \Delta F_i]$ – вектор от элемента 1 направлен на вектор 2.1, воздействующий на массу элемента 2.2 с силой $F_j - \Delta F_i$;

† (о) – данные для *обучения* системы. Они могут использоваться на следующих итерациях цикла взаимодействия.


Рис. 3. Микроуровень локации «Оренбург»


Рис. 4. Мезоуровень локации «Оренбург»


Рис. 5. Макроуровень локации «Оренбург»

**Итоги.** Анализ единичного сообщения позволил выделить и представить в удобной форме достаточно сложную динамику взаимодействия общественной системы:

1. Выделить отсутствующие в ее зонах фильтрации и интерпретации (общественном восприятии) позиций акторов взаимодействия, под другим углом взглянуть на их нормативные состояния.

2. Выдвинуть гипотезу об определяющей роли субъектов рынка, но не субъектов власти, в направлении которых на мезоуровне были попытки стремления к интеграции, а на микроуровне – наложения санкций оппозиционными им элементами. Такого рода «неверная» интерпретация привела к конфликту *властей* и увела ОС от достижения декларируемых нормативных состояний.

**Заключение**

Наблюдаемое в настоящее время изменение состава, структуры и методов взаимодействия в обществе привело к устойчивому росту объемов генерации, распространения и использования данных. Существующая тенденция привела к снижению эффективности его социологического мониторинга и прогнозирования с помощью подходов, ориентированных на типы взаимодействия уходящей формации. Кризис избытка данных возможно преодолеть только на основе комплексной методологии цифрового социологического исследования, сочетающей инструментарий как традиционной социологической науки, так и науки о данных.

Методология, предложенная автором настоящей работы, позволяет, даже на основе анализа одного короткого сообщения, хоть не любого, получить целый спектр аналитических данных о некоторой общественной системе. При расширении массива обрабатываемых сообщений можно наблюдать – люди и организации, декларирующие на первый взгляд разрозненные, даже эклектичные взгляды, могут стремиться к схожим нормативным состояниям независимо от таковых. Выявление подобных неочевидных зависимостей с применением существующих инструментов анализа является достаточно затруднительным. Регулярный анализ большего количества сообщений и иных данных расширяет возможности взаимодействия стейкхолдеров со средой исходя из их нормативного состояния.

Совокупность описанных факторов позволяет говорить о применимости разработанного подхода и необходимости продолжить настоящее исследование. На текущем этапе разработки методология является специализированным инструментом: она сшивает микро-, мезо- и макроаналитические уровни, однако применять ее необходимо с учетом имеющихся ограничений. Она будет более эффективна при необходимости увидеть целостную картину объекта, т.е. исследования должны ориентироваться преимущественно на макро- и мезоуровни, а микроуровень будет являться вспомогательным. Будущая программная реализация позволит расширить потенциал анализа микроуровня, открывая возможность исследователю оперативного перемещения между выводимыми визуализациями каждого уровня. Автор не претендует на бесспорность предложенного подхода, однако он уже сейчас может быть использован как рабочий инструмент социологического мониторинга и прогнозирования.

*Литература*

1. Батов Г.Х. Технологический аспект в концепции опережающего развития / Г.Х. Батов, З.Х. Кумышева, А.Б. Тлисов // МИР (Модернизация. Инновации. Развитие). – 2019. – Т. 10, № 2. – С. 275–287.

2. Дорожная карта по развитию сквозной цифровой технологии «Новые производственные технологии». Результаты и перспективы / А.И. Боровков, О.И. Рождественский, К.В. Кукушкин и др. // Инновации. – 2019. – № 11(253). – С. 89–104. DOI: 10.26310/2071-3010.2019.253.11.011

3. Ковалевич Д.А. Конвейер инноваций / Д.А. Ковалевич, П.Г. Щедровицкий. – М.: Агенство стратегических инициатив (АСИ), 2016. – 15 с.

4. Щедровицкий П.Г. Три индустриализации России. – М.: Terra Fantastica, 2018. – 150 с.

5. Гребенюк А.А. Исследование социальной напряженности на основе больших данных электронных социальных сетей / А.А. Гребенюк, А.С. Максимова, Л.Г. Лэмер // Цифровая социология. – 2021. – Т.4, № 4. – С. 4–12. DOI: 10.26425/2658-347X-2021-4-4-4-12

6. Сайт Европейского центра социологических исследований. – URL: srcenter.ru/stoimost/ (дата обращения: 19.06.2023).

7. Сайт компании Riversampling. Онлайн-опросы. – URL: riversampling.ru/?yclid=2793149652358174840 (дата обращения: 19.06.2023).

8. Долженко Р.А. People data («данные о людях») как новое направление работы с человеческими ресурсами // Вестник Омского ун-та. Сер.: Экономика. – 2019. – Т. 17, № 2. – С. 63–72.

9. Dai G. Social evaluation of innovative drugs: A method based on big data analytics / G. Dai, X. Fu, W. Dai, S. Lu // Computer Science and Information Systems. – 2017. – Vol. 14, Iss. 3. – P. 805–821.

10. Программируем будущее. Система Крибрум. – URL: youtube.com/watch?v=mzbnyYOBe2w&t=743s (дата обращения: 19.06.2023).

11. Боровков А.И. Цифровые двойники и цифровая трансформация предприятий ОПК / А.И. Боровков, Ю.А. Рябов, К.В. Кукушкин // Вестник Восточно-Сибирской открытой академии. – 2019. – № 32. – С. 1–39.

12. Черныш А.В. Возникновение организационных моделей: взгляд новых институционалистов // Социологические исследования. – 2017. – № 4. – С. 140–146.

13. Higgins A. Pedagogical principles and methods underpinning education of health and social care practitioners on experiences and needs of older LGBT+ people: Findings from a systematic review / A. Higgins, C. Downes, G. Sheaf // Nurse Education in Practice. – 2019. – Vol. 40, No. 102625. DOI:

10.1016/j.nepr.2019.102625. – URL: researchgate.net/publication/335784603_Pedagogical_principles_and_methods_underpinning_education_of_health_and_social_care_practitioners_on_experiences_and_needs_of_older_LGBT_people_Findings_from_a_systematic_review (дата обращения: 02.02.2024).

14. Kelly M.P. What can sociology offer urban public health? / M.P. Kelly, J. Green // Critical Public Health. – 2019. – Vol. 29, Iss. 5. – P. 517–521. DOI: 10.1080/09581596.2019.1654193

15. Яковенко А.В. О воздействии естественных и социогуманитарных наук на общественные процессы // Социологические исследования. – 2016. – № 2. – С. 12–19.

16. Button D.M. Contextualizing LGB youth's experiences with victimization and risky behaviors: a qualitative approach to general strain theory // Feminist Criminology. – 2019. – Vol. 14, Iss. 4. – P. 441–465. DOI: 10.1177/1557085118789792

17. Houseworth C.A. Intermarriage and the U.S. Military / C.A. Houseworth, K. Grayson // Armed Forces and Society. – 2019. – Vol. 45, Iss. 4. – P. 659–680. DOI: 10.1177/0095327X18769456

18. Ярская-Смирнова Е.Р. Маломобильные в российских печатных СМИ: анализ репрезентаций уязвимых групп до и во время пандемии / Е.Р. Ярская-Смирнова, О.А. Косова, В.Н. Ярская-Смирнова // Вестник Том. гос. ун-та. Философия. Социология. Политология. – 2023. – № 71. – С. 215–224. DOI: 10.17223/1998863X/71/20

19. Эфендиев А.Г. Мотивационная основа трудовой деятельности: опыт реализации многомерного подхода / А.Г. Эфендиев, Е.В. Абрамова // Журнал социологии и социальной антропологии. – 2023. – Т. 26, № 1. – С. 26–57. – DOI: 10.31119/jssa.2022.26.1.2

20. Chevalier T. Political trust, young people and institutions in Europe. A multilevel analysis // International Journal of Social Welfare. – 2019. – Vol. 28, Iss. 4. – P. 418–430. DOI: 10.1111/ijsw.12380

21. Трофимова И.Н. Представления россиян о будущем страны: существует ли консенсус? // Социологические исследования. – 2022. – № 10. – С. 37–48. DOI: 10.31857/S013216250020843-0

22. Santoprete M. Countering violent extremism: A mathematical model // Applied Mathematics and Computation. – 2019. – Vol. 358. – P. 314–329. DOI: 10.1016/j.amc.2019.04.054

23. Кирдина С.Г. Социальное прогнозирование как междисциплинарный проект / С.Г. Кирдина, Г.Б. Клейнер // Социологические исследования. – 2016. – № 12. – С. 44–51.

24. Щербина В.В. Целеформирующие и целеобеспечивающие рационализирующие социальные технологии // Социологические исследования. – 2016. – № 4. – С. 50–58.

25. Нагайцев В.В. Социальный протест в Алтайском крае: опыт исследования в методологии социального конфликта / В.В. Нагайцев, А.Н. Шрайбер, В.А. Артюхина // Siberian Socium. – 2020. – Т. 4, № 4(14). – С. 41–53. DOI: 10.21684/2587-8484-2020-4-4-41-53

26. Костко Н.А. Зелёные практики против городских практик: контент-анализ региональной прессы Тюменской области / Н.А. Костко, И.Н. Пупышева, Т.И. Паюсова // Siberian Socium. – 2023. – Т. 7, № 1(23). – С. 8–28. DOI: 10.21684/2587-8484-2023-7-1-8-28

27. Быльева Д.С. Технологии правды в сети / Д.С. Быльева // Искусственные общества. – 2023. – Т. 18, № 1. DOI: 10.18254/S207751800024139-1. – URL: artsoc.jes.su/s207751800024139-1-1/ (дата обращения: 02.02.2024).

28. Едаменко Е.П. Маркеры аудитории «облачных» сообществ на примере коммуникации пользователей в каналах «Телеграм» / Е.П. Едаменко, Е.В. Головацкий // Siberian Socium. – 2023. – Т. 7, № 1(23). – С. 45–56. DOI: 10.21684/2587-8484-2023-7-1-45-56

29. Пастухова Е.Я. Избыточная смертность в сибирских регионах в условиях пандемии COVID-19: динамика и факторы влияния / Е.Я. Пастухова, Е.А. Морозова // Регионология. – 2022. – Т. 30, № 3(120). – С. 602–623. DOI: 10.15507/2413-1407.120.030.202203.602-623

30. Luyts M. Weibull-count approach for handling under- and overdispersed longitudinal/clustered data structures / M. Luyts, G. Molenberghs, G. Verbeke // Statistical Modelling. – 2019. – Vol. 19, Iss. 5. – P. 569–589. DOI: 10.1177/1471082X18789992

31. Юревич А.В. Методология количественной оценки психологического состояния современного российского общества // Методология и история психологии. – 2018. – № 1. – С. 155–173.

32. Кинчарова А.В. Исследовательские практики российских социологов / А.В. Кинчарова, М.М. Соколов // Социологические исследования. – 2015. – № 6. – С. 58–68.

33. Molesworth M. Sociology in UK nurse education curricula: A review of the literature from 1919 to 2019 / M. Molesworth, M. Lewitt // Social Theory and Health. – 2019. – Vol. 17, Iss. 4. – P. 427–442. DOI: 10.1057/s41285-019-00104-1

34. Chun C.W. Language, discourse, and class: What's next for sociolinguistics? // Journal of Sociolinguistics. – 2019. – Vol. 23, Iss. 4. – P. 332–345. DOI: 10.1111/josl.12359

35. Земнухова Л.В. Социотехническое в цифровой социологии: методологические возможности и ограничения // Социология власти. – 2018. – Т. 30, № 3. – С. 54–68. DOI: 10.22394/2074-0492-2018-3-54-68

36. Орлов А.И. Математические методы в социологии за сорок пять лет // Политематический сетевой электронный научный журнал Кубанского гос. аграр. ун-та. – 2016. – № 117. – С. 91–119.

37. Lindstedt N.C. Structural Topic Modeling for Social Scientists: a Brief Case Study with Social Movement Studies Literature, 2005–2017 // Social Currents. – 2019. – Vol. 6, Iss. 4. – P. 307–318. DOI: 10.1177 / 2329496519846505

38. Titarenko L. Diversification and fragmentation of Russian sociology / L. Titarenko, E. Zdravomyslova // Sociology in Russia: a brief history. Sociology Transformed. SpringerLink. – 2017. – P. 103–123. DOI: 10.1007/978-3-319-58085-2_6

39. Доклад о цифровой экономике 2019. Создание стоимости и получение выгод: последствия для развивающихся стран: обзор // Матер. конф. Организации Объединенных Наций по торговле и развитию. – Женева, 2019. – 31 с. – URL: unctad.org/system/files/official-document/der2019_overview_ru.pdf (дата обращения: 22.06.2023).

40. Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы "Цифровая экономика Российской Федерации"». – URL: static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 22.06.2023).

41. Arabnezhad E. A Light in the Dark Web: Linking Dark Web Aliases to Real Internet Identities / E. Arabnezhad, M.La Morgia, A. Mei, E.N. Nemmi, J. Stefa // 2020 IEEE 40th International Conference on Distributed Computing Systems, Singapore. – 2020. – PP. 311–321. DOI: 10.1109/ICDCS47774.2020.00081

42. Simek O. Prototype and Analytics for Discovery and Exploitation of Threat Networks on Social Media / O. Simek, D. Shah, A. Heier // 2019 European Intelligence and Security Informatics Conference (EISIC), Oulu, Finland. – 2019. – PP. 9–16. DOI: 10.1109/EISIC49498.2019.9108895

43. An Online Scan of Extreme-Right Radicalization in Social Networks (The Case of the Russian Social Network VKontakte) / A.Yu. Karpova, S.A. Kuznetsov, A.O. Savelev, A.D. Vilnin // Journal of Siberian Federal University. Humani-

ties and Social Sciences. – 2022. – Vol. 15, No. 12. – P. 1738–1750. DOI: 10.17516/1997-1370-0948

44. Dragos V. Beyond Sentiments and Opinions: Exploring Social Media with Appraisal Categories / V. Dragos, D. Battistelli, E. Kelodjoue // 2018 21st International Conference on Information Fusion (FUSION), Cambridge, UK, 2018. – PP. 1851–1858. DOI: 10.23919/ICIF.2018.8455751

45. Liu X. The Analysis on the Role of Social Network in the Field of Anti-Terrorism Take the «East Turkistan» Organization as an Example / X. Liu, T. Sun, F. Bu, H. Qin // 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Harbin, China, 2020, pp. 2282–2285. DOI: 10.1109/ICMCCE51767.2020.00493.

46. Социальные сети и деструктивный контент (Теория сетевых войн) / А.Г. Остапенко, А.В. Паринов, А.О. Калашников и др. – М.: Горячая линия – Телеком, 2018. – 276 с.

47. Возможности использования цифровых следов для прогнозирования образовательных достижений студентов / В.В. Кашпур, Е.Ю. Петров, В.Л. Гойко, А.В. Фещенко // Вестник Том. гос. ун-та. Философия. Социология. Политология. – 2021. – № 64. – С. 140–150. DOI: 10.17223/1998863X/64/13.

48. Seshadri A. Graph Model of Environmental Backcloth / A. Seshadri, A.J. Park, S.Z. Stamato, V. Spicer, V.T. Nguyen, J. Song // 2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2022, pp. 0445–0451. DOI: 10.1109/IEMCON56893.2022.9946572.

49. Дудина В.И. От паноптикона к панспектрону: цифровые данные и трансформация режимов // Социологические исследования. – 2018. – № 11(415). – С. 17–26. DOI: 10.31857/S013216250002782-3

50. Крупеникова Л.Ш. Big data и новые задачи социологии // Гуманитарий Юга России. – 2022. – Т. 11, № 2. – С. 50–57. DOI: 10.18522/2227-8656.2022.2.3

51. Ницевич В.Ф. Цифровая социология: теоретико-методологические истоки и основания // Цифровая социология. – 2018. – № 1. – С. 18–28.

52. Агиева М.Т. Задачи анализа и прогноза при управлении целевой аудиторией в маркетинге / М.Т. Агиева, Ю.В. Бабичева, Н.М. Окулист, Г.А. Угольницкий // Управление большими системами: сборник трудов. – 2019. – Т. 79. – С. 27–64.

53. Азаров А.А. Профилизация пользователей цифровых сетей социального недовольства в субъектах Российской Федерации / А.А. Азаров, В.А. Лукушин, М.А. Давыдова // Гуманитарные науки. Вестник финансового ун-та. – 2022. – Т. 12, № 5. – С. 105–113. DOI: 10.26794/2226-7867-2022-12-5-105-113

54. Шумов В.В. Иерархия моделей боевых действий и пограничных конфликтов // Управление большими системами: сборник трудов. – 2019. – Т. 79. – С. 86–11.

55. Azaouzi M. Community detection in large‐scale social networks: state‐of‐the‐art and future directions / M. Azaouzi, D. Rhouma, L.B. Romdhane // Social Network Analysis and Mining. – 2019. – Vol. 9, Iss. 1, No. 23. DOI: 10.1007/s13278-019-0566-x. – URL: link.springer.com/article/10.1007/s13278-019-0566-x (дата обращения: 02.02.2024).

56. Крыштановская О.В. Бесконтактная социология: новые формы исследований в цифровую эпоху // Цифровая социология. – 2018. – № 1. – С. 4–8.

57. Милехин А.В. Социологический мониторинг – средство информационного обеспечения управления в общественных системах: дис. … д-ра соц. наук: 22.00.08. – М., 1999. – 327 с.

58. Горячев И.Н. К проблеме динамического равновесия общественных систем // XXI век: итоги прошлого и проблемы настоящего плюс. – 2013. – № 11, Т. 2. – С. 216–222.

59. Норт Д. Институты, институциональные изменения и функционирование экономики. – М.: Фонд экономической книги «Начала», 1997. – 180 с.

60. Бурков В.Н. Теория активных систем: состояние и перспективы / В.Н. Бурков, Д.А. Новиков. – М.: Синтег, 1999. – 128 с.

61. Тарасенко Ф.П. Прикладной системный анализ: учеб. пособие. – М.: КРОНУС, 2017. – 220 с.

62. Указ Президента Российской Федерации № 646 от 05.12.2016. Об утверждении Доктрины информационной безопасности. – URL: kremlin.ru/acts/bank/41460/page/1 (дата обращения: 24.06.2023).

63. Судакова А.Е. Миграция ученых: цифровой след и наукометрия // Перспективы науки и образования. – 2020. – № 3. – С. 544–557. DOI: 10.32744/pse.2020.3.39

64. Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. – 2019. – № 1. – С. 15–25. DOI: 10.24411/2414-3995-2019-10002.

65. Акофф Р. О целеустремленных системах / Р. Акофф, Ф. Эмери. – М.: Книга по требованию, 2012. – 270 с.

66. Монастырный Е.А. Инвестиционные модели развития. Приток и отток иностранных инвестиций в России / Е.А. Монастырный, В.М. Саклаков // Инновации. – 2015. – № 10. – С. 27–34.

67. Монастырный Е.А. Методологический подход к оценке эффективности инновационного развития региона / Е.А. Монастырный, В.В. Спицын, Я.Н. Грик // Инновации. – 2010. – № 1. – С. 80–86.

68. Куулар Ш.В. Психофизиологические особенности студентов с разным типом стратегии поведения в конфликтных ситуациях / Ш.В. Куулар, Л.К.-С. Будукоол // Вестник Новосиб. гос. педагогического ун-та. – 2017. – Т. 7, № 5. – С. 67–80.

69. Кирдина-Чэндлер С.Г. Кооперация versus конкуренция в трудах российских эволюционистов / С.Г. Кирдина-Чэндлер, Д. Холл // Journal of institutional studies. – 2017. – Т. 9, № 1. – С. 6–26.

70. Taibi D. How do search engines shape reality? Preliminary insights from a learning experience / D. Taibi, G. Fulantelli, L. Basteris // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). – 2020. – Vol. 11984 LNCS. – P. 370–377. DOI: 10.1007/978-3-030-38778-5_40

71. Tien J.H. Online reactions to the 2017 'Unite the right' rally in Charlottesville: measuring polarization in Twitter networks using media followership / J.H. Tien, M.C. Eisenberg, S.T. Cherng, M.A. Porter // Applied Network Science. – 2020. – Vol. 5, Iss. 1. – P. 1–27. DOI: 10.1007/s41109-019-0223-3

72. Gaaze K. Max Weber's theory of causality: An examination on the resistance to post-truth // Sotsiologicheskoe Obozrenie. – 2019. – Vol. 18, Iss. 2. – P. 41–61. DOI: 10.17323/1728-192x-2019-2-41-61

73. Peters M.A. A viral theory of post-truth / M.A. Peters, P. McLaren, P. Jandric // Educational Philosophy and Theory. – 2020. DOI: 10.1080/00131857.2020.1750090

74. Хургин В.М. Об определении понятия «информация» // Информационные ресурсы России. – 2007. – № 3. – С. 6–13.

75. Щедровицкий П.Г. От разделения труда к разделению деятельности / П.Г. Щедровицкий, Ю.В. Кузнецов // Философские науки. – 2014. – № 6. – С. 49–64.

76. ГОСТ 15971–90 от 01.01.1992. Системы обработки информации. Термины и определения. – URL: docs.cntd.ru/document/1200015664 (дата обращения: 22.06.2023).

77. ISO/IEC/IEEE 24765:2017. Systems and software engineering – Vocabulary. – URL: iso.org/obp/ui/#iso:std:iso-iec-ieee:24765:ed-2:v1:en (дата обращения: 22.06.2023).

78. Персианов В.А. Проблемные вопросы использования инструментария экономической кибернетики / В.А. Персианов, А.В. Курбатова // Управление. – 2019. – Т. 7, № 3. – С. 94–102.

79. Социология управления: фундаментальное и прикладное знание / А.В. Тихонов, А.А. Мерзляков, Е.И. Рабинович, В.А. Корнилович, А.В. Жаворонков, А.Л. Королёв, В.А. Шилова, И.М. Атаян, В.В. Пащенко, В.С. Богданов, Г.В. Градосельская, Д.В. Просянюк, А.Н. Расходчиков, Т.М. Дридзе, К.В. Быков. – М.: Канон+, 2014. – 560 с.

80. Тагиров З.И. Цифровая оперативная обстановка, цифровое имя человека и сетевая (цифровая) правоохранительная деятельность в отечественной модели цифровой экономики // Вопросы безопасности. – 2018. – № 4. – С. 28–51.

81. Юдалевич Н.В. Информационный мусор как феномен современного общества // Бизнес-образование в экономике знаний. – 2016. – № 2. – С. 119–122.

82. Hashemi A. Telegram group quality measurement by user behavior analysis / A. Hashemi, M.A. Zare Chahooki // Social Network Analysis and Mining. – 2019. – Vol. 9. Iss. 33. – P. 1–12. DOI: 10.1007/s13278-019-0575-9

83. Hosni A.I.E. Analysis of the impact of online social networks addiction on the propagation of rumors / A.I.E. Hosni, K. Li, S. Ahmad // Physica A: Statistical Mechanics and its Applications. – 2020. – Vol. 542. – P. 1–11. DOI: 10.1016/j.physa.2019.123456

84. Гаврилин Ю.В. Использование информации, полученной из сети интернет, в расследовании преступлений экстремистской направленности / Ю.В. Гаврилин, А.В. Шмонин // Труды Академии управления МВД России. – 2019. – № 1. – С. 105–111.

85. Монастырный Е.А. Классификация институтов развития / Е.А. Монастырный, В.М. Саклаков // Инновации. – 2013. – № 9. – С. 59–65.

86. Ерёмченко Е.Н. Визуализация и новое определение знака // GraphiCon – 2018: Труды 28-й Междунар. конф. по компьютерной графике и машинному зрению. – Томск, 2018. – С. 301–303.

87. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам назначения и выплаты пенсий» № 350-ФЗ от 03.10.2018.

88. Бабкин А.В. К вопросу об оценке эффективности программ развития промышленности / А.В. Бабкин, А.О. Новиков // Теория и практика сервиса: экономика, социальная сфера, технологии. – 2016. – № 4. – С. 5–13.

---

**Саклаков Василий Михайлович**
Ст. преп. отделения информационных технологий
Инженерной школы информационных технологий
и робототехники Национального исследовательского
Томского политехнического университета
Советская ул., 84/3, г. Томск, Россия, 634034
ORCID: 0000-0003-1716-4581
Тел.: +7-953-914-08-17
Эл. почта: saklavas@tpu.ru

Saklakov V.M.

**Methodology of digital sociological research: social system as a basic modeling tool**

The article analyzes the existing approaches to sociological research and provides assessment of some systemic gaps in the cycle of modeling sociological objects. The technique allowing modeling of complex social interactions based on the concept of «social system» is proposed. The modeling principles are developed, covering the levels of interaction with the environment, content and structure. The model of the social system, having a set of internal parameters, and the algorithm of its interaction with the environment are presented. To facilitate the perception of a large number of elements extracted from the collected empirical data, it is proposed to display the final result of the study on a special map. The primary testing, based on messages from the social network Twitter, allowed us to identify the elements of complex social systems and show the nature of their interaction. It is concluded that the methodology is applicable as a tool to monitor and to forecast complex social interactions.

**Keywords:** social system, interaction of complex societal actors, digital sociology, general systems theory, data analysis, extremism, social networks.
**DOI**: 10.21293/1818-0442-2023-26-4-61-77

*References*

1. Batov G.Kh., Kumysheva Z.Kh., Tlisov A.B. [Technological Aspect in the Concept of Advansed Development]. *MIR (Modernization. Innovation. Research),* 2019, vol. 10, no. 2, pp. 275–287 (in Russ.).

2. Borovkov A.I., Rozhdestvenskij O.I., Kukushkin K.V. et al. [Roadmap for the development of cross-cutting digital technology «New Manufacturing Technologies»: findings and prospects]. *Innovation*, 2019, no 11, pp. 89–104 (in Russ.).

3. Kovalevich, D.A., Shchedrovitskii, P.G. *Konveier innovatsii* [Conveyor of innovation]. Moscow, Agency for Strategic Initiatives, 2016, 15 p. (in Russ.).

4. Shchedrovitskii, P.G. *Tri industrializatsii Rossii* [Three industrializations of Russia]. Moscow, Terra Fantastica, 2018, 150 p. (in Russ.).

5. Grebenyuk A.A. [Study of social tension based on electronic social networks big data]. *Digital Sociology*, 2021, vol. 4, no 4, pp. 4–12 (in Russ.).

6. Website of the European Center for Sociological Research. (in Russ.). Available at: srcenter.ru/stoimost/ (Accessed: June 19, 2023).

7. Riversampling's Website. Online surveys. (in Russ.). Available at: riversampling.ru/?yclid=2793149652358174840 (Accessed: June 19, 2023).

8. Dolzhenko, R.A. [People data as a new trend in human resource management] // *Herald of Omsk University. Series: Economics*, 2019, vol. 17, no 2, pp. 63–72 (in Russ.).

9. Dai G., Fu X., Dai W., Lu S. Social evaluation of innovative drugs: A method based on big data analytics // Computer *Science and Information Systems*, 2017, vol. 14, iss. 3, pp. 805–821.

10. *Programmiruem budushchee. Sistema Kribrum.* [Programming the future. Cribrum system] (in Russ.). Available at: youtube.com/watch?v=mzbnyYOBe2w&t=743s (Accessed: June 19, 2023).

11. Borovkov, A.I., Ryabov, Y.A., Kukushkin, K.V. *Tsifrovye dvoiniki i tsifrovaya transformatsiya predpriyatii OPK* [Digital twins and the digital transformation of defense industry companies] // *Bulletin of the East Siberian Open Academy*, 2019, no. 32, pp. 1–39 (in Russ.).

12. Chernysh A.V. [The emergence of organizational models: new institutionalism perspective]. *Sociological Research*, 2017, no. 4. pp. 140–146 (in Russ.).

13. Higgins A., Downes C., Sheaf G. Pedagogical principles and methods underpinning education of health and social care practitioners on experiences and needs of older LGBT+ people: Findings from a systematic review. *Nurse Education in Practice*, 2019, vol. 40, no. 102625. DOI: 10.1016/j.nepr.2019.102625. Available at: researchgate.net/publication/335784603_Pedagogical_principles_and_methods_underpinning_education_of_health_and_social_care_practitioners_on_experiences_and_needs_of_older_LGBT_people_Findings_from_a_systematic_review (Accessed: February 2, 2024).

14. Kelly M. P., Green J. What can sociology offer urban public health? *Critical Public Health,* 2019, vol. 29, is. 5, pp. 517–521. DOI: 10.1080/09581596.2019.1654193

15. Yakovenko A.V. *O vozdeistvii estestvennykh i sotsiogumanitarnykh nauk na obshchestvennye protsessy* [On the impact of natural and socio-humanitarian sciences on social processes] *Sociological Research,* 2016, no. 2, pp. 12–19.

16. Button D.M. Contextualizing LGB youth's experiences with victimization and risky behaviors: a qualitative approach to general strain theory. *Feminist Criminology*, 2019, vol. 14, iss. 4, pp. 441–465. DOI: 10.1177/1557085118789792

17. Houseworth C.A., Grayson K. Intermarriage and the U.S. Military. *Armed Forces and Society,* 2019, vol. 45, iss. 4, pp. 659–680. DOI: 10.1177/0095327X18769456

18. Yarskaya-Smirnova E.R., Kosova O.A., Yarskaya-Smirnova V.N. [Low-mobility groups in Russian press: analysis of representations of vulnerable groups before and during the pandemic]. *Bulletin of Tomsk State University. Philosophy. Sociology. Political Science,* 2023, no 71, pp. 215–224 (in Russ.).

19. Ehfendiev A.G., Abramova E. V. [The motivational basis of labor activity: a multidimensional approach]. *Journal of Sociology and Social Anthropology*, 2023, vol. 26, no 1, pp. 26–57 (in Russ.).

20. Chevalier T. Political trust, young people and institutions in Europe. A multilevel analysis. *International Journal of Social Welfare,* 2019, vol. 28, is. 4, pp. 418–430. DOI: 10.1111/ijsw.12380

21. Trofimova, I.N. [Russians' ideas about the future of the country: is there a consensus?]. *Sociological Research*, 2022, no. 10, pp. 37–48 (in Russ.).

22. Santoprete M. Countering violent extremism: A mathematical model. *Applied Mathematics and Computation*, 2019, vol. 358, pp. 314–329. DOI: 10.1016/j.amc.2019.04.054

23. Kirdina, S.G., Kleiner, G.B. *Sotsial'noe prognozirovanie kak mezhdistsiplinarnyi proekt*. [Social forecasting as an interdisciplinary project]. *Sociological Research,* 2016, no. 12, pp. 44–51 (in Russ.).

24. Shcherbina, V.V. *Tseleformiruyushchie i tseleobespechivayushchie ratsionaliziruyushchie sotsial'nye tekhnologii.* [Purpose-forming and purpose-supporting rationalizing social technologies]. *Sociological Research,* 2016, no. 4, pp. 50–58 (in Russ.).

25. Nagajtsev, V.V. Shrajber A.N., Artyukhina V. A. [Social protest in the Altai Territory: research experience in the methodology of social conflict] // *Siberian Socium*, 2020, vol. 4, no. 4(14), pp. 41–53 (in Russ.).

26. Kostko, N.A., Pupysheva I.N., Payusova T.I. [Green practices versus urban practices: content analysis of the regional press of the Tyumen region]. *Siberian Socium,* 2023, vol. 7, no. 1 (23), pp. 8–28 (in Russ.).

27. Bylieva D.S. [Technologies of truth on the web] *Artificial Societies,* 2023, vol. 18, no. 1 (in Russ.). Available at: artsoc.jes.su/s207751800024139-1-1/ (Accessed: February 2, 2024).

28. Edamenko, E.P., Golovatsky E.V. [Audience markers of «cloud» communities exemplified by user communication in «Telegram» channels]. *Siberian Socium,* 2023, vol. 7, no. 1 (23), pp. 45–56 (in Russ.).

29. Pastukhova, E.Ya., Morozova E.A. [Excess Mortality in the Siberian Regions in the Context of the COVID-19 Pandemic: Dynamics and Affecting Factors]. *Russian Journal of Regional Studies*, 2022, vol. 30, no. 3 (120), pp. 602–623 (in Russ.).

30. Luyts M., Molenberghs G., Verbeke G. Weibull-count approach for handling under- and overdispersed longitudinal/clustered data structures. *Statistical Modelling*, 2019, vol. 19, is. 5, pp. 569–589. DOI: 10.1177/1471082X18789992

31. Yurevich A.V. *Metodologiya kolichestvennoi otsenki psikhologicheskogo sostoyaniya sovremennogo rossiiskogo obshchestva*. [Methodology of quantitative assessment of the psychological state of modern Russian society]. *Methodology and History of Psychology*, 2018, no. 1, pp. 155–173 (in Russ.).

32. Kincharova A.V., Sokolov M.M. *Issledovatel'skie praktiki rossiiskikh sotsiologov*. [Research practices of Russian sociologists]. *Sociological research,* 2015, no. 6, pp. 58–68 (in Russ.).

33. Molesworth M., Lewitt M. Sociology in UK nurse education curricula: A review of the literature from 1919 to 2019. *Social Theory and Health,* 2019, vol.17, iss.4, p.427–442. DOI: 10.1057/s41285-019-00104-1

34. Chun C.W. Language, discourse, and class: What's next for sociolinguistics? *Journal of Sociolinguistics*, 2019, vol. 23, is. 4, pp. 332–345. DOI: 10.1111/josl.12359

35. Zemnukhova, L.V. *Sotsiotekhnicheskoe v tsifrovoi sotsiologii: metodologicheskie vozmozhnosti i ogranicheniya* [Sociotechnical in Digital Sociology: methodological possibilities and limitations]. *Sociology of Power*, 2018, vol. 30, no. 3 (in Russ.).

36. Orlov A.I. [Mathematical methods in sociology during the last forty-five years]. *Scientific Journal of KubSAU*. 2016, no. 117, pp. 91–119 (in Russ.).

37. Lindstedt N. C. Structural Topic Modeling For Social Scientists: A Brief Case Study with Social Movement Studies Literature, 2005–2017. *Social Currents,* 2019, vol. 6, iss. 4, pp. 307–318. DOI: 10.1177 / 2329496519846505

38. Titarenko L., Zdravomyslova E. Diversification and fragmentation of Russian sociology. *Sociology in Russia: a Brief History. Sociology Transformed. SpringerLink,* 2017, pp. 103–123. DOI: 10.1007/978-3-319-58085-2_6

39. *Doklad o tsifrovoi ehkonomike 2019. Sozdanie stoimosti i poluchenie vygod: posledstviya dlya razvivayushchikhsya stran. Obzor.* [Report on the Digital Economy 2019. Value creation and benefit generation: implications for developing countries. Review]. *Materialy konferentsii Organizatsii ob'edinennykh natsii po torgovle i razvitiyu*. [Proceedings of the United Nations Conference on Trade and Development]. Geneva, 2019, 31 p. Available at: unctad.org/system/files/ official-document/der2019_overview_ru.pdf (Accessed: June 22, 2023) (in Russ.).

40. *Rasporyazhenie Pravitel'stva RF No 1632-r ot 28.07.2017 «Ob utverzhdenii programmy «Tsifrovaya ehkonomika Rossiiskoi Federatsii*. [Government of Russian Federation decree dated 07.28.2017 no. 1632-r «On Approval of the program «Digital Economy of the Russian Federation»]. Available at: static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (Accessed: June 22, 2023) (in Russ.).

41. Arabnezhad E., Morgia M.La., Mei A., Nemmi E.N., Stefa J. A Light in the Dark Web: Linking Dark Web Aliases to Real Internet Identities. *2020 IEEE 40th International Conference on Distributed Computing Systems.* Singapore, 2020, pp. 311–321. DOI: 10.1109/ICDCS47774.2020.00081

42. Simek O., Shah D., Heier A. Prototype and Analytics for Discovery and Exploitation of Threat Networks on Social Media. *2019 European Intelligence and Security Informatics Conference (EISIC)*. Oulu, Finland, 2019, pp. 9–16. DOI: 10.1109/EISIC49498.2019.9108895

43. Karpova A.Yu., Kuznetsov S.A., Savelev A.O., Vilnin A.D. An Online Scan of Extreme-Right Radicalization in Social Networks (The Case of the Russian Social Network VKontakte). *Journal of Siberian Federal University. Humanities and Social Sciences*, 2022, vol. 15, no. 12, pp. 1738–1750. DOI: 10.17516/1997-1370-0948

44. Dragos V., Battistelli D., Kelodjoue E. Beyond Sentiments and Opinions: Exploring Social Media with Appraisal Categories. *2018 21st International Conference on Information Fusion (FUSION)*. Cambridge, UK, 2018, pp. 1851–1858. DOI: 10.23919/ICIF.2018.8455751.

45. Liu X., Sun T., Bu F., Qin H. The Analysis on the Role of Social Network in the Field of Anti-Terrorism Take the «East Turkistan» Organization as an Example. *2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*. Harbin, China, 2020, pp. 2282–2285. DOI: 10.1109/ICMCCE51767.2020.00493

46. Ostapenko A.G., Parinov A.V., Kalashnikov A.O. *Sotsial'nye seti i destruktivnyi kontent*. [Social networks and destructive content]. Moscow, Scientific and technical publishing house «Hotline – Telecom» (Network warfare theory), 2018, 276 p.

47. Kashpur V.V., Petrov E.Yu., Gojko V.L., Feschenko A.V. [Possibilities of using digital footprints to predict educational achievements of students]. *Tomsk State University Journal of Philosophy, Sociology and Political Science*, 2021, no 64, pp. 140–150 (in Russ.).

48. Seshadri A., Park A.J., Stamato S.Z., Spicer V., Nguyen V.T., Song J. Graph Model of Environmental Backcloth. *2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. Vancouver, BC, Canada, 2022, pp. 0445–0451. DOI: 10.1109/IEMCON56893.2022.9946572

49. Dudina V.I. [From panopticon to panspectron: digital data and transformation of surveillance regimes]. *Sociological Research*, 2018, no 11(415), pp. 17–26 (in Russ.).

50. Krupenikova L.Sh. [Big data and new tasks of sociology]. *Humanities of the South of Russia,* 2022, vol. 11, no 2, pp. 50–57 (in Russ.).

51. Nitsevich V.F. [Digital sociology: theoretical and methodological origins and bases]. *Digital Sociology*, 2018, no. 1, pp. 18–28 (in Russ.).

52. Agieva M.T., Babicheva Yu.V., Okulist N.M., Ugol'nitskii G.A. [Analysis and forecasting problems in the control of target audience in marketing]. *Upravlenie bol'shimi sistemami: sbornik trudov* [Management of large systems: proceedings], 2019, vol. 79, pp. 27–64 (in Russ.).

53. Azarov A.A. [Profiling of Digital Network Users of Social Discontent in the Russian Federation Regions]. *Humanities and Social Sciences. Bulletin of the Financial University*, 2022, vol. 12, no. 5, pp. 105–113 (in Russ.).

54. Shumov, V.V. [Hierarchy of models of military *actions* and border conflicts]. *Upravlenie bol'shimi sistemami: sbornik trudov* [Management of large systems: proceedings] 2019, vol. 79, pp. 86–11 (in Russ.).

55. Azaouzi M., Rhouma D., Romdhane L.B. Community detection in large‐scale social networks: state‐of‐the‐art and future directions. *Social Network Analysis and Mining*, 2019, vol. 9, is. 1, no. 23. DOI: 10.1007 / s13278-019-0566-x. Available at: link.springer.com/article/10.1007/s13278-019-0566-x (Accessed: February 2, 2024).

56. Kryshtanovskaya O.V. [Contactless sociology: new forms of *researchin* a digital age]. *Digital Sociology*, 2018, no. 1, pp. 4–8 (in Russ.).

57. Milekhin, A.V. *Sotsiologicheskii monitoring – sredstvo informatsionnogo obespecheniya upravleniya v obshchestvennykh sistemakh. Diss. dokt. nauk* [Sociological monitoring is a means of information support for management in public systems: Doct. Diss]. Moscow, 1999. 327 p. (in Russ.).

58. Goryachev I.N. [The problem of dynamic balance of public]. *XXI century: Resumes of the Past and Challenges of the Present Plus*, 2013, vol. 2, no. 11, pp. 216–222 (in Russ.).

59. North D. *Instituty, institutsional'nye izmeneniya i funktsionirovanie ehkonomiki* [Institutions, institutional changes and the functioning of the economy]. Fund of the economic book «Beginning», Publ. 1997, 180 p. (in Russ.)

60. Burkov V.N., Novikov D.A. *Teoriya aktivnykh sistem: sostoyanie i perspektivy*. [Theory of active systems: state and prospects]. Moscow, Sinteg, 1999, 128 p. (in Russ.)

61. Tarasenko F.P. *Prikladnoi sistemnyi analiz: uchebnoe posobie* [Applied system analysis: study guide]. Moscow, Kronus, 2017, 220 p. (in Russ.)

62. *Ukaz Prezidenta Rossiiskoi Federatsii № 646 ot 05.12.2016 «Ob utverzhdenii Doktriny informatsionnoi bezopasnosti»*. [President of Russian Federation decree no. 646 dated 05.12.2016 «On the approval of the Information Security Doctrine»]. Available at: kremlin.ru/acts/bank/41460/page/1 (Accessed: June 24, 2023) (in Russ.).

63. Sudakova A.E. [Migration of scientists: digital footprint and scientometry]. *Perspectives of Science & Education*, 2020, № 3(45), pp. 544–557. DOI 10.32744/pse.2020.3.39 (in Russ.).

64. Golovko L.V. [The digitalization in criminal procedure: local optimization or global revolution?]. *Bulletin of Economic Security*, 2019, no 1, pp. 15–25 (in Russ.).

65. Akoff R., Ehmeri F. *O tseleustremlennykh sistemakh* [About purposeful systems]. Moscow, Book on demand, 2012. 270 p. (in Russ.).

66. Monastyrny E.A., Saklakov V.M. [Foreign investments as a mechanism for the Russian economy development] *Innovations*. 2015, no. 10, pp. 27–34 (in Russ.).

67. Monastyrny E.A., Spitsin V.V., Grik Ya.N. [Methodological approach to regional innovation development efficiency estimation]. *Innovations*, 2010, no. 1, pp. 80–86 (in Russ.).

68. Kuular Sh.V., Budukool L.K.-S. [Psychophysiological features of students with different types of conflict management strategies] // Novosibirsk State Pedagogical University Bulletin, 2017, vol. 7, no. 5, pp. 67–80 (in Russ.).

69. Kirdina-Chehndler, S. G., Kholl, D. [Cooperation versus competition in works of russian evolutionists] // *Journal of Institutional Studies*, 2017, vol. 9, no. 1, pp. 6–26 (in Russ.).

70. Taibi D., Fulantelli G., Basteris L. How do search engines shape reality? Preliminary insights from a learning experience. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020, vol. 11984 LNCS, pp. 370–377. DOI: 10.1007/978-3-030-38778-5_40

71. Tien J.H., Eisenberg M.C., Cherng S.T., Porter M.A. Online reactions to the 2017 «Unite the right» rally in Charlottesville: measuring polarization in Twitter networks using media followership. *Applied Network Science*, 2020, vol. 5, iss. 1, pp. 1–27. DOI: 10.1007/s41109-019-0223-3

72. Gaaze K. Max Weber's theory of causality: An examination on the resistance to post-truth. *Russian Sociological Review*, 2019, vol. 18, iss. 2, pp. 41–61. DOI: 10.17323/1728-192x-2019-2-41-61

73. Peters M.A., McLaren P., Jandric P.A Viral theory of post-truth. *Educational Philosophy and Theory*, 2020. DOI: 10.1080/00131857.2020.1750090

74. Khurgin V.M. *Ob opredelenii ponyatiya «Informatsiya»* [On the definition of the concept of «Information»]. *Informatsionnye resursy Rossii* [Information resources of Russia], 2007, no. 3, pp. 6–13 (in Russ.).

75. Shchedrovitskii P.G., Kuznetsov Yu.V. [From division of labour to division of activity]. *Philosophical Sciences*, 2014, no. 6, pp. 49–64 (in Russ.).

76. *GOST 15971-90 ot 01.01.1992. Sistemy obrabotki informatsii. Terminy i opredeleniya* [State standard 15971–90 dated 01.01.1992. Information processing systems. Terms and definitions:]. Available at: docs.cntd.ru/document/1200015664 (Accessed: June 22, 2023) (in Russ.).

77. ISO/IEC/IEEE 24765:2017. Systems and software engineering – Vocabulary. Available at: iso.org/obp/ui/#iso:std:iso-iec-ieee:24765:ed-2:v1:en (Accessed: June 22, 2023).

78. Persianov V.A., Kurbatova A.V. [Problematic issues of using the toolkit of economic cybernetics]. *Management*, 2019, vol. 7, no 3, pp. 94–102 (in Russ.).

79. Tikhonov A.V., Merzlyakov A.A., Rabinovich E.I., Kornilovich V.A., Zhavoronkov A.V., Korolyov A.L., Shilova V.A., Atayan I.M., Pashchenko V.V., Bogdanov V.S., Gradosel'skaya G.V., Prosyanyuk D.V., Raskhodchikov A.N., Dridze T.M., Bykov K.V. *Sotsiologiya upravleniya* [Sociology of management]. Moscow, Kanon+, 2014, 560 p. (in Russ.).

80. Tagirov Z.I. [Digitalization of Criminal Situation, Digital Human Name and Network Law Enforcement Activity in Digital Economy]. *Security Issues*, 2018, no. 4. pp. 28–51 (in Russ.).

81. Yudalevich N.V. [Information garbage as phenomenon of modern society] // *Business Education in the Knowledge Economy*, 2016, no. 2, pp. 119–122 (in Russ.).

82. Hashemi A., Zare Chahooki M.A. Telegram group quality measurement by user behavior analysis. *Social Network Analysis and Mining*, 2019, vol. 9, iss. 3, pp. 1–12. DOI: 10.1007/s13278-019-0575-9

83. Hosni A.I.E., Li K., Ahmad S. Analysis of the impact of online social networks addiction on the propagation of rumors. *Physica A: Statistical Mechanics and its Applications*, 2020, vol. 542, pp. 1–11. DOI: 10.1016/j.physa.2019.123456

84. Gavrilin Yu.V., Shmonin A.V. [Use of information obtained from the internet in the extremist crimes' investigation]. *Proceedings of Management Academy of the Ministry of the Interior of Russia*, 2019, no. 1, pp. 105–111 (in Russ.).

85. Monastyrny E.A., Saklakov V.M. [Classification of development institutions]. *Innovations*, 2013, no. 9, pp. 59–65 (in Russ.).

86. Eremchenko E.N. [Visualization and new definition of sign]. *GraphiCon 2018: trudy 28-i Mezhdunar. konf. po komp'yuternoi grafike i mashinnomu zreniyu* [GraphiCon 2018: Proceedings of the 28th International Conference on Computer Graphics and Machine Vision], Tomsk 2018, pp. 301–303 (in Russ.).

87. *Federal'nyi zakon «O vnesenii izmenenii v otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii po voprosam naznacheniya i vyplaty pensii» No 350-FZ ot 03.10.2018* [Federal Law «On Amending Certain Legislative Acts of the Russian Federation Concerning the Assignment and Payment of Pensions» no. 350-FZ of 03.10.2018] (in Russ.).

88. Babkin A.V., Novikov A.O. [To the question of the assessment of efficiency of programs of development of the industry]. *Teoriya i praktika servisa: ehkonomika, sotsial'naya sfera, tekhnologii* [Theory and practice of service: economics, social sphere, technology], 2016, no. 4, pp. 5–13 (in Russ.).

---

**Vasiliy M. Saklakov**
Senior Lecturer, Division for Information Technology,
National Research Tomsk Polytechnic University
84/3, Sovetskaya st., Tomsk, Russia, 634034
ORCID: 0000-0003-1716-4581
Phone: +7 953 914-08-17
Email: saklavas@tpu.ru

УДК 004.056.5

**П.И. Банокин**

# Модель поведения пользователя корпоративной информационной системы

Представлена модель поведения пользователя корпоративной информационной системы на основе графа де Брюина второго порядка и ассоциированных с вершинами графа признаков текстовых данных. Текстовые признаки созданы с учетом специфики данных, отображаемых в клиентских приложениях информационных систем. Модель позволяет определить отклонения в поведении, которые в том числе могут быть вызваны внутренними утечками данных. Определяемые с помощью модели отклонения включают сценарии выгрузки данных несвойственной тематики и доступа к данным типичной тематики, но с нарушением исполнения бизнес-процессов. Модель оценена на основе критериев полноты, адекватности и экономичности.

**Ключевые слова:** внутренние утечки данных, корпоративные информационные системы, модель поведения.
**DOI:** 10.21293/1818-0442-2023-26-4-78-83

Внутренняя утечка данных – это утрата конфиденциальности данных, произошедшая в результате действий сотрудника предприятия [1]. Рост активности преступников в области информационной технологий [2] и риски финансовых убытков [3] обусловливают актуальность защиты корпоративных данных. Согласно публикациям, количество случаев утечек корпоративных данных имеет устойчивую ежегодную тенденцию к увеличению [4]. Утечки данных наносят репутационный и экономический вред. По способу осуществления утечки данных разделяются на две категории: внешние и внутренние. В реализации внутренних утечек данных участвует сотрудник компании, который может выполнять заказ преступника на поставку данных [5]. Сотрудник имеет авторизованный доступ к интересующим заказчика данным и может быть хорошо осведомлен о мероприятиях и средствах обеспечения информационной безопасности. Одним из способов противодействия внутренним утечкам данных является использование специализированного программного обеспечения для анализа поведения пользователей. Модули анализа поведения пользователей предоставляются в различных пакетах DLP [6], но их исследование невозможно из-за закрытого исходного кода и лицензионных соглашений.

Поведение – это устоявшаяся система действий пользователя, учитывающая время, текущее и предыдущие состояния клиента КИС и возможные внешние воздействия. Модель поведения включает описание системы действий пользователя, позволяющее с помощью алгоритма идентификации утечек данных оценить степень нормальности (соответствия модели) действий пользователя.

Одной из ранних работ, посвященных анализу поведения и противодействию внутренним утечкам данных, является публикация [7]. В работе в качестве источника данных рассматривается коллекция лог-записей, используемая для формирования профилей поведения на основе статистических моделей. Формат лог-записи включает данные о пользователе, команде и объектах. В дальнейшем с увеличением сложности программного обеспечения и количества типов действий и событий для анализа поведения стали применяться методы обработки естественного языка и методы теории графов.

Методы обработки естественного языка включают метрики обратной частоты документа (inversed document frequency, IDF) [8, 9], применяемые для категориальных данных – типов событий, и векторные представления текстовых данных [10]. В работе [8] выявляются необычные частоты событий и необычное время их возникновения для обнаружения аномалий. В процессе выявления аномалий используется фиксированный перечень ранжированных по важности событий с применением метрики обратной частоты документа (IDF), в роли текстового документа выступает рабочий день сотрудника предприятия, содержащий перечень событий и сопоставленные им время и количественные значения. В исследовании [11] анализ текстовых данных лог-записей ограничен описанием события и базой синонимов и антонимов событий.

При моделировании поведения пользователей графовые модели создаются как для одного пользователя, так и для множества пользователей и программных ресурсов, в том числе с использованием двудольного графа [12]. Узлы графа с наибольшей степенью и ребра графа с максимальным весом присутствуют в последовательностях лог-записей, относящихся к классу нормального поведения [13]. В работе [13] степень нормальности поведения находится по категории подграфа, которая определяется рангом вершин и весом ребер. В случае анализа действий пользователя такая оценка накладывает ограничение на длину анализируемой подпоследовательности (окна) действий, так как с увеличением длины возрастает вероятность наличия шумовых данных из-за случайных ошибок в действиях сотрудника. Единичный случай посещения редкой вершины является маловероятным признаком осуществленной утечки данных, но посещение безопасных вершин безопасного подграфа может не учитывать нарушения бизнес-процессов. В задаче идентификации утечек данных более

предпочтительно создание моделей поведения для каждого пользователя отдельно, что позволит учитывать индивидуальные особенности поведения сотрудника с отбором информативных признаков. В работе [14] проводится совместный анализ последовательностей действий и вычисленных атрибутов, но не учитываются семантические признаки текстовых данных.

По способу реализации контроля за действиями пользователя можно выделить два подхода: наблюдение на сервере-источнике данных и наблюдение на конечном устройстве пользователя. При первом подходе упрощается архитектура системы предотвращения утечек данных, но возможны ограничения, накладываемые на процесс разработки программы-прокси для отслеживания сообщений – вызовов методов интерфейса программирования, из-за закрытого исходного кода КИС и системы управления базами данных. При втором подходе необходима установка программы-агента для наблюдения за действиями пользователя на клиентские устройства, но получаемые лог-записи могут включать более широкий набор атрибутов, в том числе графовые и текстовые данные. Текстовая составляющая представлена загруженными пользователем для просмотра записями корпоративной БД, а графовая – последовательностями перехода между элементами графического интерфейса клиента КИС. В статье в дальнейшем будет рассматриваться модель поведения при наблюдении на клиентских устройствах. Анализ данных графовой модели позволит определять нарушения в исполнении бизнес-процессов, а анализ текстовых данных – выявить обращения к данным несвойственной тематики.

В упомянутых выше работах не выполняется совместный анализ данных графовой и документной моделей, а также не учитывается специфика работы пользователя с КИС. Важными требованиями к модели являются объясняющая способность и возможность поиска поведенческих аномалий в коротких последовательностях действий. Объясняющая функция выражена в возможности получить характеристики поведения пользователя, включая перечень действий и признаки текстовых документов в момент обнаружения поведенческой аномалии. Поиск аномалий с использованием коротких последовательностей (окон) необходим для предотвращения хищений небольших выборок данных.

Целью работы является создание модели поведения пользователя КИС, удовлетворяющей представленными выше требованиям, и ее оценка критериями универсальности, адекватности и экономичности. В рамках исследования использованы методы теории графов и машинного обучения.

Новизна настоящей работы заключается в использовании графа де Брюина для создания модели поведения, хранящей ассоциированные со сменой состояний программы коллекции текстовых документов и их признаков, и алгоритма расчета веса вершин графа, учитывающего специфику работы с КИС. Особенностью программной реализации является получение текстовых данных корпоративных информационных систем на стороне клиента, что позволяет создавать лог-записи для облачных ERP-систем.

**Модель поведения пользователя**

При совершении пользователем действия при работе с интерфейсом клиента КИС создается лог-запись $x_i$ = (user, timestamp, text, uiElement, url), которая является вектором с компонентами, содержащими данные об идентификаторе пользователя, времени события, текстовых данных клиента КИС, идентификаторе элемента интерфейса и URL-адресе. Дано множество пользователей КИС $\mathbf{U} = \{u_i\}$. Пусть дана для каждого пользователя упорядоченная по времени поступления последовательность лог-записей $P_{u_i} = (x_1, x_2, ..., x_n)$ и задано множество состояний клиента КИС $\mathbf{S} = \{s_i\}$. Коллекция $P_{u_i}$ содержит данные о нормальном поведении пользователя: посторонние элементы отсутствуют или содержатся в крайне незначительном количестве. Состояние $s_i$ клиента КИС идентифицируется элементом управления интерфейса пользователя, при воздействии на который происходит изменение текстового содержимого клиента КИС. В случае веб-приложений таким идентификатором является значение xpath HTML-элемента интерфейса или часть этого значения при объединении нескольких элементов в один узел.

При наблюдении на клиентском устройстве пользователя значение атрибута text лог-записи $x_i$ включает все параграфы текста, отображаемые в графическом клиенте КИС. Для процесса анализа поведения необходимы только новые данные, полученные из корпоративной БД при смене состояния программы в результате совершения пользователем действия. Новые текстовые данные определяются как разность множеств

$$v_i^{<\text{pageText}>} = \mathbf{P}_{k+1} / \mathbf{P}_k \neq \varnothing,$$

где $\mathbf{P}_k$ – множество параграфов текста в состоянии программы в момент $k$, $\mathbf{P}_{k+1}$ – множество параграфов текста в состоянии программы в некоторый момент времени $k$+1, $v_i$ – вершина поведенческого графа.

Вычисление разности текстовых данных позволит получить только те параграфы текста, которые были найдены в результате изменения состояния прикладной программы. Кроме этого, из анализа будут исключены текстовые значения повторяющихся элементов интерфейса, включая меню, рубрикатор, строки состояния и другие элементы. При представлении перехода программы из состояния $s_k$ в состояние $s_{k+1}$ в виде объединённого узла $v(s_k s_{k+1})$ возможно построение графа де Брюина [15] второго порядка (рис. 2). Преимуществами использования графа второго порядка являются не только удобство получения измененных текстовых данных, но и хранение информации о предыдущем состоянии программы (контекста) в идентификаторе вершины. Использование графов более высокого порядка значительно увеличивает количество признаков-вершин и вычислительную сложность.

Таким образом, на основе накопленных лог-записей строится модель поведения, представленная графом второго порядка с вершинами, атрибуты которых хранят данные документной модели – текстовые данные и их признаки (рис. 1). Для создания поведенческого графа второго порядка дана коллекция лог-записей $P_{u_i}$, каждому элементу которой сопоставляется состояние из множества **S**. Узлы взвешенного поведенческого графа $\mathbf{G}=(V,E)$ представляют собой не отдельные состояния, а два связанных состояния $v_i=(s_t,s_{t+1})$. Одновременно с построением графа выполняется проход коллекции лог-записей $P_{u_i}$ окном window длины $l$ из множества перекрывающих окон Windows. Значение параметра $l$ соответствует среднему количеству действий пользователя, необходимого для исполнения единицы бизнес-процесса. В работе используется параметр $l$=24. Каждой вершине графа соответствуют два счетчика посещений: счетчик присутствия в окнах count_window и абсолютный счетчик присутствия в последовательности $P_{u_i}$ count_total.

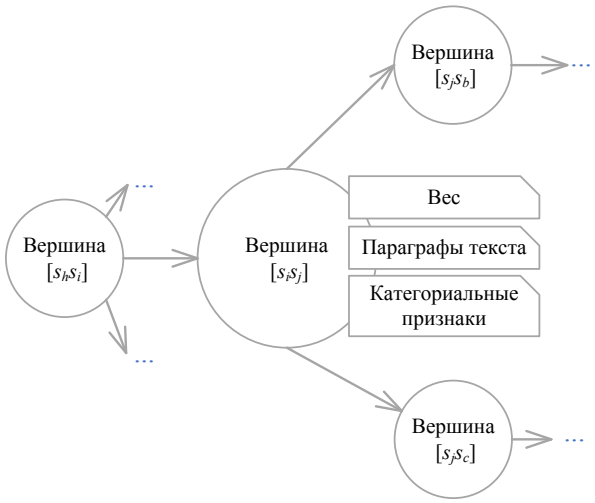



Рис. 1. Схема поведенческого графа

Значение count_window рассчитывается как сумма количества посещений вершины в каждом из временных окон:

$$v_i^{<\text{count\_window}>}=\sum_{|\text{Windows}|}\text{count}(v_i,\text{window}),$$

где count($v_i$, windows) – количество посещений вершины $v_i$ в окне window.

Итоговый вес узла $v_i$ рассчитывается по формуле и учитывает значимость узла по присутствию в последовательностях действий, понижая вес повторяющихся действий при исполнении бизнес-процессов:

$$\text{weight}(v_i)=\frac{v_i^{<\text{count\_total}>}}{v_i^{<\text{count\_window}>}}.$$

Также узлы $v_i$ графа **G** имеют атрибуты text_features, pageText, times. Атрибут узла $v_i^{<\text{text\_features}>}$ содержит коллекцию признаков текстовых данных, вычисленных на основе коллекции параграфов $v_i^{<\text{page\_text}>}$. Атрибут узла $v_i^{<\text{times}>}$ содержит коллекцию интервалов времени, в течение которых программа находилась в вершине $v_i$. Интервалы времени могут быть использованы как косвенный признак изменений поведения при подробном изучении обнаруженной аномалии. Вес ребра графа определяется отношением количества переходов по ребру edge($v_i$,$v_j$) к общему числу переходов в вершину $v_j$:

$$\text{weight}(v_i,v_j)=\frac{\text{count}(v_i,v_j)}{v_j^{<\text{count\_total}>}},$$

где count($v_i$, $v_j$) – количество переходов из вершины $v_i$ в вершину $v_j$.

Текстовые данные КИС создаются сотрудниками или поступают в корпоративную БД от сторонних организаций или программных сервисов. Текстовые документы могут быть созданы на основе типовых форм и лишены грамматической структуры и авторского стиля. В ряде случаев параграфы текста могут представлять собой короткие текстовые метки элементов интерфейса. Эти особенности делают невозможным применение методов определения авторства текста, включающих исследование стилистики текста, лексического разнообразия и других авторских особенностей. Поэтому необходимо при создании модели учитывать возможность проверки степени схожести новых текстовых документов с ранее наблюдаемыми текстовыми данными на основе категориальных признаков, полученных из текста. Примерами специфичных для корпоративного использования признаков являются следующие характеристики текста: почтовые индексы, телефонные номера, валютные коды, товарные категории, названия юридических лиц, географические коды и др.

Пусть задано множество категориальных признаков $\mathbf{Z}=\{Z_1,Z_2,...,Z_n\}$, вычисляемых в коллекции параграфов вершин $v_i^{<\text{page\_text}>}$ графа с множеством значений $\mathbf{C}=\mathbf{C}_1\cup\mathbf{C}_2\cup...\cup\mathbf{C}_n$. Каждый признак $Z_i$ имеет соответствующее ему множество значений $\mathbf{C}_i=\{c_0^i,c_2^i,c_2^i,...,c_{|C_i|}^i\}$ и функцию-гистограмму распределения этих значений $\text{hist}(c_j^i,\mathbf{C}_i)\to\mathbf{R}$, полученную на основе выборки $P_{u_i}$. Значение $c_0{}^i$ выполняет роль индикатора наличия значения, ранее не наблюдаемого в накопленной коллекции $P_{u_i}$.

Перед оценкой безопасности поведения пользователя происходит создание объекта модели – поведенческого графа второго порядка с вычисленными весами вершин и атрибутами. Оценка безопасности поведения производится с использованием последовательности новых лог-записей (временных окон) window = ($x_t$, $x_{t+1}$, ..., $x_{t+l}$) длины $l$ переходов по вершинам поведенческого графа. Для выбора параметра $l$ необходимо учитывать характер обнаруживаемых аномалий, которые по мере увеличения длины окна могут включать ошибки при работе с интерфейсом программы (несколько переходов по ребрам с низким

весом), кратковременные нарушения бизнес-процессов (выгрузка небольших выборок данных) и последовательную выгрузку данных во время перерывов в работе сотрудника. Окно window преобразуется в вектор окна $w = (\text{weight}(v_1) * v_1, ..., \text{weight}(v_m) * v_m, c_1, ..., c_{|\mathbf{C}|})$, где компоненты $\text{weight}(v_i) * v_i$ содержат количества посещений вершины $v_i$ с учетом ее веса $\text{weight}(v_i)$ в графе **G**, а компоненты $c_i$ – количества обнаруженных значений признаков из множества **C**. Значения компонент вектора $w$ нормализуются отдельно для каждого подмножества значений признака $Z_i$. Подмножества компонент вектора $w$ обрабатываются функциями поиска аномалий. Отдельная обработка подмножеств позволяет объяснить причину поведенческой аномалии. При обнаружении аномалии по несоответствию тематики происходят детализация на основе атрибутов вершин подграфа $\mathbf{G}_{\text{window}}$ и указания несоответствия значений признаков ранее наблюдаемому распределению признаков вершин. При нарушении типичного исполнения бизнес-процессов происходит детализация с указанием весов ребер, степени вершин и продолжительности посещения вершин.

Оценка соответствия последовательности window поведенческому графу производится с помощью функции поиска аномалий, реализация которой может быть выполнена на основе нейронной сети архитектуры автокодировщик, основе ансамбля классификаторов на основе сравнения гистограмм распределения значений и других алгоритмов поиска посторонних значений.

**Оценка модели**

Модель оценивается критериями универсальности, адекватности и экономичности. Представленная модель учитывает текстовые данные КИС и последовательности действий пользователя, тем самым является более универсальной по сравнению с моделями, учитывающими только текстовые данные или только последовательности действий и событий.

Экономичность модели обеспечивается хранением только измененных текстовых данных и вычисленных признаков и включением в поведенческий граф второго порядка ограниченного подмножества вершин, наблюдаемых в процессе мониторинга поведения.

Для оценки адекватности модели в качестве нулевой гипотезы выбрано утверждение о том, что поведение пользователя является нормальным. Для этого загружены лог-записи десяти пользователей ERP-системы 1С:Розница. Посторонние записи получены при выполнении пользователями инструкции-сценария, представляющей случай поведенческой аномалии.

Для наблюдения за пользователями и получения лог-записей (табл. 1) использовано расширение для веб-браузера Google Chrome. В качестве идентификаторов элементов интерфейса пользователя использованы значения атрибута xpath. Малоиспользуемые элементы интерфейса (например, отдельные строки таблиц) объединены в один узел на основе иерархии xpath. В роли характеристик текстовых данных использованы именованные сущности, префиксы телефонных номеров и подмножества почтовых индексов. Для выявления именованных сущностей использована библиотека pymorphy3.

Таблица 1

**Характеристики набора данных**

| Пример последовательности действий | Тип поведения |
|---|---|
| Количество лог-записей | 302,3 шт./ч |
| Количество элементов интерфейса | 18 |
| Количество вершин графа де Брюина второго порядка | 324 |
| Количество элементов ограниченного множества вершин графа де Брюина второго порядка | 49 |
| Размер временного окна | 24 |
| Количество признаков текстовых данных | 40 (32 – именованные сущности, 8 – географические коды) |

При выполнении экспериментального анализа проверены два сценария утечек данных:

1. Единичные случаи (табл. 2). Пользователь в течение рабочего дня просматривает несколько интересующих записей. Содержание записей соответствует служебным обязанностям сотрудника, но записи просмотрены с целью хищения данных. Последовательность работы с инструментами КИС при обычном исполнении бизнес-процессов нарушена. Например, пользователь совершает переходы: главная страница, новое обращение, список клиентов, список клиентов, анкета клиента, анкета клиента. При этом отсутствуют узлы графа «оформление обращения», «обращение создано».

2. Выгрузка записей несвойственной тематики. Пользователь в течение рабочего дня находит интересующие записи, открывая справочник с анкетами клиентов. Содержание записей не соответствует обычной работе пользователя. Например, пользователь открывает анкеты клиентов с несвойственным географическим кодом.

Таблица 2

**Примеры обычной и аномальной последовательности действий для сценария № 1**

| Пример последовательности действий | Тип поведения |
|---|---|
| (0) Главная страница<br>(1) Заказы<br>(2) Новый<br>(3) Контрагенты<br>(4) Выбор<br>(5) Продукция<br>…..<br>(7) Продукция<br>(8) Оформить<br>(9) Главная страница | Обычное |
| (0) Главная страница<br>(1) Заказы<br>(2) Новый<br>(3) Контрагенты<br>.....<br>(8) Контрагенты<br>(9) Главная страница | Аномальное (выгрузка данных контрагентов) |

Для имитации поведенческих аномалий в отдельные временные окна добавлены лог-записи, полученные при наблюдении за пользователями при выполнении сценариев № 1 и № 2.

Разреженность многомерных данных, представленных коллекцией векторов временных окон, накладывает ограничения на выбор алгоритма для поиска аномалий, включая алгоритмы на основе сравнения гистограмм [14]. В данной рассматриваемой модели отдельные лог-записи или векторы временных окон могут иметь менее 50% ненулевых атрибутов. Для поиска аномальных значений использована нейронная сеть архитектуры «автокодировщик» [17] с тремя скрытыми слоями и функцией активации сигмоида.

Произведена проверка идентификации поведенческих аномалий с помощью автокодировщика с применением данных графа первого и второго порядков для сценария № 1 (табл. 3) и сценария № 2 (табл. 4). При нарушении исполнения бизнес-процессов возникало превышение ошибки репликации (рис. 2). Использование графа де Брюина второго порядка позволяет повысить точность определения аномалий.

Таблица 3

**Результаты эксперимента по поиску посторонних элементов сценария № 1**

| Алгоритм | Площадь под ROC-кривой |
|---|---|
| Автокодировщик вершин графа второго порядка | 0,909 |
| Автокодировщик на основе текстовых данных и вершин графа второго порядка | 0,813 |
| Автокодировщик на основе текстовых данных и вершин графа первого порядка | 0,631 |

Таблица 4

**Результаты эксперимента по поиску посторонних элементов сценария №2**

| Алгоритм | Площадь под ROC-кривой |
|---|---|
| Автокодировщик на основе текстовых данных | 0,874 |
| Автокодировщик на основе текстовых данных и вершин графа второго порядка | 0,821 |

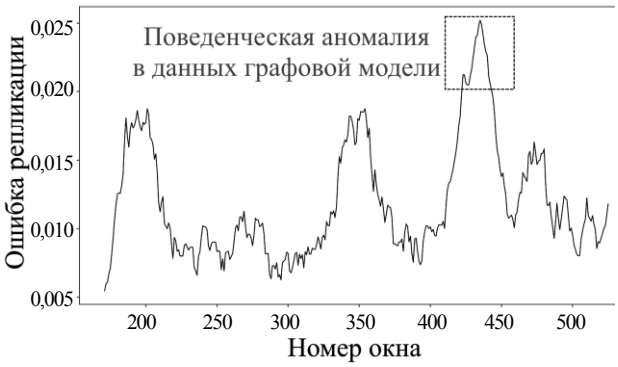



Рис. 2. Поведенческая аномалия для сценария № 1

Поиск аномалий в отдельном подмножестве признаков документной модели (текстовых данных) более предпочтителен (см. табл. 4).

**Заключение**

В результате выполненной работы создана модель поведения пользователя корпоративной информационной системы, которая позволяет находить поведенческие аномалии, характеризующиеся изменениями в последовательностях действий пользователя или использованием текстовых данных нетипичной тематики. Использование поведенческого графа второго порядка позволяет повысить точность классификации при использовании автокодировщика для поиска посторонних значений. С использованием модели обнаруженная аномалия может быть детализирована в виде подграфа поведения с указанием последовательностей смены состояний клиента КИС и связанными с изменением состояний признаков текстовых данных.

Работа выполнена в рамках проекта «Гранты ИБ МТУСИ» 2022.

*Литература*

1. Shabtai A. A survey of data leak-age detection and prevention Solutions. / A. Shabtai, Y. Elovici, L. Rokach. – Berlin, Germany: Springer, 2012. – 92 p.

2. Исакова Т. На работу, как на фишинг / Т. Исакова, Н. Королев // Газета «Коммерсантъ». – 08.08.2022. – Ст. 18.

3. «Ростелеком» оштрафовали на 60 000 рублей за утечку пользовательских данных // Хакер [Электронный ресурс]. – Режим доступа: URL: https://xakep.ru/2023/04/19/rostelekom-penalty/ (дата обращения: 19.04.2023).

4. Курашева А. Количество утечек данных в крупных компаниях выросло в 1,5 раза // Ведомости. – 2023. – 12.05. – Ст. 19.

5. Принцип работы Solar Dozor // Ростелеком [Электронный ресурс]. – Режим доступа: URL: https://rt-solar.ru/products/solar_dozor/architecture/ (дата обращения: 24.09.2023).

6. Евсиков В. Пробей меня полностью! Кто, как и за сколько пробивает персональные данные в России // Хакер. – 2020. – № 10 [Электронный ресурс]. – Режим доступа: https://xakep.ru/2020/10/09/personal-data/ (дата обращения: 05.09.2023).

7. Denning D.E. An Intrusion Detection Model // IEEE transactions on software engineering. – 1987. – Vol. SE-13. – P. 222–232.

8. Hu J. Anomalous User Activity Detection in Enterprise Multi-Source Logs / J. Hu, T. Baoming, D. Lin // International Conference on Data Mining Workshops. – New Orleans, USA: IEEE, 2017. – P. 797–803.

9. Mohotti W. Efficient outlier detection in text corpus using rare frequency and ranking / W. Mohotti, R. Nayak // ACM Transactions on Knowledge Discovery from Data. – 2020. – Vol. 14, No. 6. – P. 1–30.

10. Haixuan G. LogBERT: Log Anomaly Detection via BERT / G. Haixuan, Y. Shuhan, W. Xintao// International Joint Conference on Neural Networks (IJCNN). – Shenzhen, China: IEEE, 2021. – P. 1–8.

11. Weibin M. et al. LogAnomaly: Unsupervised Detection of Sequential and Quantitative Anomalies in Unstructured Logs // Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence. – Macao, China: IJCAI, 2019. – P. 4739–4745.

12. A Graph Embedding Approach to User Behavior Anomaly Detection / A. Modell, J. Larson, M. Turcotte, A. Bertiger // GTA 2.0: The 5th IEEE Big Data Workshop on Graph

Techniques for Adversarial Activity Analytics. – New Jersey, USA: IEEE, 2021. – P. 2650–2655.

13. Modelling User Behavior Dynamics with Embeddings / L. Han, A. Checco, D. Difallah, G. Demartini, S. Sadiq // CIKM '20: Proceedings of the 29th ACM International Conference on Information & Knowledge Management. – NY, USA: ACM, 2020. – P. 445–454.

14. Boniol P. Series2Graph: graph-based subsequence anomaly detection for time series / P. Boniol, T. Palpanas // Proceedings of the VLDB Endowment. – Tokyo: VLDB Endowment, 2020. – P. 1821–1834.

15. Bruijn de N.G. A combinatorial problem // Proceedings of the Section of Sciences of the Koninklijke Nederlandse Akademie van Wetenschappen te Amsterdam. – 1941. – Vol. 49, No. 7. – P. 758–764.

16. Pevny T. Loda: Lightweight on-line detector of anomalies // Machine Learning. – 2016. – Vol. 102. – P. 275–304.

17. Autoencoder-based outlier detection for sparse, high dimensional data / W. Chen, H. Li, H. Li, A. Arshad // Proceedings of 2020 IEEE International Conference on Big Data (Big Data). – Atlanta, USA: IEEE, 2020. – P. 2735–2742.

---

**Банокин Павел Иванович**
Преп. каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)
Томского государственного ун-та
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: + 7 (382-2) 70-15-29
Эл. почта: pavel805@gmail.com

Banokin P.I.
**Model of corporate information system user behavior**

A behavior model of corporate user is presented. The model is based on a De Bruijn graph, where the vertices store the features of text data. The values of textual features are extracted with regard to the data displayed in the client application information system. The model could be used to identify the behavioral anomalies, that could be linked to internal data leaks. The scope of detected behavioral anomalies includes scenarios of the corrupted business process flow and the data leakage of an unusual topic. The model is evaluated by criteria of efficiency, adequacy and completeness.

**Keywords:** internal data leaks, corporate information systems, behavior model.
**DOI:** 10.21293/1818-0442-2023-26-4-78-83

*References*

1. Shabtai A., Elovici Y., Rokach L. *A survey of data leakage detection and prevention Solutions*. Berlin, Germany, Springer, 2012, 92 p., pp. 39-46,

2. Isakova T., Korolev N. *Na rabotu kak na fishing*. [To go to work as to go fishing]. Newspaper «Kommersant», 08.08.2022, art. 18 (in Russ.).

3. *«Rostelekom» oshtrafovali na 60 000 rublei za utechku polzovatelskih dannyh* [Rostelecom is fined 60 000 rubles for personal data leakage]. *Haker* [Hacker]. Available at: https://xakep.ru/2023/04/19/rostelekom-penalty/, free (Accessed: April 19, 2023). (in Russ.).

4. Kurasheva A. *Kolichestvo utechek dannyh v krupnih kompaniyah uvelichlos v 1.5 raza* [The number of data leaks increased 1.5 times in large corporations]. *Vedomosti*, 2023, 12.05, article 19 (in Russ.).

*5. Printsip raboty Solar Dozor [The princi*ple of Solar Dozor]. Rostelecom. URL: https://rt-solar.ru/products/solar_dozor/architecture/ (Accessed: September 24, 2023) (in Russ.).

6. Evsikov V. *Probej menya polnost'yu. Kto, kak I za skolko probivaet personalnie dannie v Rossii* [Get my full personal data details! Who, how and for how much does it cost to access personal data in Russia?]. *Haker* [Hacker], 2020, no. 10. Available at: https://xakep.ru/2020/10/09/personal-data/ (Accessed: September 5, 2023) (in Russ.).

7. Denning D.E. An Intrusion Detection Model. *IEEE transactions on software engineering*, 1987, vol. SE-13, pp. 222–232.

8. Hu J., Baoming T., Lin D. Anomalous User Activity Detection in Enterprise Multi-Source Logs. *International Conference on Data Mining Workshops*, New Orleans, USA, IEEE, 2017, pp. 797–803.

9. Mohotti W., Nayak R. Efficient outlier detection in text corpus using rare frequency and ranking. *ACM Transactions on Knowledge Discovery from Data*, 2020, vol. 14, no. 6, pp. 1–30.

10. Haixuan G., Shuhan Y., Xintao W. LogBERT: Log Anomaly Detection via BERT. *International Joint Conference on Neural Networks* (*IJCNN*), Shenzhen, China, IEEE, 2021, pp. 1–8.

11. Weibin M. [et al.] LogAnomaly: Unsupervised Detection of Sequential and Quantitative Anomalies in Unstructured Logs. *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence*, Macao, China, IJCAI, 2019, pp. 4739–4745.

12. Modell A., Larson J., Turcotte M., Bertiger A. A Graph Embedding Approach to User Behavior Anomaly Detection. GTA 2.0: *The 5th IEEE Big Data Workshop on Graph Techniques for Adversarial Activity Analytics*, New Jersey, USA, IEEE, 2021, pp. 2650–2655.

13. Boniol P., Palpanas T. Series2Graph: graph-based subsequence anomaly detection for time series. *Proceedings of the VLDB Endowment*, Tokyo, Japan, VLDB Endowment, 2020, pp. 1821–1834.

14. Han L., Checco A., Difallah D., Demartini G., Sadiq S. Modelling User Behavior Dynamics with Embeddings. CIKM '20: *Proceedings of the 29th ACM International Conference on Information & Knowledge Management*, NY, USA, ACM, 2020, pp. 445–454.

15. Bruijn de N.G. A combinatorial problem. *Proceedings of the Section of Sciences of the Koninklijke Nederlandse Akademie van Wetenschappen te Amsterdam*, 1941, vol. 49, no. 7, pp. 758–764.

16. Pevny T. Loda: Lightweight on-line detector of anomalies. *Machine Learning*, 2016, vol. 102, pp. 275–304.

17. Chen W., Li H., Li H., Arshad A. Autoencoder-based outlier detection for sparse, high dimensional data. *Proceedings of 2020 IEEE International Conference on Big Data* (*Big Data*), Atlanta, USA: IEEE, 2020, pp. 2735–2742.

---

**Pavel I. Banokin**
Lecturer, Department of Complex Information
Security of Electronic Computer Systems (KIBEVS),
Tomsk State University of Control Systems
and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: + 7 (382-2) 70-15-29
Email: pavel805@gmail.com

УДК 004.94

**Т.Н. Зайченко, В.М. Дмитриев, Т.В. Ганджа**

# Организация учебного компьютерного эксперимента в системе многоуровневого моделирования МАРС

Рассматривается методика организации учебного компьютерного эксперимента в системе многоуровневого моделирования МАРС на примере схемы из области электроники. Представлен алгоритм действий преподавателя при создании компьютерной лабораторной работы и студента при ее выполнении.
**Ключевые слова:** компьютерный эксперимент, многоуровневая модель, компонент, система МАРС.
**DOI:** 10.21293/1818-0442-2023-26-4-84-88

Компьютерный эксперимент является неотъемлемым методом исследования и в настоящее время широко применяется во всех видах деятельности и отраслях наук [1]. Результаты такого эксперимента зависят не только от правильности задания исходных данных об исследуемом объекте, но и от выбранных метода и параметров решения математической модели, а также знания предметной области, что позволяет оценить корректность полученных результатов и принять решение либо об окончании эксперимента, либо о необходимости поиска ошибок и их исправления.

Важную роль приобретает компьютерный эксперимент в учебном процессе в связи с бурным развитием технологий дистанционного обучения [2]. Учебный компьютерный эксперимент реализуется с использованием различных программных средств моделирования, предоставляющих возможности моделирования широкого класса устройств. В области исследования устройств электротехники и электроники – это системы Matlab/Simulink, MicroCAP [3–5] и др. Учебный компьютерный эксперимент сложен тем, что студенту трудно оценить правильность полученных результатов, поскольку предметная область им только изучается, а также иногда сложно выбрать метод и параметры решения модели, так как компетенции в области применения численных методов и систем моделирования могут еще отсутствовать. Эксперимент всегда ограничен во времени длительностью аудиторных занятий либо объемом часов самостоятельной работы. В этой связи возникает необходимость исследования методики проведения учебного компьютерного эксперимента и его оптимизации.

Ниже исследуется методика проведения учебного эксперимента в среде моделирования МАРС, разрабатываемой в ТУСУРе [6] и использующейся для создания виртуальных лабораторий в области электротехники и электроники.

**Компьютерный эксперимента в системе МАРС**

Система МАРС предназначена для исследования физически неоднородных технических устройств, а также социально-экономических систем. Ее теоретической основой является метод компонентных цепей (КЦ), обеспечивающий автоматическое формирование и решение математической модели исследуемого объекта, заданного его моделью структуры в виде компонентной цепи. Язык компонентных цепей близок к инженерному языку соответствующей предметной области – языку принципиальных (электрических, кинематических, электрокинематических), структурных и т.п. схем. Для моделирования устройства необходимо построить его КЦ, задать способ визуализации и обработки результатов, режим анализа, шаги решения модели и точность.

В системе МАРС для организации эксперимента предусмотрены три уровня [7], или слоя, – объектный (схемный), логический и визуальный, на каждом из которых используется формализм КЦ. На объектном слое осуществляется формализованное представление исследуемого объекта в виде КЦ.

Результаты моделирования могут быть представлены в форме графиков. Для создания более реалистичного эксперимента предусмотрены компоненты средств эксперимента (средства измерения, индикации, управления, регулирования). Геометрические модели лицевых панелей соответствующих приборов отображаются на визуальном слое. Логический слой используется для связи между объектным и визуальным слоями, а также для описания процесса дополнительной обработки результатов моделирования.

В настоящей работе организация компьютерного эксперимента в системе МАРС рассматривается кратко на примере исследования устройства электроники – выпрямителя со сглаживающим фильтром. Цель исследования заключается в расчете временных диаграмм характерных токов и напряжений элементов схемы (входное и выходное напряжение, напряжение на диоде, токи диода и нагрузки), исследовании влияния емкости конденсатора и сопротивления нагрузки на выходное напряжение и режим работы диода.

На объектном уровне осуществляется формализованное представление исследуемого объекта. КЦ для выпрямителя (рис. 1) построена на базе схемы электрической принципиальной, в которую включены вольтметры для измерения входного и выходного напряжения и амперметры для измерения токов диода и нагрузки. Если результаты моделирования отображаются на графике, то третьи дополнительные выходы вольтметров и амперметров подключаются к компоненту «график» (см. рис. 1).

Перед началом моделирования необходимо задать режим анализа (анализ во временной области), численный метод решения (например, неявный метод Эйлера), начальное и конечное время моделирования и шаги решения модели (с учетом частоты питающего напряжения) и точность решения (с учетом значений токов и напряжений элементов схемы). Пользователю, обладающему компетенциями в области моделирования, это сделать несложно. Анализируя временные диаграммы, можем определить амплитудные значения тока и напряжения на диоде, рассчитать коэффициент пульсаций.

**Учебный компьютерный эксперимент в системе МАРС**

Для создания более реалистичного учебного эксперимента за счет визуализации напряжений и токов на панелях приборов и получения студентами навыков работы с реальными измерительными приборами, средствами управления и регулирования в КЦ включаются двухканальные осциллографы «двухканальный осциллограф 1», «осциллограф 2» (см. рис. 1), а также средства управления и измерения. Геометрические модели осциллографов, помещенные на объектном слое, отображаются на визуальном слое (рис. 2, см. «двухканальный осциллограф 1», «двухканальный осциллограф 2»).

В рассматриваемом примере исследования выпрямителя средствами управления являются регуляторы сопротивления нагрузки «Регулятор *R*н» и емкости конденсатора сглаживающего фильтра «Регулятор *C*ф» (см. рис. 2).

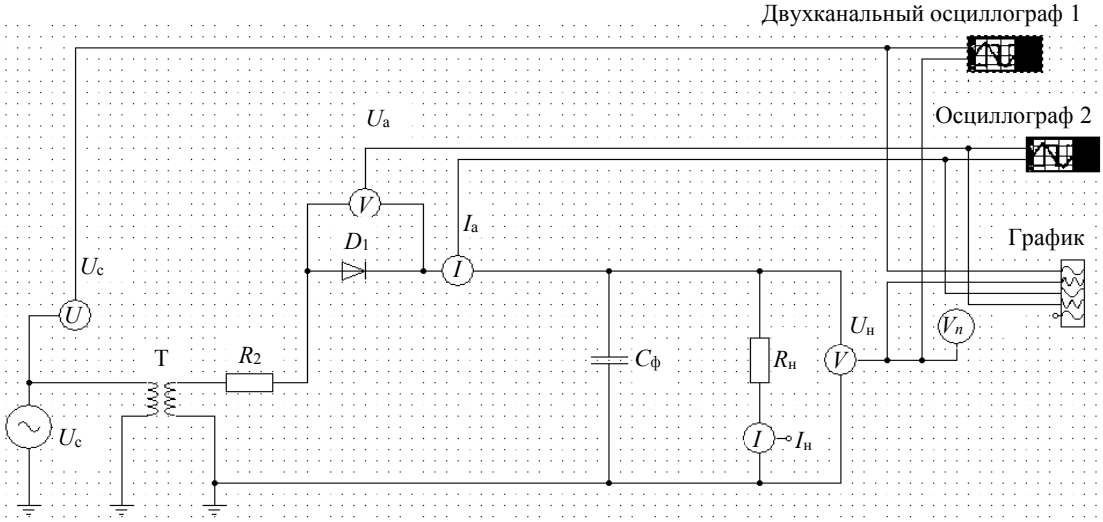



Рис. 1. Компонентная цепь выпрямителя с емкостным фильтром на объектном слое

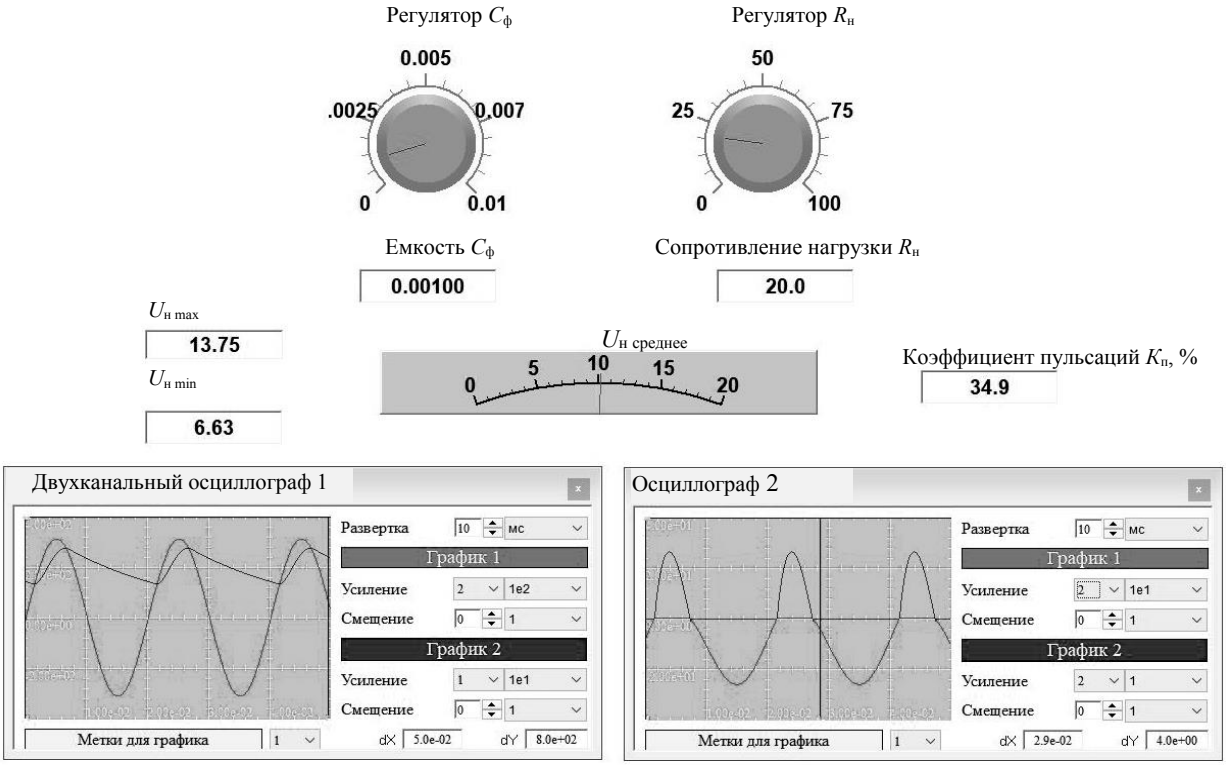



Рис. 2. Компоненты регуляторы, индикаторы и осциллографы, расположенные на визуальном слое

Связь компонентов объектного и визуального слоев осуществляется посредством компонентов логического слоя (рис. 3). Регулятор емкости конденсатора сглаживающего фильтра *С*ф и регулятор сопротивления нагрузки $R_н$, а также индикаторы этих параметров (компоненты вида 1.0 ) находятся на логическом и визуальном слоях (см. рис. 2, 3). Связь регуляторов с параметрами компонентов конденсатора $C_ф$ и резистора $R_н$ осуществляется посредством компонентов-атрибутов (компоненты вида *A* ) на логическом слое (см. рис. 2). Следует отметить, что минимальное и максимальное значения на шкале регуляторов являются параметрами компонентов и должны задаваться пользователем.

Для уменьшения времени выполнения лабораторной работы можно предусмотреть автоматическое определение амплитудных значений тока диода и напряжения на диоде, автоматический расчет коэффициента пульсаций. Для этого на логическом слое с использованием формализма структурных схем может быть задана математическая модель обработки экспериментальных данных. Структурная схема, представленная, на рис. 3, реализует приближенный расчет коэффициента пульсаций по формуле

$$K_п = \frac{\frac{1}{2}\left(U_{н\,max} - U_{н\,min}\right)}{\frac{1}{2}\left(U_{н\,max} + U_{н\,min}\right)} 100\,[\%],$$

где $U_{н\,min}$, $U_{н\,max}$ – минимальное и максимальное значения напряжения нагрузки.

Передача значений выходного напряжения на логический слой для последующей обработки осуществляется компонентом вида $V_n$. Он отображается на объектном и логическом слоях (см. рис. 1, 3).

Для выполнения исследования выпрямителя требуется задать параметры моделирования, выполнить команду «расчет» и наблюдать за результатами на экране виртуальных осциллографов и индикаторов (см. рис. 2), изменяя параметры элементов схемы с помощью регуляторов согласно плану эксперимента.

**Методические указания по подготовке учебного компьютерного эксперимента в системе МАРС**

Для сокращения длительности учебного эксперимента следует минимизировать те действия студента, которые не связаны непосредственно с изучением объекта исследования. Такими действиями являются: выделение набора компонентов системы МАРС для построения КЦ объектного слоя, наполнение визуального и логического слоев, задание метода и параметров моделирования. Наиболее трудоемким является построение КЦ логического слоя. Поэтому целесообразно для каждой работы создавать шаблон компьютерного эксперимента, включающий: КЦ либо набор компонентов объектного слоя; КЦ визуального и логического слоев; набор параметров моделирования.

Следует отметить, что изменение параметров КЦ исследуемого устройства может привести к необходимости изменения минимального и максимального значений параметров регуляторов визуального слоя. Например, изменение частоты питающего напряжения приведет к необходимости корректировки диапазона варьирования емкости конденсатора фильтра. Это следует предусмотреть при подготовке учебного эксперимента.

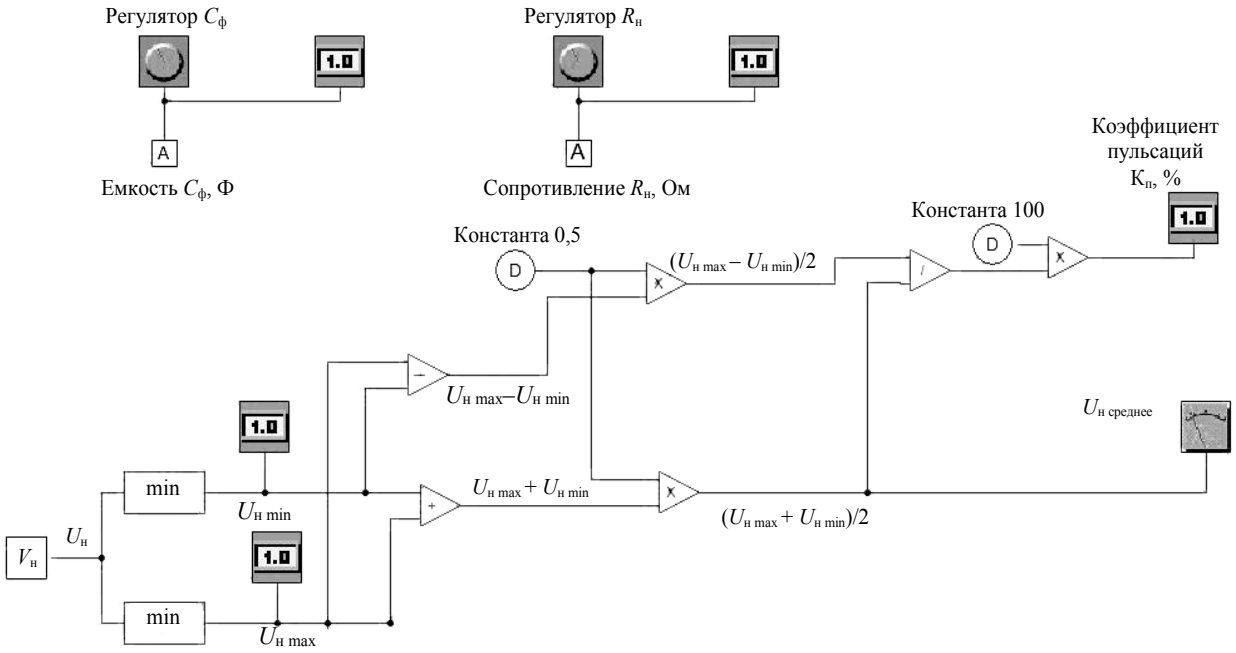



Рис. 3. Логический слой с компонентами регуляторами, индикаторами и компонентной цепью для расчета коэффициента пульсаций

Для разработки преподавателем лабораторной работы в системе МАРС предлагается следующий алгоритм:

1. Ознакомиться с библиотекой моделей компонентов в системе МАРС и разработать план компьютерного эксперимента и КЦ слоев многоуровневой модели.

2. Выполнить моделирование схемы исследуемого объекта в системе МАРС с использованием всех необходимых слоев для одного из вариантов.

2.1. Создать КЦ объектного и логического слоев, разместить компоненты визуального слоя (измерители, регуляторы, индикаторы).

2.2. Подобрать диапазон изменения варьируемых параметров. Задать параметры шкал компонентов (регуляторов, индикаторов) визуального слоя.

2.3. Выбрать метод и параметры моделирования.

2.4. Выполнить расчет и тестирование модели, при необходимости возвращаясь к шагам 2.1–2.3.

3. Сохранить отлаженную модель по варианту ЛР в файл «ЛР№_Вар№_Набор компонентов». При этом сохранятся все КЦ и параметры моделирования.

Если предполагается, что схему исследуемого объекта студент должен создать сам, то связи между элементами в файле «ЛР№_Вар№_Набор компонентов» следует удалить.

4. Выполнить шаги 2 и 3 для всех вариантов лабораторной работы.

Тогда работа студента при выполнении лабораторной работы будет состоять из следующих шагов:

1. Изучить методические указания, получить у преподавателя номер варианта лабораторной работы.

2. Открыть файл «ЛР№_Вар№_Набор компонентов». При этом на схемном слое откроется КЦ (либо набор компонентов, которые используются при выполнении лабораторной работы), а на визуальном слое – измерительные приборы, регуляторы и индикаторы. Логический слой не отображается.

3. Сохранить файл «ЛР№_Вар№_Набор компонентов» под другим именем и всю дальнейшую работу проводить с ним.

4. Выполнить исследование схемы, меняя схему либо параметры элементов схемы согласно методическим указаниям.

5. Зафиксировать результаты моделирования, оформить отчет и сделать выводы о проделанной работе.

**Заключение**

Предлагаемая методика организации учебного компьютерного эксперимента при исследовании устройств электротехники и электроники позволяет преодолеть ограничения по длительности эксперимента и компетентности студентов в области численных методов моделирования. Она может применяться при разработке виртуальных лабораторий по широкому спектру дисциплин.

У авторов имеется опыт разработки и применения в учебном процессе виртуальной лаборатории по дисциплине «Теоретические основы электротехники». Дальнейшее развитие связано с созданием учебных лабораторий по электронике, системам автоматического управления и др.

*Литература*

1. Кориков А.М. Эксперимент в научном исследовании // Доклады ТУСУР. – 2015. – № 2(36). – С. 148–156.

2. Развитие программно-методического обеспечения технологий электронного обучения в ТУСУРе / А.В. Городович, О.Ю. Исакова, И.А. Кречетов, В.В. Кручинин, Ю.В. Морозова, В.В. Романенко, И.П. Черкашина // Доклады ТУСУР. – 2017. – Т. 20, № 3. – С. 62–69.

3. Герман-Галкин С.Г. Виртуальные лаборатории полупроводниковых систем в среде Matlab-Simulink: учеб.-метод. пособие. – СПб.: Лань, 2022. – 448 с.

4. Фролов В.Я. Устройства силовой электроники и преобразовательной техники с разомкнутыми и замкнутыми системами управления в среде Matlab–Simulink / В.Я. Фролов, В.В. Смородинов. – СПб.: Лань, 2023. – 332 с.

5. Ищук А.А. Схемотехническое моделирование в среде Multisim: учеб. пособие для вузов / А.А. Ищук, И.А. Оболонин. – СПб.: Лань, 2024. – 124 с.

6. МАРС – среда моделирования технических устройств и систем / В.М. Дмитриев, А.В. Шутенков, Т.Н. Зайченко, Т.В. Ганджа. – Томск: В-Спектр, 2011. – 278 с.

7. Дмитриев В.М. Система визуализации и управления вычислительным экспериментом в среде многоуровневого моделирования МАРС / В.М. Дмитриев, Т.В. Ганджа, Т. Ю. Коротина // Доклады ТУСУР. – 2010. – № 1(21), ч. 2. – С. 149–155.

---

**Зайченко Татьяна Николаевна**
Д-р техн. наук, проф. каф. компьютерных систем
в управлении и проектировании (КСУП) ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-39-15
Эл. почта: ztn@ie.tusur.ru

**Дмитриев Вячеслав Михайлович**
Д-р техн. наук, проф. каф. КСУП ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-39-15
Эл. почта: dmitriewvm@gmail.com

**Ганджа Тарас Викторович**
Д-р техн. наук, проф. каф. КСУП ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-39-15
Эл. почта: gandgatv@gmail.com

Zaichenko T.N., Dmitriev V.M., Gandzha T.V.

**Organization of an educational computer experiment in multi-level modeling system MARS**

The methodology for organizing an educational computer experiment in MARS multi-level modeling system is considered using the example of a circuit from the field of electronics. An algorithm for the teacher's actions when creating computer laboratory work is presented.

**Keywords:** computer experiment, multilevel model, component, MARS system.
**DOI:** 10.21293/1818-0442-2023-26-4-84-88

*References*

1. Korikov A.M. [Experiment in scientific research]. *Proceedings of TUSUR University*, 2015, no. 2(36), pp. 148–156 (in Russ.).

2. Gorodovich A.V., Isakova O.Yu., Krechetov I.A., Kruchinin V.V., Morozova Yu.V., Romanenko V.V., Cherkashina I.P. [Evolution of technical and didactic solutions for e-learning technologies in TUSUR] *Proceedings of TUSUR University*, 2017. Vol. 20, no. 3, pp. 62–69 (in Russ.).

3. German-Galkin S.G. *Virtual'nye laboratorii poluprovodnikovyh sistem v srede Matlab-Simulink: uchebno-metodicheskoe posobie* [Virtual laboratories of semiconductor systems in Matlab-Simulink environment: educational and methodological manual]. Saint-Petersburg, Lan Publishing, 2022, 448 p. (in Russ.).

4. Frolov V.Ya. Smorodinov V.V. *Ustrojstva silovoj elektroniki i preobrazovatel'noj tekhniki s razomknutymi i zamknu-tymi sistemami upravleniya v srede Matlab–Simulink* [Power electronics and converter technology devices with open-loop and closed-loop control systems in Matlab – Simulink environment]. Saint-Petersburg, Lan Publishing, 2023, 332 p. (in Russ.).

5. Ishchuk A.A. Obolonin I.A. *Skhemotekhnicheskoe modelirovanie v srede Multisim: Uchebnoe posobie dlya vuzov* [Circuit modeling in Multisim environment: A textbook for universities]. Saint-Petersburg, Lan Publishing, 2024, 124 p. (in Russ.).

6. Dmitriev V.M., Shutenkov A.V., Zaichenko T.N., Gandzha T.V. *MARS – sreda modelirovaniya tekhnicheskikh ustroystv i sistem* [MARS – environment for modeling technical devices and systems]. Tomsk, V-Spectr, 2011, 278 p. (in Russ.).

7. Dmitriev V.M., Gandsha T.V., Korotina T.Y. [System of imaging and control architecture environment multilevel modeling]. *Proceedings of TUSUR University*, 2010, no. 1(21), pt. 2. – pp. 149–155 (in Russ.).

---

**Tatyana N. Zaichenko**
Doctor of Science in Engineering,
Department of Computer Control and Design Systems,
Tomsk State University of Control Systems
and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 41-39-15
Email: ztn@ie.tusur.ru

**Vjacheslav M. Dmitriev**
Doctor of Science in Engineering, Professor, Department of Computer Control and Design Systems, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 41-39-15
Email: dmitriewvm@gmail.com

**Taras V. Gandzha**
Doctor of Science in Engineering, Department of Computer Control and Design Systems, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 41-39-15
Email: gandgatv@gmail.com

УДК 001.891.573, 535-4

**А.А. Швачко, В.В. Матюшкин**

# Эффект Фарадея в знакопеременном магнитном поле: математическая модель

Одной из ключевых проблем сложных конструктивно и протяженных электронных приборов, к которым относится и лампа бегущей волны, является сложность сборки с обязательным условием совпадения геометрических осей всех элементов. Процесс неминуемой настройки совпадения осей называют юстировкой. Идеальной юстировки прибора очень сложно достичь из-за множества воздействующих факторов, следовательно, возникает необходимость создания автоматизированных комплексов моделирования юстировки электронного потока в системе формирования магнитного поля в фокусирующих системах. Решение задач юстировки можно осуществить с помощью магнитооптических методов, так как известно, что при воздействии магнитного поля свет проявляет ряд схожих свойств при воздействии на него магнитных полей. Целью работы является создание математической модели, позволяющей смоделировать изменение плоскости поляризации света при прохождении (движении магнитооптического датчика) вдоль оси магнитной системы.

**Ключевые слова:** юстировка магнитных систем, эффект Фарадея, магнитооптические среды, постоянный магнит, магнитная система, математическая модель, фокусирующая система, световой пучок.
**DOI:** 10.21293/1818-0442-2023-26-4-89-94

Одной из ключевых проблем сложных конструктивно и протяженных электронных приборов, к которым относится и лампа бегущей волны, является сложность сборки с обязательным условием совпадения геометрических осей всех элементов. Совпадение всех осей: оси магнитной фокусирующей системы, центральной оси пролетного канала, а также электронного потока – важно для обеспечения работы прибора на требуемых мощностях, а также для долговечности в целом. При несовпадении осей возможно оседание электронов с границы электронного пучка на элементах замедляющей системы, что приводит, к примеру, к раннему выходу из строя всего дорогостоящего прибора. Несовпадение осей при сборке может возникать из-за низкого качества поступающих на производство материалов (например, несовпадение сорта меди) и из-за различных отклонений в технологическом процессе при изготовлении тех или иных элементов. Обеспечение высокого качества изготовления элементов зачастую осложнено штучным или мелкосерийным характером производства. Процесс неминуемой настройки совпадения осей называют юстировкой [1–4].

Из-за невозможности изначального изготовления идеального с этой точки зрения прибора и сложности процесса (и невозможности вывести единый алгоритм) традиционно происходит поиск все новых методик, а также осуществляются попытки моделирования процесса юстировки с целью детального объяснения всех протекающих процессов.

В данном случае предлагается сосредоточиться на юстировке магнитной системы и электронного пучка. Важность данной компоненты можно объяснить на примере опыта с соленоидом. В соленоиде в отличие от постоянных магнитов поперечная компонента наиболее стабильна. В данном опыте в соленоид помещался датчик Холла для фиксации поперечной компоненты магнитного поля. Датчик помещался в соленоид на небольшом расстоянии он центра соленоида. Результат измерения приведен на рис. 1. Приведенная характеристика показывает, как даже минимальное отклонение положения датчика Холла от центральной оси способно спровоцировать неравномерность поперечной компоненты магнитного поля, что свидетельствует о несовпадении с центральной осью магнитного поля.

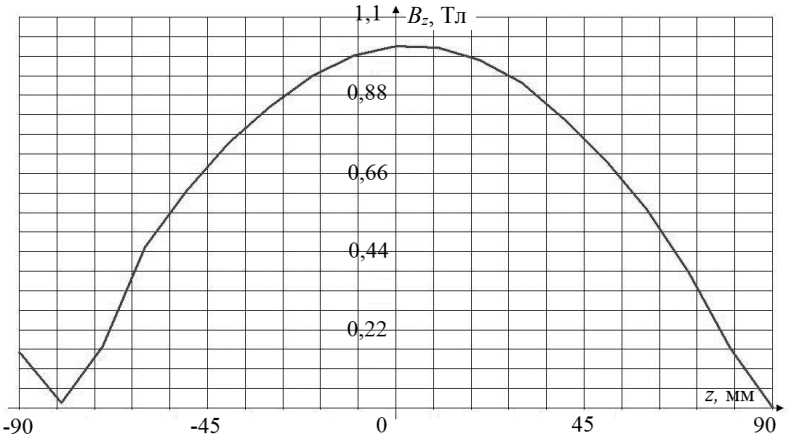



Рис. 1. Изменение поперечной составляющей магнитного поля при вращении датчика (угол γ)

Схема магнитной периодической фокусирующей системы (МПФС) и графики возможного несовпадения механической, магнитной осей и электронного потока приведены на рис. 2, 3.

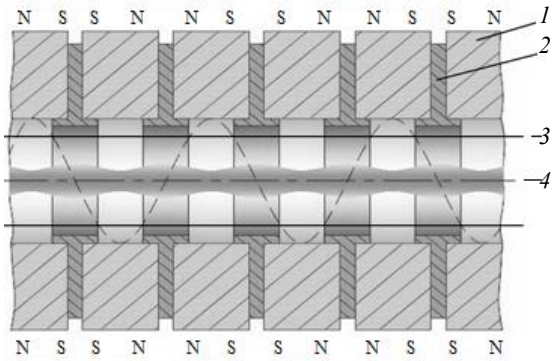



Рис. 2. Схема МПФС и электронного потока (ЭП):
*1* – постоянные магниты, *2* – полюсные наконечники, *3* – поверхность колбы лампы, *4* – ось электронного пучка

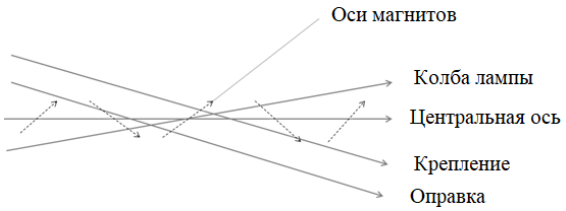



Рис. 3. Схема осей для юстировки в МПФС

Решение задач юстировки можно осуществить с помощью магнитооптических методов, так как известно, что при воздействии магнитного поля свет проявляет ряд схожих свойств (реакция) при воздействии на него магнитных полей. А так как создание светового пучка с помощью лазера осуществляется при заметно более простых условиях, нежели электронного пучка, то данный факт говорит о перспективности практического применения разрабатываемых методов.

Цель работы – создание математической модели, позволяющей смоделировать и оценить характеристики процесса прохождения светового пучка через знакопеременную магнитную систему на основе магнитооптического датчика.

**Математическая модель**

В качестве метода для моделирования процесса юстировки и возможности в перспективе использовать при настройке магнитной системы был выбран магнитооптический эффект Фарадея. Данный эффект основан на повороте плоскости поляризации светового пучка в магнитооптической среде при воздействии магнитного поля [5, 6]. Данный факт позволяет поставить ставит знак равенства между световым и электронным пучком. Использование светового пучка вместо электронного позволит осуществлять юстировку элементов системы без окончательной сборки прибора, что впоследствии должно снизить затраты на изготовление прибора как в денежном выражении, так и в плане затрачиваемого времени в случае отбраковки.

Сложность при анализе систем таким методом заключается в отсутствии экспертной системы, позволяющей оценить сопоставление полученного угла поворота плоскости поляризации с величиной магнитного поля на оси магнитных систем со сложной конфигурацией полей (например, МПФС). Также необходимо как минимум определить поведение угла поляризации по мере как прохождения знакопеременных магнитных полей в области отдельных магнитов, так и влияние на общую фокусирующую способность магнитной системы.

Одной из главных проблем при разработке метода анализа магнитных фокусирующих систем магнитооптическими методами является малое количество информации, учитывающей вращение плоскости поляризации светового луча при прохождении сложных знакопеременных магнитных полей и как следствие экспертной системы на основе таких данных по установлению конечной годности магнитных систем.

Для этого необходимо на первом этапе осуществить математическое моделирование процесса прохождения светового луча через магнитную систему. Данная математическая модель должна позволять оценивать поворот плоскости поляризации в ту или иную сторону при прохождении зон изменения знака магнитного поля.

Угол поворота плоскости поляризации оценивается с помощью следующего выражения [7–10]:

$$U_{\text{фарад}} = \upsilon B_z l, \qquad (1)$$

где $v$ – постоянная Верде, $B_z$ – магнитное поле на оси $z$, $l$ – длина оптического пути.

Индукция магнитного поля вдоль оси симметрии отдельного кольцевого магнита оценивается следующим образом [11]:

$$B_z(z) = \frac{\mu_0 M}{2}\left[\frac{2z+L}{\sqrt{D^2+(2z+L)^2}} - \frac{2z-L}{\sqrt{D^2+(2z-L)^2}} - \frac{2z+L}{\sqrt{d^2+(2z+L)^2}} + \frac{2z-L}{\sqrt{d^2+(2z-L)^2}}\right], \qquad (2)$$

где $\mu_0$ – магнитная постоянная, $M$ – намагниченность магнита, $L$ – толщина кольцевого магнита, $D$ и $d$ – внешний и внутренний диаметры, $z$ – координата на оси $z$.

Существующие математические модели магнитного поля постоянных магнитов не позволяют оценить влияние каждого отдельного магнита на величину получающегося магнитного поля в фокусирующей системе [12–15]. Сложные магнитные системы можно смоделировать на основе принципа суперпозиции, когда векторы магнитных полей отдельных магнитов будут математически складываться в вектор магнитного поля магнитной системы. Тогда чтобы учитывать координату и смещение каждого отдельного магнита, осуществим в выражение (2) подстановку $z = z - l(n - 1)$, где $l$ – длина оптического пути, $n$ – порядковый номер магнита. Данная подстановка необходима, чтобы осуществить смещение постоянного магнита вдоль оси на величину пройденного уже оптического пути. В результате выражение (2) примет вид

$$B_n(z)=\frac{\mu_0 M}{2}\left[\frac{2(z-l(n-1))+L}{\sqrt{D^2+(2(z-l(n-1))+L)^2}}-\frac{2(z-l(n-1))-L}{\sqrt{D^2+(2(z-l(n-1))-L)^2}}-\right.$$
$$\left.-\frac{2(z-l(n-1))+L}{\sqrt{d^2+(2(z-l(n-1))+L)^2}}+\frac{2(z-l(n-1))-L}{\sqrt{d^2+(2(z-l(n-1))-L)^2}}\right], \quad (3)$$

где $n$ – порядковый номер магнита в системе, $l$ – расстояние между магнитами.

Итоговое магнитное поле магнитной системы формируется на основе принципа суперпозиции и математически его можно представить, как сумму магнитных полей отдельных магнитов:

$$B_{\text{сист}}=\sum B_n\ . \quad (4)$$

Длинна оптического пути $l$ преобразуется в половину толщины магнита $L$, т.е. ($L$/2). Данная добавка ($L$/2) необходима по следующим причинам: на момент достижения центра кольцевого магнита в координате z световой луч уже пройдет как минимум половину толщины магнита, и этот пройденный путь необходимо учитывать в итоговой модели, а также чтобы убрать двойственность значения переменной $l$ в рамках всей математической модели.

В итоге после подстановки в (1) выражения (4), а также осуществив замену $l$ = $L$/2, выражение для оценки угла поворота поляризации во время прохождения магнитной системы примет сокращенный вид:

$$U_{\text{фарад}}=\upsilon(L/2)\sum B_n. \quad (5)$$

**Результаты**

В рамках моделирования были выбраны следующие параметры: $L$ = 10 мм, $d$ = 10 мм, $D$ = 20 мм, расстояние $l$ между магнитами = 15 мм, постоянная Верде для длины волны 633 нм $v$ = 4 рад / (Т м) для $SiO_2$, намагниченность магнитов задавалась в произвольном диапазоне, но в качестве точки отсчета были взяты параметры для магнитного сплава КС37А [ГОСТ 21559–76].

На рис. 4 приведены графики изменения амплитуды магнитного поля на оси постоянного кольцевого магнита (сверху) и изменения величины угла поворота плоскости поляризации (снизу) в привязке к координатам на оси (ось $x$).

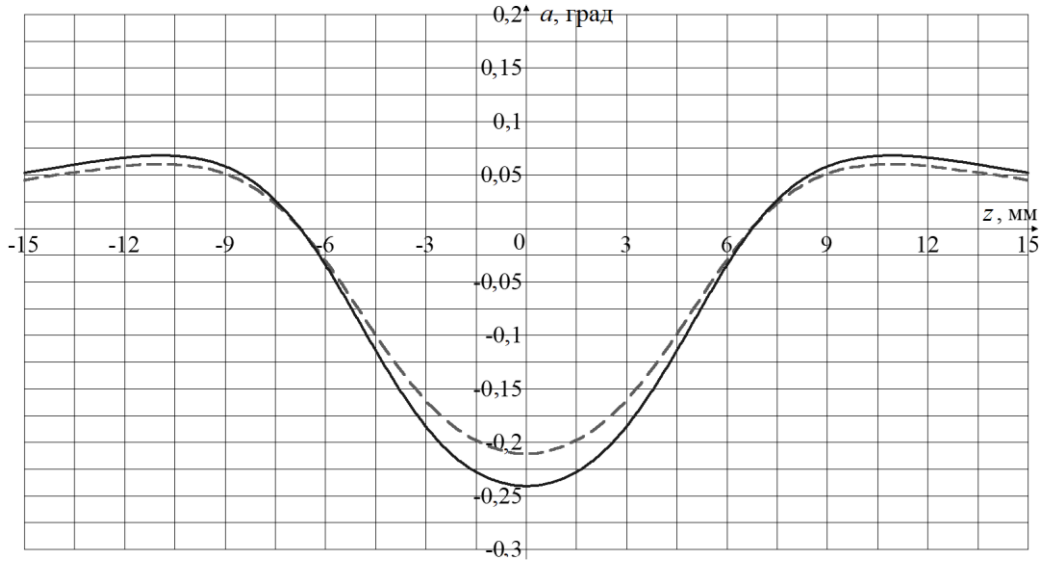



Рис. 4. График изменения величины магнитного поля (пунктирная линия) и угла плоскости поляризации вдоль центральной оси одного постоянного магнита (сплошная линия)

Данный рисунок иллюстрирует принцип работы указанной математической модели. Данная модель должна позволить смоделировать изменение плоскости поляризации света при прохождении (движении магнитооптического датчика) вдоль оси магнитной системы.

На рис. 4 проиллюстрирован случай для одного магнита. В рамках данного численного эксперимента воображаемый магнитооптический датчик двигался вдоль оси постоянного магнита, значения его магнитного поля вдоль оси проиллюстрированы на рис. 4 (слева). Соответствующее изменение величины поворота угла поляризации проиллюстрированы на рис. 4 (справа). За координату $z$ = 0 мм принят геометрический центр магнита, в котором фиксируется максимум магнитного поля. Из графика видно, что плоскость поляризации реагирует на изменение магнитного поля пропорционально изменению величины магнитного поля на оси магнита. Величина отклика на величину магнитного поля прямо пропорциональна величине постоянной Верде. Данный факт доказывает соответствие математической модели теоретическим положениям.

Также был осуществлен численный эксперимент для системы из 5 магнитов, проиллюстрированный на рис. 5.

Графики повторяют движения друг друга, изменение величины магнитного поля отражается изменением величины угла поворота плоскости поляризации. Графики на рис. 5 в целом отражают ожидаемую тенденцию отражения знакопеременного магнитного поля в соответствующем изменении знака угла поворота поляризации.

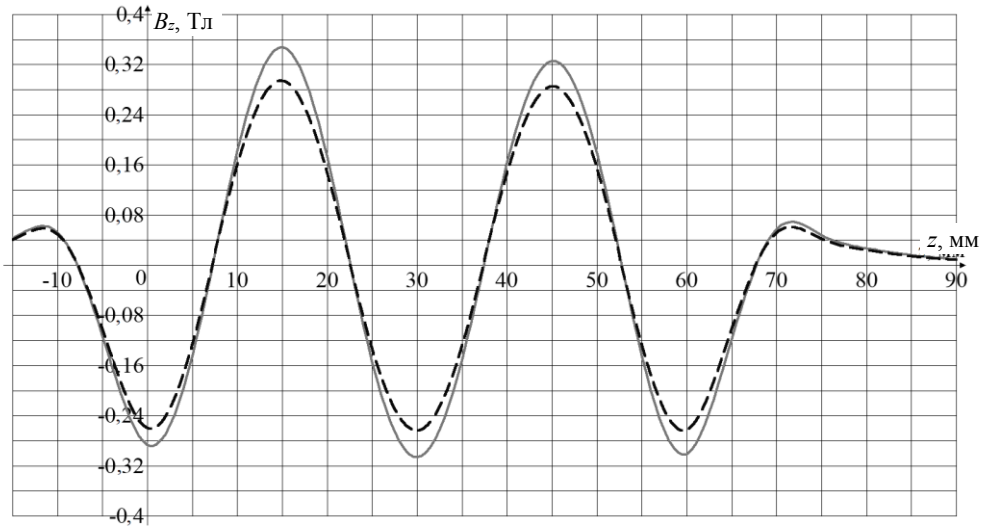



Рис. 5. График изменения величины магнитного поля (пунктирная линия) и угла плоскости поляризации вдоль центральной оси магнитной системы (сплошная линия), состоящей из пяти постоянных магнитов

**Заключение**

Приведено обоснование возможности использования для юстировки электронных приборов систем на основе магнитооптического эффекта Фарадея. Получена математическая модель, позволяющая смоделировать изменение плоскости поляризации света при прохождении (движении магнитооптического датчика) вдоль оси магнитной системы. Данные, полученные с помощью численного эксперимента, не противоречат теоретическим постулатам магнитооптической теории эффекта Фарадея. Использование данной модели позволит исследовать влияние изменения различных параметров магнитной системы на соответствующий отклик магнитооптического датчика. Данные, полученные таким образом, позволят в дальнейшем разработать эффективную установку по юстировке электронных приборов на основе магнитооптических эффектов.

Данные моделирования могут стать основой для калибровки (установления соответствия между углом поворота и величиной магнитного поля) установки. Также данная модель позволит подобрать наиболее эффективные для использования с магнитными полями сложной конфигурации материалы с необходимой по величине отклика постоянной Верде.

*Литература*

1. Васичев Б.Н. Конструирование электронно-оптических систем микросистемной электронно-лучевой техники / Б.Н. Васичев, Г.И. Фатьянова // Поверхность. Рентгеновские, синхротронные и нейтронные исследования. – 2006. – № 9. – С. 26–31.

2. Швачко А.А. К моделированию юстировки электронного потока в магнитных фокусирующих системах / А.А. Швачко, А.А. Захаров // Математические методы в технике и технологиях (ММТТ). – 2013. – № 10–2. – С. 53–55.

3. Кожухова А.А. Разработка методики настройки и юстировки магнитных систем на основе плоских магнитов для многолучевых клистронов миллиметрового диапазона / А.А. Кожухова, Д.А. Терентьев // Фундаментальные проблемы радиоэлектронного приборостроения. – 2014. – Т. 14, № 4. – С. 131–134.

4. Емельянов Е.А. Изменение структуры магнитного поля МПФС ЛБВ посредством внешнего корректирующего воздействия / Е.А. Емельянов, А.А. Захаров // Инженерный вестник Дона. – 2014. – № 3 (30). – С. 78.

5. Савельев И.В. Курс общей физики: учеб. пособие для студентов высших учебных заведений, обучающихся по техническим направлениям и специальностям. – В 4-х томах. – М.: КноРус, 2012. – 570 с.

6. Трофимова Т.И. Курс физики. – М.: ИЦ «Академия». – 2014, 560 с.

7. Дейнека И.Г. Изучение магнитооптического эффекта Фарадея / И.Г. Дейнека, О.А. Шрамко, С.А. Тараканов // Научно-технический вестник информационных технологий, механики и оптики. – 2008. – № 49. – С. 84–89.

8. Цуканов Б.Д. Магнитное вращение плоскости поляризации в прозрачных средах // Современные проблемы физико-математических наук. – 2020. – С. 570–576.

9. Паранин В.Д. Математическое моделирование однокаскадного магнитооптического датчика на основе продольного эффекта Фарадея / В.Д. Паранин, Л.И. Синицын // Актуальные проблемы радиоэлектроники и телекоммуникаций: матер. Всерос. науч.-техн. конф., г. Самара, 16–18 мая 2017 г. / Самар. нац. исслед. ун-т им. С.П. Королева. – Самара: ООО «Офорт», 2017. – С. 164–167.

10. Маврицкий О.Б. Эффект Фарадея в магнитных плѐнках. Лабораторный практикум по физике конденсированного состояния: учеб. пособие. – М.: НИЯУ МИФИ, 2012. – 72 с.

11. Царев В.А. Магнитные фокусирующие системы электровакуумных микроволновых приборов О-типа: учеб.

пособие / В.А. Царев, Р.В. Спиридонов. – Саратов: Новый ветер, 2010. – 352 с.

12. Горбатенко Н.И. Комбинированная математическая модель магнитного поля для автоматизированной селективной сборки электромагнитов / Н.И. Горбатенко, В.В. Гречихин, Н.М. Кыонг // Изв. высш. учеб. завед. Электромеханика. – 2010. – № 5. – С. 43–47.

13. Наракидзе Н.Д. Определение структуры математической модели распределения магнитного поля / Н.Д. Наракидзе, М.В. Ланкин // Изв. высш. учеб. завед. Северо-Кавказский региона. Технические науки. – 2007. – № S1. – С. 92–94.

14. Применение негармонического распределения магнитного поля для фокусировки интенсивных электронных потоков в магнитных периодических фокусирующих системах / А.В. Архипов, А.Н. Дармаев, Д.А. Комаров, Ю.А. Мирошников, С.П. Морев, А.В. Фетисова // Радиотехника и электроника. – 2008. – Т. 53, № 5. – С. 606–612.

15. Лапшин Э.В. Магнитостатический расчёт систем с постоянными магнитами // Труды междунар. симпозиума «Надежность и качество». – 2012. – Т. 2. – С. 257–258.

---

**Швачко Александр Алексеевич**
Канд. техн. наук, доцент каф. электронных приборов и устройств (ЭПУ) Саратовского технического ун-та им. Ю.А. Гагарина (СГТУ им. Ю.А. Гагарина)
Политехническая ул., 77, г. Саратов, Россия, 410054
ORCID: 0000-0001-6633-0975
Тел.: +7-937-972-51-56
Эл. почта: alexandr1899@gmail.com

**Матюшкин Владислав Владимирович**
Аспирант каф. ЭПУ СГТУ им. Ю.А. Гагарина
Политехническая ул., 77, г. Саратов, Россия, 410054
Тел.: +7-986-999-88-70
Эл. почта: vladisla7@mail.ru

Shvachko A.A., Matyushkin V.V.

**Faraday effect in an alternating magnetic field: a mathematical model**

When creating magnetic focusing systems, for example, for traveling wave lamps, there are known problems associated with the need to adjust the electron flow moving in a given direction along the axis of the device, that is, to align its axis with the magnetic axis of the focusing system. The ideal adjustment of the device is very difficult to achieve due to many influencing factors, therefore, it becomes necessary to create automated complexes for simulating the alignment of the electron beam in the magnetic field formation system for focusing systems. The alignment problems can be solved using magneto-optical methods, since it is known that when exposed to a magnetic field, the light exhibits a number of similar properties (reaction). The aim of the work is to create a mathematical model for the passage of a light beam through an alternating magnetic system based on the Faraday effect. As a result, a mathematical model has been obtained, that should allow modeling the change in the plane of light polarization during the passage (movement of the magneto-optical sensor) along the axis of the magnetic system. The simulation of the passage of light according to the Faraday effect through a magnetic system of one and five magnets is considered.

**Keywords:** adjustment of magnetic systems, Faraday effect, magneto-optical media, permanent magnet, magnetic system, mathematical model, focusing system, light beam.
**DOI:** 10.21293/1818-0442-2023-26-4-89-94

*References*

1. Vasichev B.N., Fatyanova G.I. *Konstruirovanie jelektronno-opticheskih sistem mikrosistemnoj jelektronno-luchevoj tehniki* [Design of electron-optical systems of microsystem electron beam technology]. *Journal of Surface Investigation: X-ray, Synchrotron and Neutron Techniques*, 2006, no. 9, pp. 26–31 (in Russ.).

2. Shvachko A.A., Zakharov A.A. *K modelirovaniju justirovki jelektronnogo potoka v magnitnyh fokusirujushhih sistemah* [Towards modeling the adjustment of the electron flow in magnetic focusing systems]. *Mathematical Methods in Engineering and Technology* – MMTT, 2013, no. 10–2, pp. 53–55 (in Russ.).

3. Kozhukhova A.A., Terentyev D.A. *Razrabotka metodiki nastrojki i justirovki magnitnyh sistem na osnove ploskih magnitov dlja mnogoluchevyh klistronov millimetrovogo diapazona* [Development of a technique for tuning and adjusting magnetic systems based on flat magnets for multibeam klystrons in the millimeter range]. *Fundamental Problems of Radio-Electronic Instrument Making*, 2014, vol. 14, no. 4, pp, 131–134 (in Russ.).

4. Emelyanov E.A., Zakharov A.A. *Izmenenie struktury magnitnogo polja MPFS LBV posredstvom vneshnego korrektirujushhego vozdejstvija* [Changing the structure of the magnetic field of the MPFS TWT through external corrective action]. *Engineering Bulletin of the Don*, 2014, no. 3(30), pp. 78 (in Russ.).

5. Savelyev, I.V. *Kurs obshhej fiziki: uchebnoe posobie dlja studentov vysshih uchebnyh zavedenij, obuchajushhihsja po tehnicheskim napravlenijam i special'nostjam* [General physics course: a textbook for students of higher educational institutions studying in technical areas and specialties]. Moscow: KnoRus, 2012, 570 p. (in Russ.).

6. Trofimova T.I. Kurs fiziki [Physics course]. Moscow: Publishing Center “Academy”, 2014, 560 p. (in Russ.).

7. Deineka I.G., Shramko O.A., Tarakanov S.A. *Izuchenie magnitoopticheskogo jeffekta Faradeja* [Study of the magneto-optical Faraday Effect]. *Scientific and Technical Bulletin of information Technologies, Mechanics and Optics*, 2008, no 49. pp. 84–89 (in Russ.).

8. Tsukanov B.D. *Magnitnoe vrashhenie ploskosti poljarizacii v prozrachnyh sredah* [Magnetic rotation of the plane of polarization in transparent media], *Modern Problems of Physical and Mathematical Sciences,* 2020, pp. 570–576 (in Russ.).

9. Paranin V.D., Sinitsyn L.I. [Mathematical modeling of a single-stage magneto-optical sensor based on the longitudinal Faraday Effect]. *Aktual'nye problemy radiojelektroniki i telekommunikacij: materialy vserosssiskoy nauchno-technicheskoy konferencii.* [Current problems of radio electronics and telecommunications: materials of All-Russian scientific-technical conference]. Samara, Samara National Research University named after S.P. Korolev, 2017, pp. 164–167 (in Russ.).

10. Mavritsky O.B. Jeffekt *Faradeja v magnitnyh plènkah. Laboratornyĭ praktikum po fizike kondensirovannogo sostojanija: Uchebnoe posobie* [Faraday Effect in magnetic films. Laboratory workshop on condensed matter physics: Textbook]. M.: National Research Nuclear University, 2012, 72 p. (in Russ.).

11. Tsarev V.A., Spiridonov R.V. *Magnitnye fokusirujushhie sistemy jelektrovakuumnyh mikrovolnovyh priborov O-tipa: uchebnoe posobie* [Magnetic focusing systems of O-type electrovacuum microwave devices: textbook]. Saratov: publishing house «New Wind», 2010, 352 p. (in Russ.).

12. Gorbatenko N.I., Grechikhin V.V., Cuong N.M. *Kombinirovannaja matematicheskaja model' magnitnogo polja dlja avtomatizirovannoj selektivnoj sborki jelektromagnitov* [Combined mathematical model of the magnetic field for automated selective assembly of electromagnets]. *News of Higher Educational Institutions. Electromechanics*, 2010, no. 5, pp. 43–47 (in Russ.).

13. Narakidze N.D., Lankin M.V. *Opredelenie struktury matematicheskoj modeli raspredelenija magnitnogo polja* [Determination of the structure of a mathematical model of magnetic field distribution]. *News of Higher Educational Institutions. North Caucasus Region. Technical Science*, 2007, no. S1, pp. 92–94 (in Russ.).

14. Arkhipov A.V., Darmaev A.N., Komarov D.A., Miroshnikob Y.A., Morev S.P., Fetisova A.V., *Primenenie negarmonicheskogo raspredelenija magnitnogo polja dlja fokusirovki intensivnyh jelektronnyh potokov v magnitnyh periodicheskih fokusirujushhih sistema* [Application of non-harmonic magnetic field distribution for focusing intense electron flows in magnetic periodic focusing systems]. *Radio engineering and Electronics*, 2008, vol. 53, no. 5, pp. 606–612 (in Russ.).

15. Lapshin E.V. [Magnetostatic calculation of systems with permanent magnets]. *Trudy mezhdunarodnogo sim-poziuma Nadezhnost' i kachestvo'*[Proceedings of the international symposium «Reliability and quality»], 2012, vol. 2, pp. 257–258 (in Russ.).

**Alexander A. Shvachko**
Candidate of Sciences in Engineering,
Department of Electronic Instruments and Devices,
Yu.A. Gagarin State Technical University of Saratov
77, Politekhnicheskaya st., Saratov, Russia, 410054
ORCID: 0000-0001-6633-0975
Phone: +7-937-972-51-56
Email: alexandr1899@gmail.com

**Vladislav V. Matyushkin**
Postgraduate student,
Department of Electronic Instruments and Devices,
Yu.A. Gagarin State Technical University of Saratov
77, Politekhnicheskaya st. Saratov, Russia, 410054
Phone: +7-986-999-88-70
Email: vladisla7@mail.ru

УДК 620.179.152.1

**А.В. Пешков**

# Вычислительная диагностика трещин и отслоений с использованием томографического подхода при наличии эталона исследуемого объекта

Рассматривается развитие подхода для решения задач промышленной дефектоскопии, использующее информацию об эталоне исследуемого объекта. Предлагаемый алгоритм томографической реконструкции основан на использовании априорной информации об эталонном образце. В случае промышленной томографии мы имеем дело с типовым изделием, для которого заранее известна вся его структура, следовательно, целесообразно использовать эти данные в качестве априорной информации при решении обратной задачи томографической реконструкции. Приведены результаты численных экспериментов для упрощенной модели изделия. Предложенный алгоритм демонстрирует свою эффективность в ситуации, когда классический алгоритм уже не справляется. Сделаны выводы о перспективности использования данного подхода при диагностике дефектов типа отслоений и трещин в промышленных изделиях.

**Ключевые слова:** компьютерная томография, дефектоскопия, томография области интереса, эталонный образец, вычислительно-эвристический алгоритм.
**DOI:** 10.21293/1818-0442-2023-26-4-95-101

Вычислительная (компьютерная) томография (КТ) представляет собой пример научного направления, проникающего практически во все области науки и техники, в которых применяются или могут быть применены какие-либо виды излучений.

Среди областей использования КТ можно выделить следующие: медицинская диагностика, неразрушающая диагностика промышленных изделий, системы безопасности, реконструкция объектов в электронной микроскопии, задачи геофизики.

Томография биологических объектов и тканей является очень важной задачей, имеющей большое прикладное значение для современной медицины. С её помощью получают необходимую диагностическую информацию о заболеваниях и травматических повреждениях [1–4].

Системы компьютерной томографии (КТ) для анализа материалов и других промышленных приложений, например неразрушающих испытаний, принципиально отличаются от клинических сканеров. В этих системах объект вращается, в то время как система источник рентгеновского излучения − регистратор остается неподвижной. Следует отметить, что в промышленной компьютерной томографии, как правило, не существует ограничений на дозы поглощенной энергии рентгеновского излучения облучения, поэтому используются источники с большей интенсивностью излучения по сравнению с клиническими компьютерными томографами. В промышленной томографии требования к разрешающей способности систем и точности измерений отличаются от клинической томографии, поэтому и параметры сканирования могут существенно отличаться от клинической КТ [5, 6].

В промышленности часто необходимо получить реконструкцию с высоким разрешением не всего объекта, а его фрагмента или нескольких фрагментов. Прогресс в области алгоритмического и программного обеспечения привел к возможности решения этой задачи [7–9]. Объект вначале сканируется целиком с грубым разрешением, затем область, представляющая интерес, сканируется при большом увеличении и, соответственно, более высоком разрешении. При конечной обработке используется информация о реконструкции, полученная при сканировании с разных разрешений [10].

Данный подход, основанный на изучении интересующей области, представлен в работе [11]. Автор предлагает метод восстановления изображения области интереса по усеченным проекциям, основанный на применении цифровой рекурсивной фильтрации имеющихся данных. Предложенный подход позволяет уменьшить среднеквадратичную ошибку реконструкции по сравнению с алгоритмом Шеппа–Логана, однако целесообразность его применения зависит от радиуса интересующей области.

В работе [12] представлен метод реконструкции изображения сечения объекта, содержащего непрозрачное включение. Предложенный алгоритм решения задачи двумерной томографии на основе условия Кавальери позволяет оценить неизвестные проекционные данные в области тени. Использование данного алгоритма приводит к уменьшению среднеквадратичной ошибки реконструкции, однако требует большого количества ракурсов наблюдения.

Для случая, когда число проекций ограничено, существуют специальные алгоритмы малоракурсной компьютерной томографии. В работе [13] описаны пять алгоритмов реконструкции изображений по малому числу ракурсов. Данные алгоритмы показали свою эффективность при исследовании энерговыделения газодинамических объектов, однако они плохо адаптируются к задачам промышленной томографии.

Существуют также алгоритмы томографической реконструкции, основанные на попиксельном анализе томограмм. Например, в работе [14] предложен метод определения на томограмме области, соответствующей участкам объекта, заполненным однород-

ным веществом с заданной плотностью. Его суть заключается в том, что пиксели реконструированного изображения считаются принадлежащими рассматриваемой области, если их яркость лежит в определенном интервале, границы которого определяются из условия минимума взвешенной суммы вероятностей ошибок первого и второго рода. Эффективность данного алгоритма во многом зависит от выдвинутых предположений о статистическом распределении яркости пикселей томограммы.

Применение систем рентгеновской томографии ограничено в некоторых случаях в связи с малым уровнем сигналов на выходе детекторов. Для решения этой проблемы в работе [15] авторы предлагают математическую модель формирования высокоэнергетических цифровых радиографических изображений в условиях низких уровней цифровых сигналов. Данная модель показала эффективность применительно к контролю крупногабаритных объектов за счет цифрового суммирования изображений.

Среди отечественных исследователей также существуют проекты в области томографии с использованием «цифрового двойника». В работе [16] представлена блок-схема «цифрового двойника» рентгеновского 3D-микротомографа. В вычислительном блоке устройства предполагается использование следующих средств: искусственный интеллект, анализ больших данных, алгоритмы распознавания образов, цифровая экосистема. Проект предполагает масштабную и перспективную разработку, однако в настоящее время он находится только на стадии создания модели интеллектуального томографа.

Таким образом, существующие исследования направлены на повышение качества обработки полученных томографических изображений. Однако в настоящее время благодаря развитию технологий искусственного интеллекта возможно применение новых подходов, использующих вычислительно-эвристические методы. В данной работе далее будет представлен подход для промышленной томографии, использующий эвристический поиск на основе априорной информации об эталонном образце диагностируемого изделия.

**Постановка задачи**

Рассмотрим следующую ситуацию, когда исследуемый объект содержит дефекты с избирательной чувствительностью к зондирующему (в данном случае рентгеновскому) излучению, а именно трещины и отслоения. Такие дефекты отличаются узким поперечным сечением (раскрытием), имея при этом протяженное «простирание». Это создает условия, при которых часть лучей, пересекающих дефект существенно поперек (вкрест простирания), из-за ограниченных возможностей измерительной аппаратуры не «почувствуют» дефект, а тогда нарушается полнота проекционных данных, и классическая КТ неприменима. Конечно, лучи, тангенциально проходящие через дефект, будут информативными в отличие от уже отмеченных, назовем их нормальными.

Ставится задача, имея проекционные данные, включающие общую лучевую картину, диагностировать описанный выше дефект.

В условиях промышленной дефектоскопии в нашем распоряжении находится полная априорная информация об исследуемом объекте – это проектная документация, в соответствии с которой данное изделие выпускается. Таким образом, имеется возможность синтеза проекционной матрицы для эталонного образца (случаи, когда это невозможно, в данное исследование не включаются). Данное обстоятельство дает возможность построения решения поставленной задачи.

В данной работе в качестве «решателя» (базового метода) используется алгебраическая реконструкция, сводящая решение томографической задачи к решению системы линейных алгебраических уравнений (СЛАУ) с сильно разреженной матрицей, т.е. присутствует достаточно большое число нулевых элементов. Однако априорная информация об объекте исследования позволяет эту систему «дозаполнить» априори известными слагаемыми в уравнениях, что значительно облегчает процедуру решения и повышает устойчивость и достоверность интерпретации измерительных данных. Таким образом, используемый метод попадает в категорию «сильных», то есть примененная эвристика дает прогрессивный эффект. Такой подход определяет название разработанного алгоритма как «вычислительно-эвристический алгоритм». Сюда же следует отнести и способ отбора информативных (рабочих) лучей, который будет описан далее.

**Классический метод томографической реконструкции**

Рассмотрим описанные выше этапы на примере упрощенной модели. Пусть мы имеем изделие с круглым поперечным сечением единичного радиуса, внутри которого имеется трещина, представленная областью между двух парабол (рис. 1). Далее на рабочее пространство накладывается сетка, разбивая исследуемый объект на пиксели. В данном исследовании используется сетка 40×40 пикселей.

Томографическое исследование начинается с измерения проекционных данных, полученных с помощью сканирования изделия множеством лучей с разных точек. В данной работе используется веерная схема сканирования, которая поворачивается вокруг объекта исследования (рис. 2). Имеется возможность устанавливать количество лучей, исходящих из источника, и количество положений источника, т.е. угол поворота.

Набор измерений для одного положения источника называется проекцией. Располагая полученные проекции в виде соответствующих матричных строк, получим проекционную матрицу **A**, элементы которой представляют характеристику луча на основе плотности пройденного им материала:

$$\mathbf{A}=\begin{pmatrix} a_{11} & \cdots & a_{1M} \\ \vdots & \ddots & \vdots \\ a_{N1} & \cdots & a_{NM} \end{pmatrix}=\left\{a_{ij}\right\}, \qquad (1)$$

где $a_{ij}$ – значение на приемнике для $i$-го луча при $j$-м положении источника, $N$ – количество лучей в веере, $M$ – количество положений источника, $i \in 1\ldots N$, $j \in 1\ldots M$.

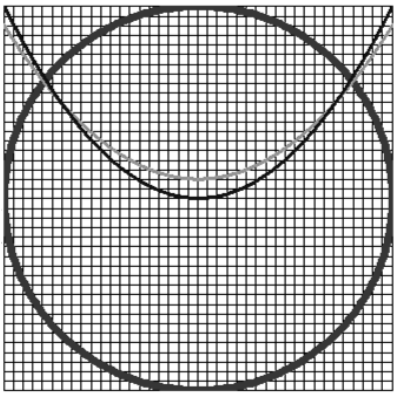
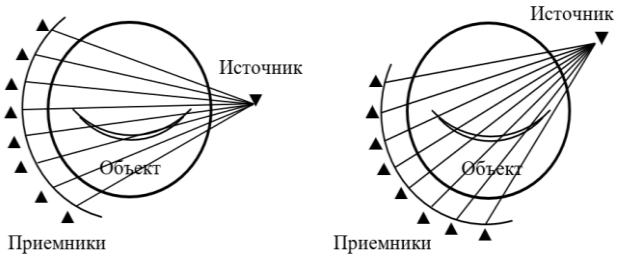


Рис. 1. Модель объекта с дефектом

Такая матрица может быть получена либо экспериментально путем пропуска через объект исследования рентгеновского излучения, соответственно, элементами проекционной матрицы будут значения интенсивности, полученные на приемнике, либо рассчитана синтетически для цифрового двойника объекта исследования.




*а* *б*

Рис. 2. Модель объекта с дефектом: *а* – начальное положение; *б* – положение после перемещения

Так как в данном исследовании речь идет о модельном эксперименте, то необходимо использовать синтетический алгоритм генерации проекционных данных. В качестве моделируемого значения интенсивности рентгеновского излучения на приемнике будет выступать следующая величина:

$$a = \sum_{i}^{H} l_i \cdot p_i \,, \qquad (2)$$

где $l_i$ – длина луча на $i$-м отрезке, $\rho_i$ – значение плотности материала на $i$-м отрезке, $H$ – количество отрезков луча со сменой плотности, $i \in 1\ldots H$.

Для удобства расчетов плотность внутри изделия принята равной единице, а вне изделия и внутри дефекта – равной нулю. Таким образом, смоделированное значение интенсивности сигнала будет уменьшаться при прохождении луча через дефект.

Так как нас интересуют только численные значения плотности материала в каждом пикселе, а не его функциональная зависимость от координат, то можно перейти от решения системы интегральных уравнений к решению СЛАУ. Таким образом, для решения задачи томографической реконструкции без использования априорной информации об эталонном образце используется следующий алгоритм:

1. Вычислить проекционную матрицу **A** для исследуемого объекта.

2. Преобразовать матрицу **A** в вектор **B**, который будет соответствовать правой части СЛАУ, где $B_i$ – смоделированное значение интенсивности сигнала $i$-го луча на приемнике.

3. Разбить рабочее пространство на $P$ пикселей с помощью наложения сетки.

4. Рассчитать матрицу коэффициентов СЛАУ **AA**, где $AA_{ij}$ – длина $i$-го луча в $j$-м пикселе ($i$ от 1 до $M \times N$, $j$ от 1 до $P$).

5. Задать вектор неизвестных СЛАУ **X**, где $X_j$ – значение плотности материала объекта в $j$-м пикселе.

6. Решить систему **AA** × **X** = **B** приближенным итерационным методом с заданными ограничениями на неизвестные ($0 \le X_j \le 1$).

7. Преобразовать вектор **X** в матрицу **XX** и построить ее графическое изображение (тепловую карту).

В качестве метрики достоверности будет использована средняя абсолютная ошибка MAE (Mean Absolute Error):

$$\mathrm{MAE} = \frac{1}{Pixels} \sum_{j=1}^{Pixels} \left| X_j - X\_\mathrm{real}_j \right| , \qquad (3)$$

где *Pixels* – количество пикселей рабочей области, $X_j$ – вычисленное алгоритмически значение плотности в $j$-м пикселе, $X\_\mathrm{real}_j$ – реальное (модельное) значение плотности в $j$-м пикселе. Так как $X_j$ может принимать значения только из диапазона 0…1, то метрику MAE в данном случае можно считать относительной оценкой, которая преобразуется в процентную ошибку при умножении на 100%.

Для нахождения $X\_\mathrm{real}$ необходимо рассчитать модельные значения плотностей пикселей (рис. 1). Расчет модельного (реального) значения плотности в пикселе производится следующим образом:

1. Пиксель равномерно заполняется $F$-точками.

2. Для каждой точки определяется ее статус: «в объекте», «в дефекте», «за пределами объекта» (рис. 3).

3. Количество точек со статусом «в объекте» делится на $F$ – общее число точек в пикселе.

4. Таким образом, получается нормированное значение плотности в диапазоне от 0 до 1.

Рассмотрим работу алгоритма на примере модели со следующими параметрами: число положений источника – 80, число лучей от одного источника – 80, размер сетки 40×40, в алгебраической реконструкции участвуют все 80·80 = 6 400 лучей. При этом ширина раскрытия дефекта изменяется с 0,2 (4 пикселя) до 0,05 (1 пиксель).

Результат работы алгоритма томографической реконструкции в виде тепловой карты представлен на рис. 4. Справа от изображений приведена шкала плотности пикселей. Выходные параметры работы алгоритма приведены в таблице.

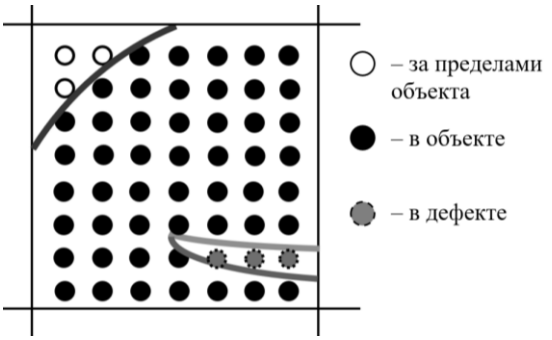



Рис. 3. Статусы точек в пикселе

Как видно из приведенных в таблице показателей для данной серии экспериментов, трудоемкость классического метода значительно велика. Также на изображениях восстановленных дефектов присутствуют некоторые артефакты, т.е. точечные пиксели вне дефекта, значения которых заметно отличаются от соседних. При ширине раскрытия дефекта менее 0,15 восстановленное изображение дефекта смазывается, а при 0,05 алгоритм не позволяет восстановить форму дефекта. Следовательно, достигнута граница применимости классического метода КТ для имеющегося набора измерений.

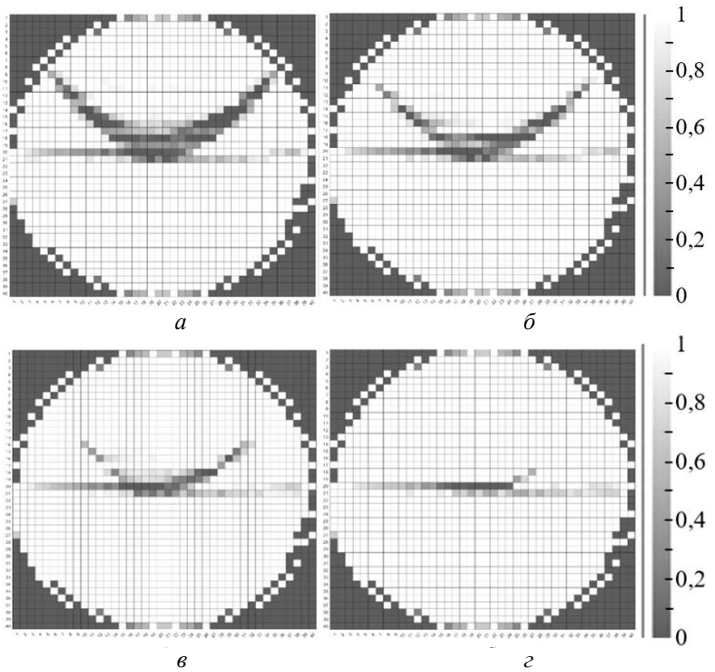



Рис. 4. Результат работы алгоритма без использования априорной информации для дефекта шириной:
*а* – четыре пикселя; *б* – три пикселя; *в* – два пикселя; *г* – один пиксель

**Результаты экспериментов**

| Ширина раскрытия дефекта *d*, доля от радиуса объекта | Кол-во лучей в веере *N* | Кол-во положений веера *M* | Кол-во используемых лучей *L* | Размер сетки *P* | Ошибка восстановления MAE | Время вычисления *t*, с |
|---|---|---|---|---|---|---|
| 0,20 | 80 | 80 | 6 400 | 40×40 | 0,0832 | 75 |
| 0,15 | 80 | 80 | 6 400 | 40×40 | 0,0813 | 75 |
| 0,10 | 80 | 80 | 6 400 | 40×40 | 0,0762 | 78 |
| 0,05 | 80 | 80 | 6 400 | 40×40 | 0,0676 | 76 |
| 0,05 | 80 | 80 | 250* | 40×40 | 0,0531 | 17 |
| 0,05 (3 шт.) | 80 | 80 | 350* | 50×50 | 0,0582 | 37 |

* Отобранные информативные лучи.

**Метод реконструкции с использованием априорной информации**

Для построения локальной томографической реконструкции в случаях, когда классические методы КТ неприменимы (например, из-за низкой чувствительности дефекта к зондирующему излучению), предлагается подход, основанный на эвристическом поиске, который использует априорную информацию об эталонном образце исследуемого изделия.

Эвристические алгоритмы широко используются для решения задач высокой вычислительной сложности, к которым относится компьютерная томография. В данном подходе эвристический поиск заключается в следующем: вместо алгебраической реконструкции на основе всех лучей, занимающей значительное время, используется гораздо более быстрый ограниченный поиск дефекта среди «перспективных» пикселей, отобранных с помощью информативных лучей. Тогда алгоритм томографической реконструкции будет выглядеть следующим образом:

1. Вычислить проекционную матрицу **A** для исследуемого объекта.

2. Вычислить проекционную матрицу **A*** для эталонного объекта без дефекта.

3. Получить рабочую матрицу **RR**, полученную вычитанием матриц из первых двух пунктов.

4. Преобразовать матрицу **RR** в трехмерный вектор **R**, где $R^1$ – значение разницы интенсивности для объекта и его эталона, $R^2$ – номер луча в пучке, $R^3$ – номер положения источника.

5. Отсортировать по убыванию вектор **R** по измерению $R^1$.

6. Построить графическое изображение вектора $\mathbf{R}^1$ и определить по графику точку резкого изменения крутизны, которая будет соответствовать количеству информативных лучей $L$ (рис. 5).

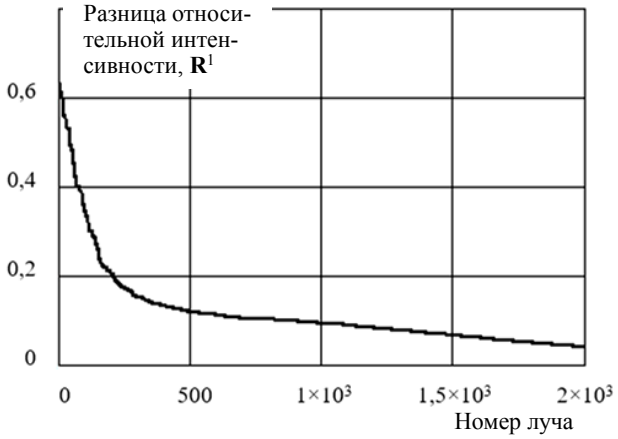



Рис. 5. Отсортированные по убыванию значения вектора **R**

7. На основании векторов $\mathbf{R}^1$ и $\mathbf{R}^2$ преобразовать матрицу **A** в вектор **B**, где $B_i$ – смоделированное значение интенсивности сигнала $i$-го луча на приемнике ($i$ от 1 до $L$).

8. Разбить рабочее пространство на $P$ пикселей с помощью наложения сетки.

9. Рассчитать матрицу коэффициентов СЛАУ **AA**, где $AA_{ij}$ – длина $i$-го луча в $j$-м пикселе ($i$ от 1 до $L$, $j$ от 1 до $P$).

10. Задать вектор неизвестных СЛАУ **X**, где $X_j$ – значение плотности материала объекта в $j$-м пикселе.

11. Вырезать из матрицы **AA** матрицу **Cut_MM**, состоящую из столбцов **AA**, сумма значений которых меньше порогового значения. Таким образом, получаем матрицу коэффициентов **MM**, из которой исключены пиксели, через которые не проходят (или проходят мало) отобранные $L$ лучей.

12. Вырезать из вектора **X** элементы, соответствующие пикселям, сумма значений которых в **AA** меньше порогового. Таким образом получаем вектор неизвестных **NN**, из которого исключены пиксели, через которые не проходят (или проходят мало) отобранные $L$ лучей.

13. Рассчитать вектор **BB**, соответствующий скорректированной правой части СЛАУ: **BB** = = **B** – **Cut_MM**×**E**, где **E** – единичный вектор, соответствующий количеству вырезанных столбцов из **AA**.

14. Решить систему **MM** × **NN** = **BB** приближенным итерационным методом с заданными ограничениями на неизвестные ($0 \le NN_j \le 1$).

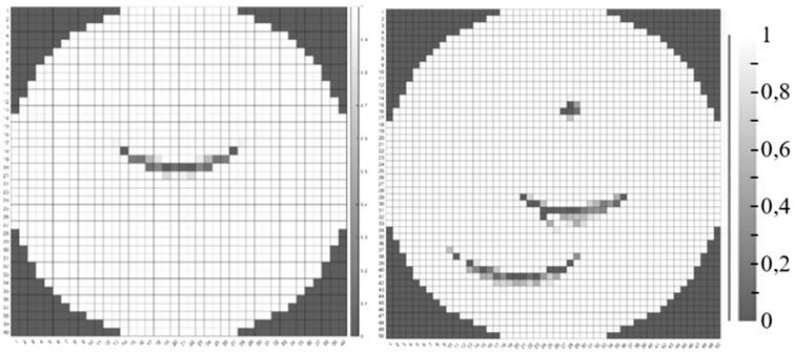
15. Преобразовать вектор **NN** в матрицу **XX** с учетом восстановления вырезанных единичных значений и построить ее графическое изображение (тепловую карту).

Рассмотрим работу модифицированного алгоритма на той же модели. Результат п. 6 описанного выше алгоритма представлен в виде графика на рис. 5. По приведенному графику определяется количество «рабочих» (информативных) лучей $L$ равное 250. В результате 11-го и 12-го пунктов алгоритма СЛАУ заметно упрощается, и из всей сетки 40×40 пикселей необходимо рассчитать значения только для 62.

Результат работы модифицированного алгоритма локальной томографической реконструкции представлен на рис. 6, *а*. Параметры сканирования такие же, как в предыдущем разделе, в алгебраической реконструкции участвуют 250 отобранных лучей, пороговое значение суммы длин лучей в пикселе – 1,5.

Далее предложенный алгоритм был применен на измененной модели: был добавлен еще один дефект такого же типа со смещением по оси абсцисс и один дефект в виде небольшого отверстия.

Параметры сканирования остались теми же, но размерность сетки была увеличена до 50×50, а для реконструкции использовались отобранные 350 информативных лучей. Результат работы модифицированного алгоритма томографической реконструкции для усложненной модели представлен на рис. 6, *б*.




*а* *б*

Рис. 6. Результат работы алгоритма с использованием априорной информации для:
*а* – дефекта шириной один пиксель; *б* – двух дефектов шириной одни пиксель и одного радиусом один пиксель

В таблице представлены численные результаты применения описанных выше алгоритмов.

Как видно из приведенных выше результатов, модифицированный алгоритм значительно лучше справился с локализацией дефекта. При этом временные затраты заметно сократились за счет отброса неинформативных лучей и упрощения СЛАУ путем дозаполнения значений известных пикселей, т.е. тех, в которых сумма длин лучей меньше порогового значения.

**Заключение**

В результате исследования была выполнена программная реализация модифицированного алгоритма локальной томографической реконструкции изделия с внутренним дефектом типа отслоения или трещины, имеющего избирательную чувствительность к зондирующему излучению, при системе наблюдений в виде окружности. Модификация заключается в использовании априорной информации об эталонном образце исследуемого объекта.

Также была проведена серия экспериментов по локализации дефекта при разной ширине его раскрытия. Представленные результаты работы алгоритма с использованием эвристической составляющей демонстрируют существенное уменьшение времени расчета и повышение точности реконструкции при том же разрешении, когда классический алгоритм не справляется.

Сказанное выше позволяет сделать вывод о перспективности предложенного подхода в области промышленной дефектоскопии и в общем о применимости рентгеновской вычислительной томографии для совершенствования производственных процессов.

Цифровая модель объекта испытаний позволяет встраивать ее в математические модели производственных процессов.

Возможные ограничения предложенного подхода включают необходимость точного расчета проекционной матрицы для эталонного образца. Эффективность предлагаемого алгоритма во многом зависит от выбранного количества информативных лучей, а также порогового значения для пикселей. Поэтому в дальнейшем необходимо разработать рекомендации по выбору этих параметров алгоритма.

Также необходимо провести серию экспериментов, используя обширное тестовое покрытие, для установления достоверности и границ применимости предложенного алгоритма.

В процессе дальнейших исследований планируется разработать адаптацию предложенного алгоритма для трехмерного случая, т.е. выполнить томографическое сканирование в конусе лучей.

Выражаю благодарность профессору Сергею Михайловичу Зеркалю за помощь в разработке предложенного подхода и пристальное внимание к процессу исследования. Работа выполнена при финансовой поддержке Новосибирского государственного технического университета.

*Литература*

1. Габуния Р.И. Компьютерная томография в клинической диагностике / Р.И. Габуния, Е.К. Колесникова. – М.: Медицина, 1995. – 352 с.

2. Хофер М. Компьютерная томография. Базовое руководство. – М.: Медицинская литература, 2006. – 208 с.

3. Блинов Н.Н. Методы компьютерной томографии в медицине // Здравоохранение и медицинская техника. – 2005. – Т. 17, № 3. – С. 10–11.

4. Kalender W.A. Computed tomography: fundamentals, system technology, image quality, applications. – John Wiley & Sons, 2011. – 372 p.

5. Kastner J. New X-ray computed tomography methods for research and industry // 7th Conference on Industrial Computed Tomography (iCT2017). – ICT, Leuven, Belgium. – 2017. – Vol. 22 (3). – URL: https://www.ndt.net/?id=20884 (дата обращения: 27.11.2023).

6. Goebbels J. Determining the spatial resolution in computed tomography – comparison of MTF and line-pair structures // International Symposium on Digital Industrial Radiology and Computed Tomography, Berlin, Germany. – 2011. – URL: https://www.ndt.net/?id=11138 (дата обращения: 27.11.2023).

7. Kastner J. X-ray computed tomography for the development of materials and components // Habilitation thesis, Vienna University of Technology, Vienna. – 2011. – URL: http://hdl.handle.net/20.500.12708/159002 (дата обращения: 27.11.2023).

8. ROI-Tomografie (Lokale Tomografie) / C. Maass, M. Knaup, S. Sawall, M. Kachelriess // e-Journal of Nondestructive Testing. – 2010. – Vol. 16(6). – URL: https://www.ndt.net/?id=10773 (дата обращения: 27.11.2023).

9. Computed Tomography of Large Components in Aerospace Industry / M. Luxa, T. Schön, S. Schröpfer, S. Oeckl, M. Eberhorn, T. Wenzel, J. Bouteyre // 4th International Symposium on NDT in Aerospace 2012, Augsburg, Germany. – 2013. – URL: https://www.ndt.net/?id=13822 (дата обращения: 27.11.2023).

10. Bateni S.H. Development of coordinate metrology with optical sensors, computed tomography and multisensor systems / S.H. Bateni, R. Christoph // TM-Technisches Messen. – 2019. – Vol. 86, No. 9. – P. 464–468.

11. Лихачев А.В. Исследование рекурсивной фильтрации проекционных данных в задаче томографии области интереса // Вычислительные технологии. – 2017. – Т. 22, № 1. – С. 25–36.

12. Лихачев А.В. Новый метод решения задачи томографии при наличии непрозрачного включения // Вычислительные методы и программирование. – 2017. – Т. 18, № 2. – С. 129–137.

13. Коновалов А.Б. Разработка алгоритмов реконструкции изображений для малоракурсной компьютерной томографии в РФЯЦ-ВНИИТФ: история, современное состояние и перспективы / А.Б. Коновалов, В.В. Власов, А.Н. Киселев // Дефектоскопия. – 2022. – № 6. – С. 37–47.

14. Лихачев А.В. Томографическая реконструкция области, имеющей заданное значение плотности // Вычислительные методы и программирование. – 2018. – Т. 19. – С. 516–521.

15. Жвырбля В.Ю. Повышение проникающей способности систем цифровой радиографии на основе анализа сигналов низкой интенсивности / В.Ю. Жвырбля, С.П. Осипов, Д.А. Седнев // Дефектоскопия. – 2022. – № 7. – С. 39–53.

16. Сырямкин В.И. Проектирование рентгеновского 3D-микротомографа на основе его «цифрового двойника» /

В.И. Сырямкин, С.А. Клестов, С.Б. Сунцов // Инноватика–2022: сборник матер. XVIII Междунар. школы-конф. студентов, аспирантов и молодых ученых, Томск, 21–22 апреля 2022 г. – Томск: ООО «СТТ», 2022. – С. 204–206.

---

**Пешков Александр Викторович**
Аспирант каф. вычислительной техники (ВТ)
Новосибирского государственного
технического университета (НГТУ)
К. Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0001-7517-5858
Тел.: +7-905-930-62-33
Эл. почта: mupeskov1997@mail.ru

Peshkov A.V.

**Computational diagnostics of cracks and delaminations using a tomographic approach and a sample of the object under study as a reference**

The development of an approach to solve problems of industrial flaw detection, using information about the standard state of the object under study, is considered. The proposed tomographic reconstruction algorithm is based on the use of a priori information about the reference sample. In the case of industrial tomography, we are dealing with a standard product which entire structure is known in advance; therefore, it is advisable to use this data as a priori information when solving the inverse problem of tomographic reconstruction. The results of numerical experiments for a simplified model of the product are presented. The proposed algorithm demonstrates its efficiency in situations where the classical algorithm can no longer cope. Conclusions are drawn about the prospects of using this approach in diagnosing defects such as delaminations and cracks in industrial products.

**Keywords:** computed tomography, flaw detection, region of interest tomography, reference sample, computational-heuristic algorithm.
**DOI:** 10.21293/1818-0442-2023-26-4-95-101

*References*

1. Gabuniya R.I., Kolesnikova E.K. *Komp'yuternaya tomografiya v klinicheskoj diagnostike* [Computed tomography in clinical diagnostics]. Moscow, Medicine Publ., 1995, 352 p. (in Russ.).

2. Hofer M. *Komp'yuternaya tomografiya. Bazovoe rukovodstvo* [Computed tomography. Basic guide]. Moscow, Medical literature Publ., 2006, 208 p. (in Russ.).

3. Blinov N.N. *Metody komp'yuternoj tomografii v medicine* [Computed tomography methods in medicine]. *Zdravoohranenie i medicinskaya tekhnika* [Healthcare and medical technology], 2005, vol. 3(17), pp. 10–11 (in Russ.).

4. Kalender W.A. *Computed tomography: fundamentals, system technology, image quality, applications*. John Wiley & Sons, 2011, 372 p.

5. Kastner J. New X-ray computed tomography methods for research and industry. *Proceedings of the 7th Conference on Industrial Computed Tomography (iCT2017)*. ICT, Leuven, Belgium, 2017, vol. 22(3). Available at: https://www.ndt.net/?id=20884, free (Accessed: November 27, 2023).

6. Goebbels J. Determining the spatial resolution in computed tomography – comparison of MTF and line-pair structures. *Proceedings of the International Symposium on Digital Industrial Radiology and Computed Tomography*. Berlin, Germany, 2011. Available at: https://www.ndt.net/?id=11138, free (Accessed: November 27, 2023).

7. Kastner J. X-ray computed tomography for the development of materials and components. Habilitation thesis, Vienna University of Technology, Vienna, 2011. Available at: http://hdl.handle.net/20.500.12708/159002, free (Accessed: November 27, 2023).

8. Maass C., Knaup M., Sawall S., Kachelriess M. ROI-Tomografie (Lokale Tomografie). *e-Journal of Nondestructive Testing*, 2010, Vol. 16(6). Available at: https://www.ndt.net/?id=10773, free. (Accessed: November 27, 2023).

9. Luxa M., Schön T., Schröpfer S., Oeckl S., Eberhorn M., Wenzel T., Bouteyre J. Computed Tomography of Large Components in Aerospace Industry. *Proceedings of the 4th International Symposium on NDT in Aerospace 2012*, Augsburg, Germany, 2013. Available at: https://www.ndt.net/?id=13822, free (Accessed: November 27, 2023).

10. Bateni S.H., Christoph R. *Development of coordinate metrology with optical sensors, computed tomography and multisensor systems*. TM-TECHNISCHES MESSEN, 2019, Vol. 86, no. 9, pp. 464–468.

11. Lihachev A.V. *Issledovanie rekursivnoj fil'tracii proekcionnyh dannyh v zadache tomografii oblasti interesa* [Study of recursive filtering of projection data in the problem of tomography of a region of interest]. *Vychislitel'nye tekhnologii* [Computing technologies], 2017, vol. 1(22), pp. 25–36 (in Russ.).

12. Lihachev A.V. *Novyj metod resheniya zadachi tomografii pri nalichii neprozrachnogo vklyucheniya* [A new method for solving the tomography problem in the presence of an opaque inclusion]. *Vychislitel'nye metody i programmirovanie* [Computational methods and programming], 2017, vol. 2(18), pp. 129–137 (in Russ.).

13. Konovalov A.B., Vlasov V.V., Kiselev A.N. *Razrabotka algoritmov rekonstrukcii izobrazhenij dlya malorakursnoj komp'yuternoj tomografii v RFYAC—VNIITF: istoriya, sovremennoe sostoyanie i perspektivy* [Development of image reconstruction algorithms for low-angle computed tomography in the RFFC—VNIITF: history, state of the art and prospects]. *Defektoskopiya* [Defectoscopy], 2022, vol. 6, pp. 37–47 (in Russ.).

14. Lihachev A.V. *Tomograficheskaya rekonstrukciya oblasti, imeyushchej zadannoe znachenie plotnosti* [Tomographic reconstruction of an area having a given density value]. *Vychislit-el'nye metody i programmirovanie* [Computational methods and programming], 2018, vol. 4(19), pp. 516–521 (in Russ.).

15. Zhvyrblya V.Y., Osipov S.P., Sednev D.A. *Povyshenie pronikayushchej sposobnosti sistem cifrovoj radiografii na osnove analiza signalov nizkoj intensivnosti* [Improving the penetration power of digital radiography systems based on low-intensity signal analysis]. *Defektoskopiya* [Defectoscopy], 2022, vol. 7, pp. 39–53 (in Russ.).

16. Syryamkin V.I., Klestov S.A., Suncov S.B. *Proektirovanie rentgenovskogo 3d mikrotomografa na osnove ego «cifrovogo dvojnika»* [Designing a 3D X-ray microtomograph based on its «digital twin»]. *Innovatika–2022: Sbornik materialov XVIII mezhdunarodnoj shkoly-konferencii studentov, aspirantov i molodyh uchenyh* [Innovation–2022. Procceedings of the XVIII International School-Conference of Students, Postgraduate Students and Young Scientists]. Tomsk, LLC «STT», 2022, pp. 20–23 (in Russ.).

---

**Alexander V. Peshkov**
Postgraduate student, Department of Computer Science,
Novosibirsk State Technical University
20, K. Marks pr., Novosibirsk, Russia, 630073
ORCID: 0000-0001-7517-5858
Phone: +7-905-930-62-33
Email: mupeskov1997@mail.ru

# ЭЛЕКТРОТЕХНИКА

УДК 631.37

**М.В. Паринов, А.В. Сергеев, Д.В. Васильченко**

# Схемотехнические решения помехоустойчивого регулятора оборотов бесщеточного электродвигателя беспилотного воздушного судна

Работа посвящена особенностям разработки схемотехнических решений помехоустойчивых регуляторов оборотов бесщеточных электродвигателей для беспилотных воздушных судов. В ней проанализированы особенности эксплуатации, на основании которых сформулированы технические требования для целого класса устройств. В процессе анализа состояния вопроса сделан вывод о высокой актуальности развития решения с полным программным управлением. Представлены основные принципы управления бесщеточным электродвигателем, рекомендуемые для построения регулятора. В качестве практического решения разработаны структурная и принципиальная схемы с описанием работы основных элементов. В заключении статьи рассмотрены практические результаты испытания данного регулятора. Даны их оценка на текущем этапе, пути улучшения и развития в ближайшей перспективе.

**Ключевые слова:** регулятор скорости вращения электродвигателя, бесщеточный электродвигатель, беспилотное воздушное судно, помехоустойчивые решения, программное управление, микроконтроллер.
**DOI:** 10.21293/1818-0442-2023-26-4-105-110

В настоящее время большинство беспилотных воздушных судов (БВС) используют электрическую силовую установку. Исключением являются крупные летательные аппараты. Однако и для них намечена тенденция перехода на электрическую тягу.

Подавляющее большинство электрических БВС оснащаются бесколлекторными трехфазными электродвигателями. Это объясняется их высоким КПД, долговечностью, надежностью и размерами, что недостижимо для коллекторных электромашин [1]. Однако рассматриваемые электродвигатели имеют некоторые недостатки. К основным из них относятся относительно высокая стоимость и необходимость использования сложной электронной системы управления.

Для управления трехфазными бесколлекторными электродвигателями (BLDC-моторами) используются типовые регуляторы скорости вращения. На практике для их обозначения используется аббревиатура ESC (Electric Speed Controller). Обычно ESC приобретаются в виде готовых электронных модулей.

В настоящее время на рынке РФ присутствует широкая номенклатура регуляторов, охватывающая все основные задачи беспилотной авиации. Однако все массовые изделия являются зарубежными, что часто приводит к проблемам при закупках и противоречит политике технологического суверенитета. Также при использовании готовых зарубежных модулей существенно снижаются возможности по расширению функциональности и внесению изменений в конструкцию.

**Постановка задачи и анализ методов ее решения**

Для формирования требований к разработке необходимо ограничить область применения БВС легкого типа с максимальной потребляемой мощностью каждого двигателя 1 кВт при питании от 6-ячеечной литиевой аккумуляторной батареи под управлением классического полетного контроллера (используется программное обеспечение на основе ArduPilot [2], INAV [3], BetaFlight [4], PX4 [5] и др.).

Разрабатываемое решение должно быть универсальным, позволяя создать широкое множество устройств, и отвечать следующим основным требованиям: совместимость с классическими полетными контроллерами; возможность создания версий с повышенной устойчивостью к электромагнитным помехам; наличие средств телеметрии, включая передачу значений суммарного потребляемого тока, напряжения на батарее, скорости вращения вала электродвигателя.

Известно несколько методик управления BLDC-моторами. В стандартном двигательном режиме могут использоваться системы управления с датчиками [6], а также без датчиков на основе вычисления обратной ЭДС [7, 8]. Для рассматриваемых задач подходит только второй вариант, так как двигатели БВС, соответствующие требованиям, не имеют датчиков положения вала.

Для реализации регулятора управления скоростью вращения BLDC-мотора без датчиков необходимо аппаратно-программное решение. Уровень программной автоматизации может существенно отличаться в зависимости от принятой методики реализации. Логика управления коммутацией силовыми ключами [9] может быть реализована аппаратно посредством специальных драйверов высокой степени интеграции или может быть выполнена программно, при этом аппаратная часть отвечает только за включение и выключение силовых ключей. Программное обеспечение обычно реализуется на микроконтроллере. Однако существуют альтернативные варианты. Например, в [10] представлен регулятор BLDC-мотора на программируемой логической интегральной схеме (ПЛИС).

Реализуемое решение должно обладать низкой стоимостью и возможностью крупносерийного про-

изводства. Поэтому с учетом особенностей управления для реализации программной части выбран микроконтроллер. Независимо от принятой методики построения регулятора на микроконтроллере необходимо реализовать программное обеспечение для обработки входных данных со стороны полетного контроллера, обеспечить передачу телеметрии и организовать взаимодействие с драйверами силовых ключей.

Для передачи команд от полетного контроллера регулятору ESC может использоваться широтно-импульсная модуляция (ШИМ) [11] или один из специализированных протоколов [12], большинство из которых являются цифровыми. Как показывают исследования [13], для создания помехозащищенных регуляторов скорости вращения первоочередной задачей является защита цепей передачи команд от электромагнитных помех, а также использование надежного протокола данных. Управление посредством ШИМ-сигнала не подходит для этих целей.

Аналоговая передача телеметрии подвержена помехам и не позволяет передать достаточное количество параметров для типовых полетных контроллеров, которые обычно имеют только аналоговый вход датчика суммарного тока. Проблема решается использованием цифровых протоколов. Например, KISS [14], который позволяет передавать до 8 параметров одновременно.

Таким образом, в создаваемом решении реализация цифровых протоколов управления и телеметрии необходима. Однако отказ от ШИМ- и аналоговых сигналов не рекомендован, чтобы обеспечить совместимость со старыми полетными контроллерами.

На основании выполненного анализа можно сделать вывод о необходимости решения двух крупных задач в процессе реализации ESC-регулятора: разработка прототипа схемотехнического решения и разработка алгоритмов и программ для микроконтроллера. В рамках данной работы будет реализована первая из них.

В основу разработки положены изложенные выше требования, теоретические основы BLDC-моторов и накопленный опыт родственных проектов.

**Разработка схемотехнического решения**

Авторами данной работы предложено решение, имеющее следующие отличительные черты: поддержка помехозащищенных протоколов управления и телеметрии, обеспечение корректной работы двигателей на высоких оборотах (до 120 000 мин$^{-1}$), простота, компактность, низкая стоимость. Требуемые протоколы перечислены в предыдущем разделе. Представленные в источниках [15–17] не удовлетворяют данным требованиям, а также ряду других пунктов технического задания.

На рис. 1 показана структурная схема ESC-регулятора БВС. Ее отличительной особенностью является отсутствие специализированного контроллера.

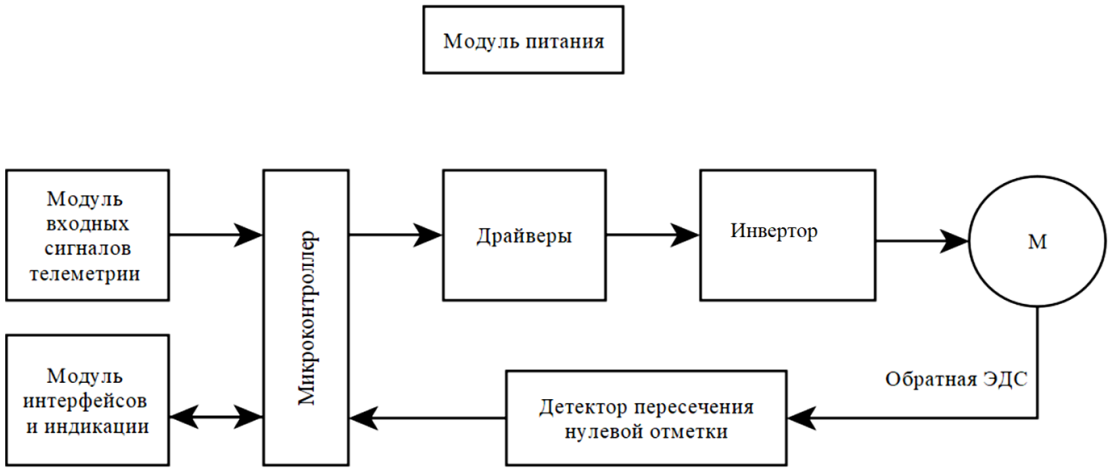



Рис. 1. Структурная схема регулятора на классическом микроконтроллере

Функция низкоуровневого управления электродвигателем (коммутации обмоток) в данном решении возложена на соответствующее программное обеспечение микроконтроллера. Его объем занимает основную часть программы, а потребление вычислительных ресурсов – 70–80% от общего объема.

Для управления силовыми ключами дополнительно применяется модуль драйверов. Для программного определения момента коммутации используется детектор перехода через нулевое значение обратной ЭДС.

На рис. 2 представлены сигналы при трапецеидальном управлении BLDC-мотором. Порядок коммутации представлен в нижней части рисунка. Из него следует, что средний потребляемый ток от батареи делится на три фазы, каждая из которых коммутируется двумя плечами полумоста. Таким образом, интегральный ток каждого транзистора равен 1/6 от паспортного потребляемого, а пиковый – 1/2.

Землей, которая показана на рисунке, является средняя точка обмоток электродвигателя. На большинстве моделей она не выведена. Поэтому для обратной связи используется искусственная средняя точка, которая в иностранной литературе именуется виртуальной землей (virtual ground). Для ее реализации используются три резистора равного сопротивле-

ния, включенные звездой. Сигнал со средней точки данной схемы используется для эмуляции средней точки обмоток электродвигателя.

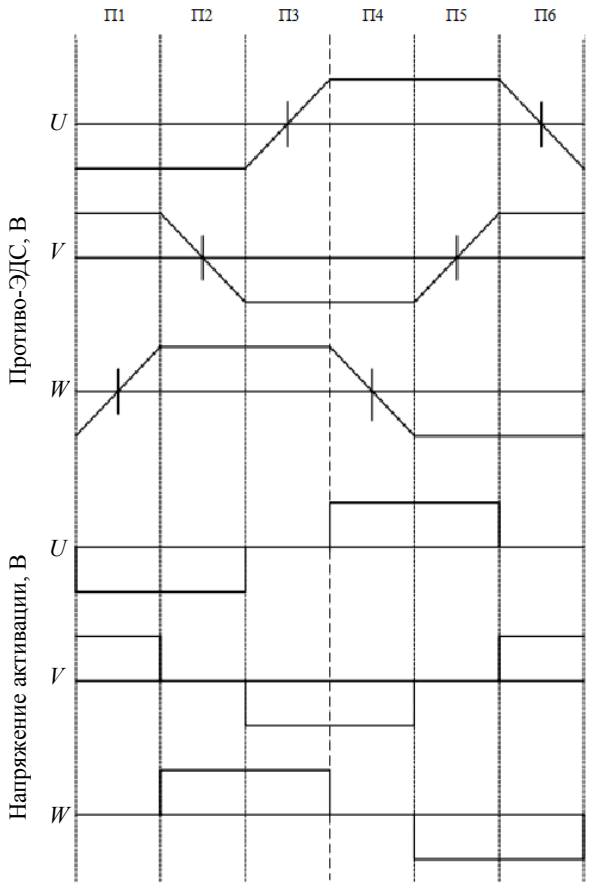



Рис. 2. Принцип управления

Для управления скоростью вращения реализуется изменение напряжения на фазах электродвигателя посредством ШИМ. Рекомендуемая кратность модуляции – не менее 5.

Крутизну фронтов напряжения на обмотках необходимо учитывать при расчете реальной мощности электродвигателя. При частотах коммутации более 50 кГц данный параметр оказывает существенное влияние на механические параметры устройства для большинства комбинаций двигатель – регулятор.

При выборе частоты ШИМ следует учитывать тепловую энергию включения / отключения и отвод мощности от кристалла с учетом температурного сопротивления всех элементов конструкции. Необходимо не только предотвратить температурное разрушение, но и обеспечить работу транзистора в температурном режиме, допускающем расчётные ток и напряжение.

На рис. 3 представлена принципиальная схема разработанного устройства. Для коммутации обмоток BLDC-мотора предлагается классическая трехфазная мостовая схема. Транзисторы VT1–VT6 – полевые с изолированным затвором. Максимальный ток исток-сток при нормальной работе возникает при максимальном напряжении на фазе; режим электродинамического торможения для БВС не предусмотрен.

D4 – микроконтроллер STM32F103C8T6. Помехоустойчивость управления устройством реализуется программно посредством реализации специализированных цифровых протоколов; данные передаются посредством линии MOT_IN. Также данная линия допускает управление посредством ШИМ-сигнала для совместимости с устаревшими полетными контроллерами. В этом случае для реверсирования вращения используется линия MOT_REV.

SWCLK и SWDIO – стандартный интерфейс для программирования микроконтроллера и отладки.

TEL_OUT – обеспечивает вывод помехоустойчивой цифровой телеметрии. В текущей версии она реализуется протоколом KISS [14]. Также для совместимости параметры работы передаются в виде аналоговых сигналов: CUR_OUT передают значение общего потребляемого тока. В нашем решении данный сигнал снимается с выхода цифроаналогового преобразователя (ЦАП) микроконтроллера. Это позволяет повысить помехоустойчивость посредством цифровой обработки сигналов, получаемых с измерительного усилителя.

Микроконтроллер получает данные о значении суммарного потребляемого тока через вход аналого-цифрового преобразователя (АЦП) CS, к которому подключен измерительный усилитель. Аналогично выполняется измерение напряжения батареи: линия VBAT+ подключена к делителю напряжения на резисторах R6, R7.

Для связи с каждым драйвером D5–D7 полевого транзистора используются 2 линии: выход ШИМ-сигнала заполнения импульсов включения фазы и цифровая линия команды блокировки двух ключей полумоста одновременно, которая используется для гарантированного предотвращения короткого замыкания и выхода из строя полевых транзисторов в случае рассинхронизации выполнения программных процедур. Драйверы полевых транзисторов используют бутстрепный конденсатор и диод.

При использовании управления BLDC-мотором без датчиков необходимо отслеживать обратную ЭДС по каждой фазе для реализации трапецеидального управления BLDC-мотором. Упрощенный вид сигналов управления показан на рис. 2. Точный момент коммутации задается обратной связью, указывающей позицию ротора. В текущей схеме реализуется метод определения нулевого значения обратной ЭДС, которая возникает на отключенной в текущий момент времени обмотке (оба транзистора полумоста закрыты).

Для этого используется узел на встроенном компараторе D8. На резисторах $R_{12}$–$R_{17}$ собраны три делителя напряжения для каждой из фаз. Сигналы с них передаются на неинвертирующие входы компараторов. Резисторы $R_9$–$R_{11}$ образуют виртуальную среднюю точку электродвигателя (виртуальную землю), которая подключается к инвертирующим входам компаратора. Выходы компаратора соединены с цифровыми входами микроконтроллера. По изменению их уровня определяется переход обратной ЭДС через нулевую точку.

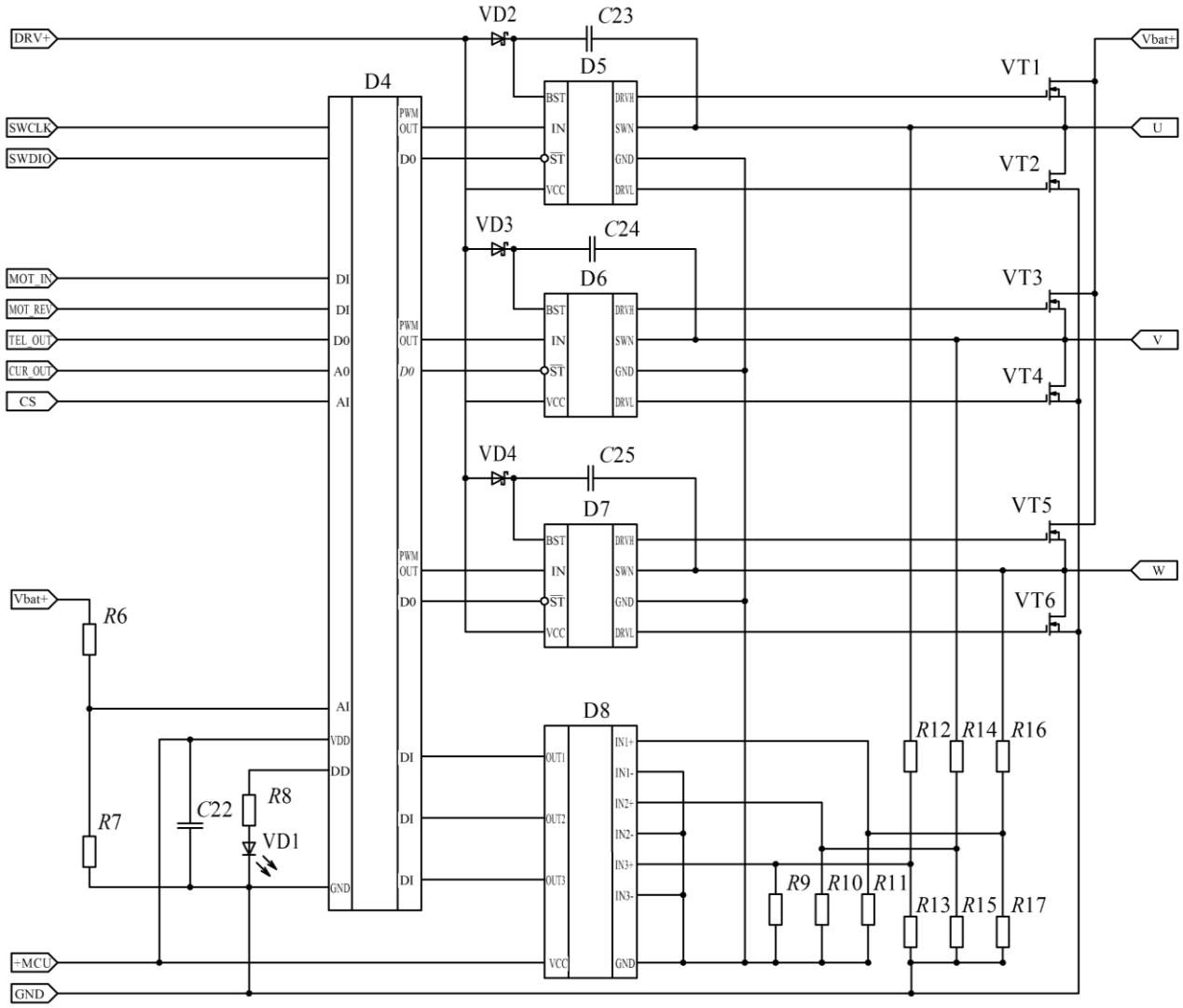



Рис. 3. Принципиальная схема регулятора с полным программным управлением

**Экспериментальное макетирование**

Регулятор, выполненный согласно рис. 3, был реализован в виде одноканального решения (для управления одним электродвигателем). В тестовом экземпляре использовались детали импортного производства. В качестве микроконтроллера применялся STM32F103C8T6, в качестве драйверов – ADP3120.

Для управления регулятором реализованы цифровые протоколы (Proshot, Dshot) и работа с ШИМ-сигналом. Управление выполнялось посредством полетного контроллера SpeedyBee F4 V3. На нем установлено программное обеспечение BetaFlight [4].

Целью эксперимента являлась проверка работоспособности изделия. Первая часть включает проверку возможности обеспечить вращение электродвигателя без его перегрева и нехарактерных вибраций. Вторая – исследование соответствия реальной скорости вращения заданному значению. Третья – порядок и своевременность коммутации обмоток.

Тестирование созданного ESC-регулятора выполнялось посредством серии тестов. В качестве нагрузки использовался BLDC-мотор T-Motor Velox V2 V2207 1750kv с установленным трехлопастным воздушным винтом диаметром 5 дюймов и шагом 4 дюйма. Питание осуществлялось от батареи 4S напряжением 16,8 В.

Измерение скорости оборотов выполнялось лазерным тахометром МЕГЕОН 18005. Сравнение измеренных результатов с заданными значениями показало разницу менее 5%.

При работе двигателя в циклах по 10 мин нагрев его корпуса не превысил 70 °С, а температура полупроводниковых компонентов регулятора ESC была менее 80 °С. Отсутствовали не характерные для испытуемого объекта вибрации, звуки.

Полученные осциллограммы с созданного регулятора показаны на рис. 4.

Сигнал, показанный в верхней части экрана, соответствует обратной ЭДС. Сигнал в нижней части экрана – напряжению на фазе электродвигателя. Сигнал в средней части – напряжению на средней точке двигателя. Сигнал в верхней части – выходу компаратора, соответствующему данной фазе. Осциллограмма показывает, что определение перехода через

нулевую отметку происходит своевременно: переключение высокого и низкого уровня выхода компаратора происходит строго между минимальным и максимальным уровнем сигнала на данной фазе. Форма сигналов и тайминги соответствуют выбранному трапецеидальному методу регулирования: измеренный сигнал напряжения на фазе приближен к теоретическому, показанному на рис. 2.

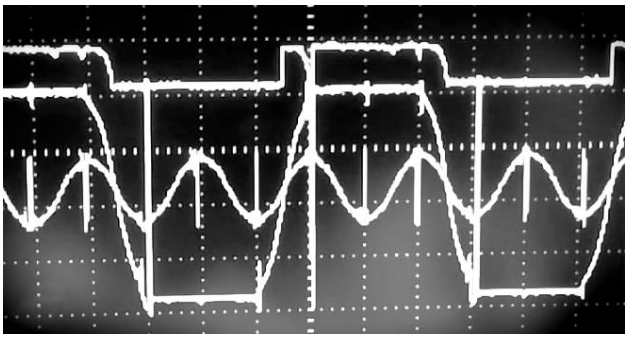


Рис. 4. Осциллограммы сигналов на входах микроконтроллера, фазах электродвигателя и земле компаратора относительно общей земли схемы

Это говорит о корректной работе изделия. Однако отмечены незначительные задержки коммутации обмоток.

**Заключение**

Было предложено схемотехническое решение ESC легких БВС, разработаны структурная и принципиальная схемы. Они отличаются от известных аналогов возможностью простого сопряжения с типовыми полетными контроллерами, наличием помехоустойчивых интерфейсов, возможностью работать в режимах, соответствующих легким БВС, включая скоростные аппараты мультироторного типа. Структурная схема является инвариантной и может быть использована для построения широкого модельного ряда устройств на отечественной и импортной элементной базе.

На основе решения с полным программным управлением создан прототип регулятора. По результатам его испытаний сделан вывод о качестве предложенного схемотехнического решения, что подтверждается работоспособностью созданного регулятора.

*Литература*

1. Уразбахтин Р.Р. Двигатели для беспилотных летательных аппаратов // Международный научно-исследовательский журнал. – 2017. – № 2. – С. 142–144.

2. Ardupilot [Электронный ресурс]. – Режим доступа: https://www.ardupilot.org (дата обращения: 13.10.2023).

3. INAV [Электронный ресурс]. – Режим доступа: https://github.com/iNavFlight/inav, свободный (дата обращения: 13.10.2023).

4. Betaflight [Электронный ресурс]. – Режим доступа: https://www.betaflight.com, свободный (дата обращения: 13.10.2023).

5. PX4 Autopilot [Электронный ресурс]. – Режим доступа: https://www.px4.io, свободный (дата обращения: 13.10.2023).

6. Никитин А.О. Магнитоэлектрическая система управления оборотами бесколлекторного электродвигателя для беспилотных летательных аппаратов / А.О. Никитин, А.Р. Петрова, Р.В. Петров // Вестник Новгородского государственного университета. – 2017. – № 7. – С. 26–31.

7. Бездатчиковый регулятор бесколлекторного двигателя постоянного тока с постоянными магнитами на роторе / В.Т. Пенкин, Д.В. Сухов, Д.А. Шевцов, Д.М. Шишов // Практическая силовая электроника. – 2014. – № 3 (55). – С. 46–51.

8. Intelligent Control of High-Speed Sensorless Brushless DC Motor for Intelligent Automobiles. / Jung-Sheng Wen, Chi-Hsu Wang, Ying-De Chang, Ching-Cheng Teng // IEEE/SMC. – 2008. – P. 3394–3398.

9. 6-шаговая коммутация BLDC-моторов [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/745372/, свободный (дата обращения: 13.10.2023).

10. Ильюшин С.А. Разработка блока управления электродвигателем типа BLDC на базе ПЛИС / С.А. Ильюшин, А.А. Шаронов, В.В. Киселев // Информационно-измерительные и управляющие системы. – 2015. – Т. 13, № 9. – С. 51–55.

11. Использование бесколлекторных двигателей в качестве исполнительных приводов с высокой точностью позиционирования / О.О. Соломин, С.В. Рослов, С.В. Козелетов, М.С. Храмихин // Наука и военная безопасность. – 2020. – № 1 (20). – С. 27–33.

12. Чипизубов А.М. Методы связи ESC-регуляторов оборотов современных потребительских дронов гражданского назначения / А.М. Чипизубов, В.В. Солецкий, Р.В. Шибеко // Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований: матер. V Всерос. национальной науч. конф. молодых учёных. – Комсомольск-на-Амуре: Комсомольский-на-Амуре гос. ун-т, 2022. – Т. 1, № 1. – С. 334–336.

13. Исследование влияния импульсных помех на работу бесколлекторного двигателя [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/stc_spb/articles/755814/ (дата обращения: 13.10.2023).

14. KISS ESC 32-bit series onewire telemetry protocol [Электронный ресурс]. – Режим доступа: https://www.rcgroups.com/forums/showatt.php?attachmentid=8524039&d=1450424877 (дата обращения: 13.10.2023).

15. VESC – Open Source ESC [Электронный ресурс]. – Режим доступа: https://vedder.se/2015/01/vesc-open-source-esc/, свободный (дата обращения: 01.12.2023).

16. BlueESC [Электронный ресурс]. – Режим доступа: https://github.com/bluerobotics/BlueESC, свободный (дата обращения: 01.12.2023).

17. MY OPEN SOURCE ESC [Электронный ресурс]. – Режим доступа: https://electronoobs.com/eng_arduino_tut91.php, свободный (дата обращения: 01.12.2023).

**Паринов Максим Викторович**
Канд. техн. наук, доцент каф. компьютерных интеллектуальных технологий проектирования
Воронежского государственного технического ун-та
20-летия Октября ул., 84, г. Воронеж, Россия, 34006
Тел.:+7 (473-2) 43-77-29
Эл. почта: parmax@mail.ru

**Сергеев Александр Викторович**
Канд. физмат. наук, нач. управления науки и инновации,
Воронежского государственного технического ун-та
20-летия Октября ул., 84, г. Воронеж, Россия, 34006
Тел.:+7 (473-2) 43-77-29
Эл. почта: parmax@mail.ru

**Васильченко Дмитрий Владимирович**
Аспирант каф. конструирования и проектирования радиоаппаратуры Воронежского государственного технического ун-та
20-летия Октября ул., 84, г. Воронеж, Россия, 34006
Тел.:+7 (473-2) 43-77-29
Эл. почта: shadow951@bk.ru

Parinov M.V., Sergeev A.V., Vasilchenko D.V.

**Circuit solutions for an interference-resistant electronic speed controller of a brushless electric motor for an unmanned aircraft**

The article is devoted to the features of the circuit solutions development for noise-resistant electronic speed controllers of brushless electric motors for unmanned aircraft. It analyzes the operating features, that allowed to formulate the technical requirements for a whole class of devices. When analyzing the state-of-the-art, it was concluded that the development of a solution with full program control is highly relevant. The basic principles for controlling a brushless electric motor, recommended for constructing a regulator, are presented. As a practical solution, a structural and circuit diagram has been developed describing the operation of the main elements. In the conclusion, the practical results of testing this regulator are considered. The assessment at the current stage is provided, as well as the ways to improve and develop the regulator in the near future.

**Keywords:** electronic speed controller, BLDC motor, unmanned aircraft, interference-resistant solutions, software control, microcontroller.
**DOI:** 10.21293/1818-0442-2023-26-4-105-110

*References*

1. Urazbahtin R.R. *Mezhdunarodnyj nauchno-issledovatel'skij zhurnal*, [Engines for unmanned aerial vehicles]. 2017, no 2, pp. 142–144 (in Russ.).

2. Ardupilot. Available at: https://www.ardupilot.org, free (Accessed: October 13, 2023).

3. INAV. Available at: https://github.com/iNavFlight/inav, free. (Accessed: October 13, 2023).

4. Betaflight. Available at: https://www.betaflight.com, free (Accessed: October 13, 2023).

5. PX4 Autopilot. Available at: https://www.px4.io, free (Accessed: October 13, 2023).

6. Nikitin A.O., Petrova A.R., Petrov R.V. [Magnetoelectric ]. *Vestnik Novgorodskogo Gosudarstvennogo Universiteta*, 2017, no. 7, pp. 26–31 (in Russ.).

7. Penkin V.T., Suhov D.V., SHevcov D.A., SHishov D.M. [Sensorless controller of BLDC motor with permanent magnets]. *Prakticheskaya Silovaya Elektronika*, 2014, no. 3 (55), pp. 46–51 (in Russ.).

8. Jung-Sheng Wen, Chi-Hsu Wang, Ying-De Chang, Ching-Cheng Teng. Intelligent Control of High-Speed Sensorless Brushless DC Motor for Intelligent Automobiles. *IEEE/SMC,* 2008, pp. 3394–3398.

9. 6-shagovaya kommutaciya BLDC motorov. Available at: https://habr.com/ru/articles/745372/, free (Accessed: October 13, 2023).

10. Il'yushin, S. A., Sharonov A. A., Kiselev V. V. [Development of the control unit of the BLDC motor on the base of the programmable logic device]. *Informacionno-izmeritel'nye i upravlyayushchie sistemy*, 2015, no. 9, T. 13, pp. 51–55 (in Russ.).

11. Solomin O.O., Roslov S.V., Kozeletov S.V., Hramihin M.S. [Use of brushless motors as actuators with high positioning accuracy]. *Nauka i voennaya bezopasnost'*, 2020, no. 1(20), pp. 27–33 (in Russ.).

12. Chipizubov A.M., Soleckij V.V., Shibeko R.V. *Metody svyazi ESC-regulyatorov oborotov sovremennyh potrebitel'skih dronov grazhdanskogo naznacheniya* [Methods of ESC RPM Regulators Communication in Modern Civil Consumer Drones]. *Molodezh' i nauka: aktual'nye problemy fundamental'nyh i prikladnyh issledovanij: Materialy P'atoi Vserossijskoj nacional'noj nauchnoj konferencii molodyh uchyonyh* [Youth and Science: Current Issues in Fundamental and Applied Research: Proceedings of the Fifth All-Russian National Scientific Conference of Young Scientists]. *Komsomol'sk-na-Amure, Komsomol'skij-na-Amure Gosudarstvennyj Universitet*, 2022, pp. 334–336 (in Russ.).

13. Issledovanie vliyaniya impul'snyh pomekh na rabotu beskollektornogo dvigatelya. Available at: https://habr.com/ru/companies/stc_spb/articles/755814/, free (Accessed: October 13, 2023).

14. KISS ESC 32-bit series onewire telemetry protocol. Available at: https://www.rcgroups.com/forums/showatt.php?attachmentid=8524039&d=1450424877, free (Accessed: October 13, 2023).

15. VESC – Open Source ESC. Available at: https://vedder.se/2015/01/vesc-open-source-esc/, free (Accessed: December 1, 2023).

16. BlueESC. Available at: https://github.com/bluerobotics/BlueESC, free (Accessed: December 1, 2023).

17. MY OPEN SOURCE ESC. Available at: https://electronoobs.com/eng_arduino_tut91.php, free (Accessed: December 1, 2023).

---

**Maksim V. Parinov**
Candidate of Sciences in Engineering, Associate Professor
Department of Intelligent Computer Technologies for Design Voronezh State Technical University
84, 20-letiya Oktyabrya st., Voronezh, Russia, 394006
Phone: +7(473-2) 43-77-29
Email: parmax@mail.ru

**Aleksander V. Sergeev**
Candidate of Sciences in Physics and Mathematics,
Head of the Research and Innovation Administration,
Voronezh State Technical University
84, 20-letiya Oktyabrya st., Voronezh, Russia, 394006
Phone: +7(473-2) 43-77-29
Email: asergeev@cchgeu.ru

**Dmitriy V. Vasilchenko**
Postgraduate student, Department of Design and Engineering of Radio Equipment, Voronezh State Technical University
84, 20-letiya Oktyabrya st., Voronezh, Russia, 394006
Phone: +7(473-2) 43-77-29
Email: shadow951@bk.ru

# 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; $\sin x(t_1)$; $U_{\text{in}}$; $I_{\text{вх}}$; $T_z$; $\beta_2$; $H_2O$, 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

9 771818 044708 02007