



Том 9. № 1
2023

ISSN: 1813-324X (print)
ISSN: 2712-8830 (online)

ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ

Темы номера:

- ✓ Оценка помехоустойчивости сигналов квадратурной модуляции
- ✓ Математическая модель кластерной V2X системы
- ✓ Исследование параметров Хёрста потоков данных облачных систем

Vol. 9. Iss. 1
2023

PROCEEDINGS
OF TELECOMMUNICATION UNIVERSITIES

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича» (СПбГУТ)

Научный журнал

**ТРУДЫ
УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ**

Том 9. № 1

Proceedings of Telecommunication Universities

Vol. 9. Iss. 1

Санкт-Петербург

2023

Описание журнала

Научный журнал. Включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (распоряжение Минобрнауки России № 21-р от 12.02.2019), по специальностям (распоряжение № 33-р от 01.02.2022):

1.2.2. Математическое моделирование, численные методы и комплексы программ

2.2.6. Оптические и оптико-электронные приборы и комплексы

2.2.13. Радиотехника, в том числе системы и устройства телевидения

2.2.14. Антенны, СВЧ-устройства и их технологии

2.2.15. Системы, сети и устройства телекоммуникаций

2.2.16. Радиолокация и радионавигация

2.3.1. Системный анализ, управление и обработка информации

2.3.6. Методы и системы защиты информации, информационная безопасность

Выпускается с 1960 года. Выходит 6 раз в год. Издается на русском и английском языках.

Редакционный совет

Киричек Р.В. <i>Главный редактор</i>	д.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия
Владыко А.Г. <i>Зам. Главного редактора</i>	к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия
Буйневич М.В. <i>Шеф-редактор</i>	д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия
Розанов Н.Н.	д.ф.-м.н., проф., чл.-корр. РАН, АО «Государственный оптический институт им. С.И. Вавилова» (ГОИ), г. Санкт-Петербург, Россия
Дукельский К.В.	д.т.н., доцент, АО «Государственный оптический институт им. С.И. Вавилова» (ГОИ), г. Санкт-Петербург, Россия
Кучерявый Е.	PhD, Технологический университет Тампере, г. Тампере, Финляндия
Гошек И.	PhD, Технологический университет Брно, г. Брно, Чешская республика
Тиамийу О.А.	PhD, Университет Илорина, г. Илорин, Нигерия
Козин И.Д.	д.ф.-м.н., проф., Алматинский университет энергетики и связи, г. Алма-Аты, Казахстан
Самуйлов К.Е.	д.т.н., проф., Российский университет дружбы народов (РУДН), г. Москва, Россия
Степанов С.Н.	д.т.н., проф., Московский технический университет связи и информатики (МТУСИ), г. Москва, Россия
Росляков А.В.	д.т.н., проф., Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), г. Самара, Россия
Кучерявый А.Е.	д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия
Канаев А.К.	д.т.н., проф., Петербургский университет путей сообщения имени Александра I (ПГУПС), г. Санкт-Петербург, Россия
Новиков С.Н.	д.т.н., проф., Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ), г. Новосибирск, Россия
Дворников С.В.	д.т.н., проф., Военная академия связи им. Маршала Советского Союза С.М. Буденного (ВАС), г. Санкт-Петербург, Россия
Коржик В.И.	д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия
Ковалгин Ю.А.	д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Регистрационная информация

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций: ПИ № 77-77501 от 17.01.2020 г. (пред. рег. № 77-17986 от 07.04.2004 г.)

Подписной индекс в объединенном каталоге «ПРЕССА РОССИИ»: 59983

Размещение в РИНЦ (elibrary.ru) по договору: № 59-02/2013R от 20.02.2013

Контактная информация

Учредитель и издатель: Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)

Адрес: 191186, Санкт-Петербург, набережная реки Мойки, д. 61, литера А

Адрес: 193232, Санкт-Петербург,
редакции: пр. Большевиков, 22/1, к. 334/2
Тел.: +7 (812) 326-31-63, м. т. 2022, +79643759970
E-mail: tuzs@sut.ru
Web: <http://tuzs.sut.ru>
ВК: <http://vk.com/spbtuzs>

Description

Scientific journal. The journal is included in the List of reviewed scientific publications, in which the main scientific results of dissertations for the degree of candidate of science and for the degree of doctor of science should be published (order of the Ministry of Education and Science of Russia No 21-r of 12 February 2019) in the field of (order of the Ministry of Education and Science of Russia No 33-r of 01 February 2022):

1.2.2. Mathematical modeling, numerical methods and complexes of programs

2.2.6. Optical and optoelectronic devices and complexes

2.2.13. Radio engineering, including television systems and devices

2.2.14. Antennas, microwave devices and its technologies

2.2.15. Systems, networks and telecommunication devices

2.2.16. Radiolocation and radio navigation

2.3.1. System analysis, management and information processing

2.3.6. Methods and systems of information security, cybersecurity

Since 1960. Published 6 times per year. Published in Russian and English.

Editorial Board

R.V. Kirichek <i>Editor-in-chief</i>	DSc, associate prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunications (SPbSUT), Saint-Petersburg, Russia
A.G. Vladiko <i>Deputy editor-in-chief</i>	PhD, associate prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunications (SPbSUT), Saint-Petersburg, Russia
M.V. Buinevich <i>Chief editor</i>	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunications (SPbSUT), Saint-Petersburg, Russia
N.N. Rozanov	DSc, prof., member-corr. RAS, Open Joint Stock Company «S.I. Vavilov State Optical Institute» (SOI), Saint-Petersburg, Russia
K.V. Dukel'skii	DSc, associate prof., Open Joint Stock Company «S.I. Vavilov State Optical Institute» (SOI), Saint-Petersburg, Russia
Y. Koucheryavy	PhD, Tampere University of Technology, Tampere, Finland
I. Hošek	PhD, Brno University of Technology, Brno, Czech Republic
O.A. Tiamiyu	PhD, University of Ilorin, Ilorin, Nigeria
I.D. Kozin	DSc, prof., Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
K.E. Samuilov	DSc, prof., Peoples' Friendship University (RUDN), Moscow, Russia
S.N. Stepanov	DSc, prof., Moscow Technical University of Communication and Informatics (MTUCI), Moscow, Russia
A.V. Roslyakov	DSc, prof., Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara, Russia
A.E. Koucheryavy	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia
A.K. Kanaev	DSc, prof., Emperor Alexander I-st Petersburg State Transport University (PSTU), Saint-Petersburg, Russia
S.N. Novikov	DSc, prof., Siberian State University of Telecommunications and Information Sciences (SibSUTIS), Novosibirsk, Russia
S.V. Dvornikov	DSc, prof., Military Academy of Telecommunications named after Marshal Union S.M. Budyonny, Saint-Petersburg, Russia
V.I. Korzhik	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia
Yu.A. Kovalgin	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia

Registration Information

Registered by Federal Service for Supervision of Communications, Information Technology and Mass Media on 17.01.2020: PI No. 77-77501 (prev. reg. on 04.07.2004: No. 77-17986)

Subscription index for joint catalog «PRESSA ROSSII»: 59983

Accommodation in RINC (elibrary.ru) by agreement on 20.02.2013: No. 59-02/2013R

Contact Information

Publisher:	Federal State Budget-Financed Educational Institution of Higher Education «The Bonch-Bruевич Saint-Petersburg State University of Telecommunications» (SPbSUT)	Post address:	193232, Saint Petersburg, Prospekt Bolshevikov, 22/1
Publisher address:	191186, Saint Petersburg, Moika river embankment, 61-A	Phone:	+7 (812) 326-31-63, local 2022, +79643759970
		E-mail:	tuzs@sut.ru
		Web:	http://tuzs.sut.ru

СОДЕРЖАНИЕ

CONTENTS

КОМПЬЮТЕРНЫЕ НАУКИ И ИНФОРМАТИКА

Дворников С.С. Обоснование эмпирического выражения для оценки помехоустойчивости сигналов квадратурной модуляции	6	Dvornikov S. Justification of the empirical expression for assessing the noise immunity of quadrature modulation signals
Плотников П.В., Владыко А.Г. Численный анализ математической модели кластерной V2X-системы	14	Plotnikov P., Vladiko A. Numerical analysis of the mathematical model of a cluster V2X-system
Попов О.В., Тумашов А.В., Борисов Г.Н., Коровин К.О. Математическая модель несимметричного вибратора с вынесенной точкой питания. Часть 1. Общий подход к построению математической модели	24	Popov O., Tumashov A., Borisov G., Korovin K. Mathematical model of the unbalanced monopole feed. Part 1. General approach to building a mathematical model

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

Брусин Е.А. Реализация алгоритма начальной синхронизации демодулятора сигналов с прямым расширением спектра на основе быстрого преобразования Фурье. Часть 2. Оценивание несущей частоты	35	Brusin E. Direct sequence spread spectrum signal's demodulator acquisition implementation based on fast Fourier transform. Part 2. Carrier frequency estimation
Викулов А.С. Эффективное частотно-территориальное планирование сетей IEEE 802.11 как задача «замоещения» плоской зоны покрытия регулярными структурами. Часть 3. Решения задачи выбора частотной конфигурации для случая с 8 каналами	41	Vikulov A. Effective channel planning of IEEE 802.11 networks as a plane tessellation problem. Part 3. Solution of best channel configuration selection problem for eight-channel case
Картак В.М., Губарева О.Ю., Дашков М.В., Гуреев В.О., Евтушенко А.С. Исследование чувствительности оптических волокон в контексте локализации злоумышленника в защищенном помещении	52	Kartak V., Gubareva O., Dashkov M., Gureev V., Evtushenko A. The sensitivity investigation of fiber optic paths in the framework of an intruder localization at a protected facility
Киричек Р.В., Березкин А.А., Кукунин Д.С., Колесников А.В. Тестирование облачных систем видеоконференцсвязи на основе параметра Хёрста	59	Kirichek R., Berezkin A., Kukunin D., Kolesnikov A. Analysis of experience quality parameters of cloud video conferencing systems under interference conditions

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

Израилов К.Е. Моделирование программы с уязвимостями с позиции эволюции ее представлений. Часть 1. Схема жизненного цикла	75	Izrailov K. Modeling a program with vulnerabilities in the terms of its representations evolution. Part 1. Life cycle scheme
Коломеец М.В., Чечулин А.А. Метрики вредоносных социальных ботов	94	Kolomeets M., Chechulin A. Properties of malicious social bots
Левшун Д.С. Иерархическая модель для проектирования систем на основе микроконтроллеров защищенными от киберфизических атак	105	Levshun D. Hierarchical model for the design of microcontroller-based systems protected from cyber-physical attacks

КОМПЬЮТЕРНЫЕ НАУКИ И ИНФОРМАТИКА

1.2.2 – Математическое моделирование, численные методы и комплексы программ

Научная статья

УДК 621.396

DOI:10.31854/1813-324X-2023-9-1-6-13



Justification of the Empirical Expression for Assessing the Noise Immunity of Quadrature Modulation Signals

Sergei Dvornikov^{1, 2} ✉, dvornik.92@mail.ru

¹Saint Petersburg State University of Aerospace Instrumentation,
St. Petersburg, 190000, Russian Federation

²Military Academy of Communications,
St. Petersburg, 194064, Russian Federation

Abstract: An approach to the substantiation of the empirical formula for calculating the bit error probability of quadrature modulation signals in terms of the average signal energy and the minimum Euclidean distance is considered. An analytical description of quadrature synthesis signals in the time and frequency continuum is presented. An approach to assessing the noise immunity of quadrature modulation signals from the standpoint of the indicator of the average signal energy and the Euclidean distance is considered. The equivalence of various well-known approaches to the analytical calculation of the bit error probability is shown. Graphic materials are presented, as well as simulation results. Empirically substantiated is a universal expression for assessing the noise immunity of receiving quadrature modulation signals, based on the differences in the average energy value and the value of the minimum Euclidean distance. Its generality with known expressions is shown.

Keywords: quadrature modulation signals, signal noise immunity, minimum Euclidean distance, bit error probability

For citation: Dvornikov S. Justification of the Empirical Expression for Assessing the Noise Immunity of Quadrature Modulation Signals. *Proc. of Telecom. Universities*. 2023;9(1):6–13. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-6-13

Обоснование эмпирического выражения для оценки помехоустойчивости сигналов квадратурной модуляции

Сергей Сергеевич Дворников^{1, 2} ✉, dvornik.92@mail.ru

¹Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Санкт-Петербург, 190000, Российская Федерация

²Военная академия связи им. С.М. Буденного,
Санкт-Петербург, 194064, Российская Федерация

Аннотация: Рассмотрен подход к обоснованию эмпирической формулы для расчета вероятности битовой ошибки сигналов квадратурной модуляции по показателям средней энергии сигнала и минимального евклидова расстояния. Представлено аналитическое описание сигналов квадратурного синтеза во временном и частотном континууме. Рассмотрен подход к оценке помехоустойчивости сигналов квадратурной модуляции с позиций показателя средней энергии сигнала и евклидова расстояния. Показана эквивалентность различных известных подходов к аналитическому расчету вероятности битовой ошибки. Представлены графические материалы, а также результаты моделирования. Эмпирически

обосновано универсальное выражение для оценки помехоустойчивости приема сигналов квадратурной модуляции, основанное на различиях величины средней энергии и значения минимального евклидова расстояния. Показана его общность с известными выражениями.

Ключевые слова: сигналы квадратурной модуляции, помехоустойчивость сигналов, минимальное евклидово расстояние, вероятность битовой ошибки

Ссылка для цитирования: Дворников С.С. Обоснование эмпирического выражения для оценки помехоустойчивости сигналов квадратурной модуляции // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 6–13. DOI:10.31854/1813-324X-2023-9-1-6-13

Introduction

Quadrature modulation (QAM) is widely used in standards of local area networks broadband access (LAN) IEEE 802.11, distributed under the commercial brand Wi-Fi [1–4]. The peculiarity of this type of modulation lies in the independent coding of the in-phase and quadrature channels by manipulating pulses, with their subsequent combination into a single signal structure [5–8]. As a rule, the bit length of the M code selection for M-QAM signals is determined by the level of channel noise and reaches the value $M = 32768$ in ADSL modems [9].

The theory of formation and processing of signals of quadrature modulation is deeply developed and its methods are actively used in various areas of radio engineering and telecommunications [10–13].

At the same time, research continues in the field of synthesis of new signal structures formed by the quadrature method. And for the theoretical study of this direction, more general expressions are needed that allow one to evaluate their noise immunity based only on energy differences in relation to known signal structures [14, 15]. This will make it possible to determine the prospects of their application even at the stage of theoretical study.

Within the framework of this problem, this article presents an approach to justifying an empirical expression that allows estimating the probability of a bit error in a channel depending on the noise level by introducing a correction factor that takes into account the energy characteristics of the signal structure formed by quadrature synthesis.

Introduction to Quadrature Modulation

At its core, quadrature modulation is a symbiosis of amplitude manipulation in each of the channels, with a quadrature shift (the phase difference between the channels is $\pi/2$) between the channels [16]. This allows the resulting signal construction to be represented in the following form [17]:

$$s(t) = I(t)\cos(2\pi f_0 t) + Q(t)\cos\left(2\pi f_0 t + \frac{\pi}{2}\right), \quad (1)$$

where f_0 is the carrier frequency, and $I(t)$ and $Q(t)$ are manipulating information sequences.

In accordance with formula (1), the signals $I(t)$ and $Q(t)$ are formed from the original information bit sequence $u_m(t)$ by appropriate structuring (here m is the ordinal number of the information bit). As a result odd pulses $u_{2m-1}(t)$ manipulate the in-phase component, and even pulses $u_{2m}(t)$ manipulate the quadrature one [17, 18].

On Fig. 1 shows a typical quadrature modulator for synthesizing 4-QAM signals.

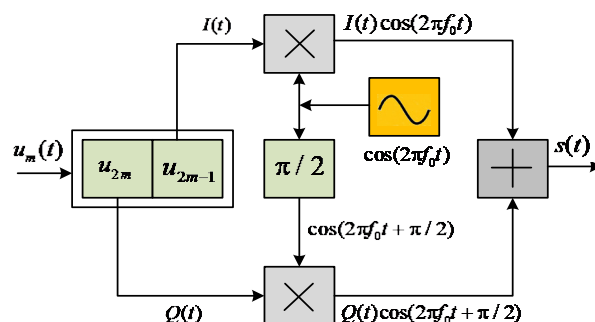


Fig. 1. Structure of a Standard 4-QAM Quadrature Signal Modulator

It should be noted that when dividing the information manipulating sequence $u_m(t)$ into an in-phase one, containing only odd pulses $u_{2m-1}(t)$, and a quadrature one, containing only even components $u_{2m}(t)$, the length of the pulses in these sequences doubles [19].

Quite often, the signals $I(t)$ and $Q(t)$ are directly associated with the manipulating sequence $u_m(t)$, which is not entirely true.

According to the structure of the modulator (see Fig. 1), the signal $s(t)$ must be high-frequency. But such an implementation is difficult for practical use, so the signals $I(t)$ and $Q(t)$ supplied to the multipliers already initially represent low-frequency keyed oscillations:

$$\begin{cases} I_n(t) = a_n \cos[\Omega_{2m-1} u_{2m-1}(t - (2m-1)T)]; \\ Q_n(t) = b_n \sin[\Omega_{2m} u_{2m}(t - 2mT)], \end{cases} \quad (2)$$

where a_n and b_n are the amplitude values of the manipulation pulses; Ω is the full phase of the forming initial low-frequency oscillation; T is a clock interval, by means of which the manipulation speed is set.

In expression (2), the subscript n is introduced for clarity of the procedure for structuring the flows $I(t)$ and $Q(t)$, since the manipulating pulses are divided in

the quadrature and in-phase channels into even and odd sequences.

The convenience of square modulation is determined not only at the stage of signal synthesis, but also at the stage of their processing in a coherent demodulator [18]. Thus, the resulting signal at the reception will be an additive mixture of the useful component $s(t)$ and channel noise $n(t)$ [20]:

$$z(t) = s(t) + n(t), \quad (3)$$

which goes to the demodulator (see Fig. 2).

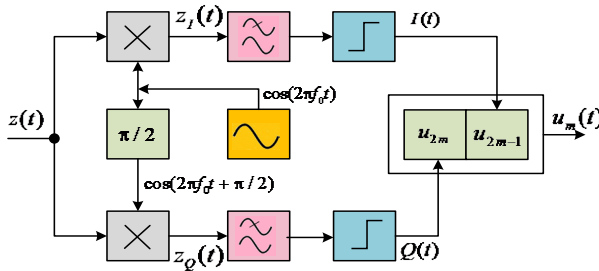


Fig. 2. Structure of a Standard 4-QAM Quadrature Signal Demodulator

When describing the processing procedures for quadrature modulation signals, some publications miss such an important point as the need to implement low-frequency filtering procedures in the in-phase and quadrature channels after removing the carrier wave.

In the demodulator, the removal of the carrier is carried out by multiplying the accepted implementation $z(t)$ (expression (3)), respectively, by the in-phase and quadrature components generated by the reference generator. To clarify this point, consider the implementation of this procedure in more detail using the example of an in-phase channel.

Analytically, the signal $z_I(t)$ can be represented as follows:

$$z_I(t) = z(t) \cos(2\pi f_0 t) = I(t) \cos(2\pi f_0 t) \times \cos(2\pi f_0 t) - Q(t) \sin(2\pi f_0 t) \cos(2\pi f_0 t). \quad (4)$$

And, using the trigonometric transformation, we bring the expression (4) to the form:

$$z_I(t) = 0,5I(t)[1 + \cos(4\pi f_0 t)] - 0,5Q(t)\sin(4\pi f_0 t) = 0,5I(t) + 0,5[I(t)\cos(4\pi f_0 t) - Q(t)\sin(4\pi f_0 t)] \quad (5)$$

Similarly carry out the removal of the carrier in the quadrature channel.

In the demodulator, the removal of the carrier is carried out by multiplying the accepted implementation $z(t)$ (expression (5)). Note that the carrier removal procedure does not yet provide the original keying sequence, since the signal $z_I(t)$ has a high-frequency component. For its localization, low-frequency filtering is used [21, 22].

Further, the filtered signals in each of the channels are fed to the forming devices, from where the pulse sequences (odd from the in-phase channel, and even from the quadrature channel) come to the output, where they are structured into the resulting information sequence $u_m(t)$. An important feature of quadrature modulation signals is that the total signal bandwidth $s(t)$ at the modulator output is similar to DSB (Double-Sideband) transmission signals [23, 24], which have a symmetrical spectrum with respect to the carrier. Note that the spectral redundancy of DSB signals potentially doubles the information capacity when using the quadrature method. Since the spectrum of signals formed in quadrature, unlike DSB signals, does not have a constant component at the carrier frequency [25], it is easy to restore the phase of the carrier oscillation with clock synchronization.

Thus, in order to preserve the independence of the signals $I(t)$ and $Q(t)$, hard clock synchronization must be provided at the reception when the carrier is removed. In the absence of synchronization of the transceiver equipment, a phase mismatch occurs between the oscillation of the demodulator reference oscillator and the carrier frequency of the received signal. As a result of such a mismatch, the effect of mutual penetration of the signal $I(t)$ into the quadrature channel, and the signal $Q(t)$ into the in-phase channel occurs, as a result of which crosstalk occurs [26–28]. In this context, the clock signal is called the "phase reference". In practice, synchronization in radio links using signals based on quadrature modulation is provided by additional transmission of a pilot signal [17].

In the interests of studying the spectral images of quadrature modulation signals, we transform expression (1) taking into account the equality:

$$\cos(2\pi f_0 t + \pi/2) = -\sin(2\pi f_0 t) \quad (6)$$

expression (6) and Euler's formulas to the form:

$$s(t) = I(t) \cos(2\pi f_0 t) - Q(t) \sin(2\pi f_0 t) = 0,5 \exp(j2\pi f_0 t) [I(t) + jQ(t)], \quad (7)$$

where j is the sign of the complex representation.

And applying the Fourier transform to expression (7), we obtain the desired spectrum $F_s(f)$:

$$F_s(f) = 0,5[F_I(f - f_0) + \exp(j2\pi f_0)F_Q(f - f_0)], \quad (8)$$

here $F_I(f)$ and $F_Q(f)$ are the spectral representations of the signals $I(t)$ and $Q(t)$ after the execution of the Fourier transform procedure.

Noise immunity of quadrature modulation signals

The noise immunity of any signal structure is determined by the energy of the signal symbol E [10, 15, 16]. Considering that with quadrature modulation, the signal symbol is formed on the basis of two components, then its energy of the n^{th} symbol will be determined as follows:

$$E_n = (a_n^2 + b_n^2)E_0, \quad (9)$$

where a_n and b_n are the scaling amplitude coefficients of the in-phase and quadrature components of the shaping pulses; E_0 is the energy of the forming pulse.

Note that formula (9) fully characterizes only 4-QAM signals, in which a_n and b_n have the same values for any symbol, see Fig. 3.

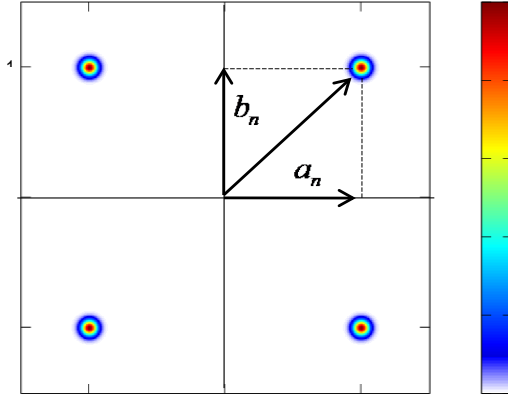


Fig. 3. 4-QAM Signal Constellation

However, things are more complicated for multiposition quadrature modulation signals with $n > 4$.

So, as an example, in Fig. 4 shows the signal constellation for 16-QAM, as well as the amplitudes A_n and A_k , which have different values, since they are formed by different values of a_n and b_n . Obviously, for a signal construction, one can only talk about the average energy E_Σ per N symbols.

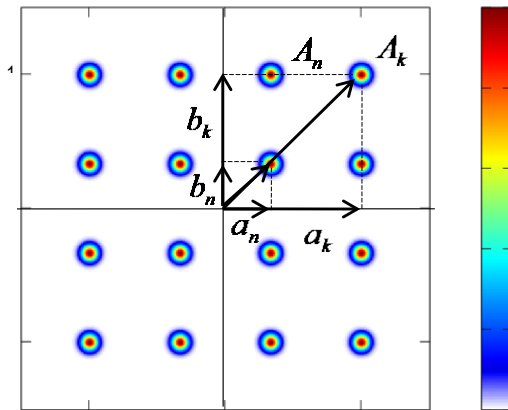


Fig. 4. 16-QAM Signal Constellation

$$E_\Sigma = \frac{1}{N} \sum_{n=1}^N (a_n^2 + b_n^2) E_0. \quad (10)$$

Formula (10) introduces the concept of the energy of the smallest impulse E_0 , so the quantities a_n and b_n act as amplitude values. This is done so that expression (10) can be conveniently used for complex structures with dimensions $n > 4$.

Since the matrix of a_n and b_n values for 16-QAM is as follows:

$$\{a_k, b_k\} = \begin{bmatrix} (-3, 3) & (-1, 3) & (1, 3) & (3, 3) \\ (-3, 1) & (-1, 1) & (1, 1) & (3, 1) \\ (-3, -1) & (-1, -1) & (1, -1) & (3, -1) \\ (-3, -3) & (-1, -3) & (1, -3) & (3, -3) \end{bmatrix}, \quad (11)$$

then if we hypothetically assume that in the 16-QAM signal structure the order of symbol change is uniform, then we can calculate the average energy E_{16} in energy units of the smallest pulse E_0 (in this case, in relation to Fig. 4, this is the pulse formed by the amplitude values a_n and b_n).

The resulting value will be equal to $E_{16} = 10 E_0$. Here and below, the subscript indicates the positional nature of the construction. To understand the considered approach, the energy E_4 for the 4-QAM signal structure, calculated in a similar way according to formula (11), will be $E_4 = 18 E_0$.

That is, the average energy of the 4-QAM signal construct is 1.8 times higher than the average energy of the 16-QAM signal construct. By the way, for the 2-QAM design, the symbol energy will also be $E_2 = 18 E_0$, which corresponds to the well-known fact about the equality of the noise immunity of QPSK and BPSK signals.

When assessing the noise immunity of quadrature modulation signals, the formula proposed in [16] is often used, which makes it possible to estimate the probability of a bit error depending on the signal-to-noise (hereinafter referred to as SNR) ratio $h^2 = E_b / N_0$, where E_b is the energy per bit, and N_0 is noise power spectral density:

$$P_b = \frac{2(1 - L^{-1})}{\log_2 L} Q \left[\sqrt{\frac{(3 \log_2 L) 2 E_b}{L^2 - 1} \frac{1}{N_0}} \right], \quad (12)$$

where L is the number of keying levels defined for the M -QAM signal as $L = \sqrt{M}$; E_b is the signal energy per bit; N_0 is the noise power spectral density: the Q -function is the Gaussian error integral:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp \left(-\frac{u^2}{2} \right) du, \quad (13)$$

However, formula (12) in its final form does not reveal the essence of the noise immunity of QAM signals. Therefore, in the interest of revealing the generality of signal structures formed on the basis of quadrature modulation to signals of phase and multiposition amplitude manipulation, we consider the probability of their detection at the reception using expression (13).

Thus, the probability of reliable reception of the QAM signal is possible in the case of a positive decision to receive the signal in both in-phase and quadrature channels. Taking into account that the error probability of the L -level amplitude shift keying is determined in accordance with the formula presented in [29] (the validity of the formula is justified when encoding the levels with the Gray code):

$$P_s = \frac{2(\sqrt{M} - 1)}{\sqrt{M}} Q \left[\sqrt{\frac{3E_s}{(M-1)N_0}} \right], \quad (14)$$

then the probability of correct reception simultaneously in both channels of the quadrature demodulator will be determined as 6:

$$P_0 = (1 - P_s)^2. \quad (15)$$

In formula (12), E_s is the energy per signal symbol.

Considering that the energy E_b is related to E_s by the following relationship [16, 30]:

$$E_s = E_b \log_2(M), \quad (16)$$

the probability of a bit error of reception, taking into account formulas (14), (15) and (16), we write in the following form:

$$P_b = \frac{1 - \left[1 - \frac{2(\sqrt{M}-1)}{\sqrt{M}} Q \left(\sqrt{\frac{3E_b \log_2(M)}{(M-1)N_0}} \right) \right]^2}{\log_2 M}, \quad (17)$$

where division by $\log_2 M$ is due to the fact that the value of P_b is related to the probability of a symbol error $P_c = 1 - P_0$ as follows $P_c = P_b \log_2 M$.

Formula (17) is a general expression for assessing the noise immunity of M -QAM signal structures. Therefore, for 4-QAM, i. e. for $M = 4$, we get:

$$P_b = Q(\sqrt{2}h) [1 - 0.5Q(\sqrt{2}h)]. \quad (18)$$

Accordingly, for 16-QAM, i. e. for $M = 16$:

$$P_b = \frac{3}{4} Q \left(\sqrt{\frac{4}{5}} h \right) \left[1 - \frac{3}{4} Q \left(\sqrt{\frac{4}{5}} h \right) \right], \quad (19)$$

where $h = \sqrt{E_b/N_0}$.

The analysis of the obtained results showed that the calculation results, according to formulas (18) and (19), completely coincide with the results obtained in accordance with (16), see Fig. 5.

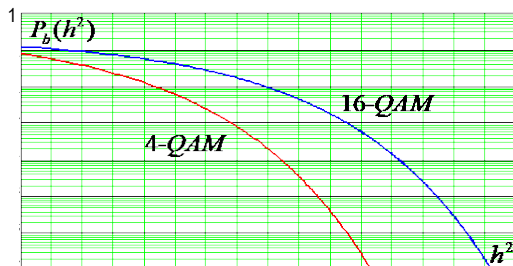


Fig. 5. Bit Error Probability for 4-QAM and 16-QAM Signals

In addition, the result (17) is similar to the calculations obtained in accordance with the well-known expression [17]:

$$P_b = Q(\sqrt{2}h). \quad (20)$$

In [16], it is indicated that when encoding with a Gray code, the noise immunity of QPSK signals be-

comes equal to the noise immunity of BPSK signals. On Fig. 5 and further in the text along the abscissa of the SNR value in dB.

Justification of the calculated expression based on the empirical approach

The analytical complexity of expression (16) and the strict dependence on the value of the parameter M limit its practical application in experimental studies.

At the same time, another important indicator that determines the noise immunity of a signal structure is the minimum Euclidean distance (MED) Δ [31, 32], which can also be used to estimate the probability of a bit error. And then, given the equality of the signal energy, to assess the noise immunity, you can use formula (20) with a correction factor Y :

$$\tilde{P}_b = Q(\sqrt{2}hY). \quad (21)$$

In turn, the coefficient Y will be equal to:

$$Y = \frac{[\Delta_{M_1}/\Delta_{M_2}]}{[E_{M_1}/E_{M_2}]},$$

here Δ_{M_1} is the value of the MEP of the reference signal structure, relative to which the comparison is carried out; Δ_{M_2} is the value of the MEP of the compared signal structure; E_{M_1} is the average energy of the reference signal structure against which the comparison is made; E_{M_2} is the average energy of the compared signal structure.

The MEP value can be calculated based on the logic of constructing the signal structure itself [33]. So for BPSK MEP is $\Delta_2 = 2\sqrt{2}$, for 4-QAM MEP is $\Delta_4 = 2$, for 16-QAM MEP is $\Delta_{16} = 2/3$. You can also calculate the values of the average energy. In particular, a value of 1.8 was previously obtained for 16-QAM. Then, taking into account the value of MEP $\Delta_{16} = 2/3$, it is possible to calculate the probability of a bit error using formula (21).

On Fig. 6 shows the results of calculating the bit error probability for a 16-QAM signal based on formulas (18) and (20).

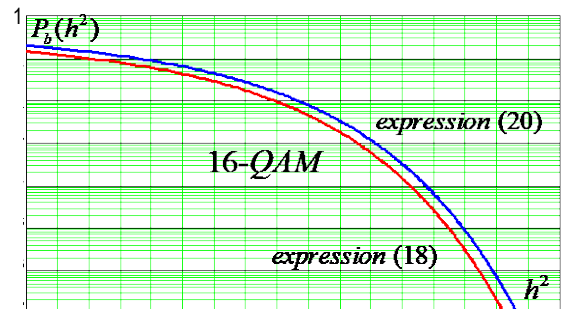


Fig. 6. Bit Error Probability for 16-QAM Signal

An analysis of the obtained results allows us to judge that the differences in the calculations do not exceed 0.5 dB over the entire range of SNR changes. In

the course of substantiating the calculated expression, other signal structures formed by the quadrature method were also investigated. The results obtained have similar calculation errors, which indicates the generality of formula (21).

Conclusion

The validity of the proposed approach is based on the correspondence of the results of analytical modeling to well-known data. The convenience of the empirical formula (19) is that it allows using only the values of MEP and average energy in the synthesis of new signal structures to assess its noise immunity. This opens up

the possibility of its application even at the stage of developing a hypothesis. For example, when synthesizing signal structures with transformed constellations obtained in [34], or for QAM signals built on the basis of various types of hexagonal arrays [35]. This is due to the fact that for such structures it is not applicable in the direct formulation of the analytical apparatus for assessing noise immunity.

Further research will be related to the development of an approach to increasing the spectral efficiency of signal structures formed by the quadrature synthesis method. Including using wavelet functions.

Reference

1. Dovbnya V.G., Koptev D.S., Babanin I.G., Knyazev A.A. Evaluation of the influence of the value of the dynamic range of the radio receiver on the noise immunity of receiving signals with quadrature amplitude modulation. *T-Comm*. 2021;15(6): 65–69. DOI:10.36724/2072-8735-2021-15-6-65-69
2. Zasenkov V., Prosviryakova L. Shaper of quadrature components of a complex envelope signal with minimal frequency modulation. *The Herald of the Siberian State University of Telecommunications and Informatics*. 2020, № 2:20–29. (in Russ.)
3. Rabin A.V. Combining of Orthogonal Coding and Quadrature Amplitude Modulation. *Journal Achievements of Modern Radioelectronics*. 2020;74(9):44–52. (in Russ.) DOI:10.18127/j20700784-202009-05
4. Dvornikov S.V., Pshenichnikov A.V. Design of spectral-efficient signal construction in radio data transmission control and measuring complexes. *Journal of Instrument Engineering*. 2017;60(3):221–228. (in Russ.) DOI:10.17586/0021-3454-2017-60-3-221-228
5. Ryumshin K.Y., Atakischev O.I., Amelenkov A.A., Zhuravlev A.P. Phasing algorithm for demodulation of phase-keyed signals with quadrature amplitude modulation. *Izvestiya Instituta inzhenernoy fiziki*. 2022;2(64):35–39. (in Russ.)
6. Dvornikov S.V., Borodin E.Yu., Madzhar Kh., Makhlufov Yu.Kh. Time-Frequency Estimation of Signal Parameters Based on the Envelope Functions of Their Energy Distribution Density. *Information and Space*. 2007;4:41–45. (in Russ.)
7. Simongauz V.I. Digital system for entering into communication when receiving a radio signal with quadrature phase modulation. *Radioengineering*. 2020;84(1):24–34. (in Russ.) DOI:10.18127/j00338486-202001(02)-03
8. Rec. ITU-T G.992.3 (04/2009) *Asymmetric digital subscriber line transceivers 2 (ADSL2)*
9. Goldsmith A. *Wireless Communication*. Cambridge University Press; 2005. 644 p.
10. Al Safi A., Bazuin B. FPGA based implementation of BPSK and QPSK modulators using address reverse accumulators. *Proceedings of the 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, UEMCON, 20–22 October 2016, New York, USA*. IEEE; 2016. DOI:10.1109/UEMCON.2016.7777861
11. Ali M., Ahsan T., Armughan A., Bilal H., Farhan A., Rehan C., Mehr D. BER Reduction in QPSK. *Journal of Applied Environmental and Biological Sciences*. 2017;7(60):57–64.
12. Choi D.Y., Kim W.K., Kim J.H., Cho H. Performance of analog and digital modulation schemes under sweep jamming. *Proceedings of the 8th International Conference on Ubiquitous and Future Networks, ICUFN, 05–08 July 2016, Vienna, Austria*. IEEE; 2016. p.13–15. DOI:10.1109/ICUFN.2016.7536970
13. Agievich S.N., Dvornikov S.V., Guselnikov A.S. Signal description in basis of Vilenkin – Chrestenson spline-function. *Testing. Diagnostics*. 2009;3:52–57. (in Russ.)
14. Kulikov G.V., Shamshura A.O., Pechenin E.A., Shatalov E.V. Analysis of the noise immunity of receiving signals with quadrature amplitude modulation against the background of frequency-shift keyed interference. *Vestnik of Voronezh Institute of the Russian Federal Penitentiary Service*. 2022;2:9–15. (in Russ.)
15. Proakis J.G. *Digital communication*. New York: Mc Graw-Hill, 1995.
16. Feher K. *Wireless Digital Communication: Modulation and Spread Spectrum Applications*. New Jersey: Prentice Hall, 1995. 544 p.
17. Dvornikov S.V. Demodulation of Signals Based on the Processing of their Modified Frequency-Time Distributions. *Digital Signal Processing*. 2009;2:7–11. (in Russ.)
18. Bakulin M.G., Grigor'ev V.A., Lagutenko I.O., Kreindelin V.B. Synthesis of Multidimensional Signal Constellations with Quadrature Amplitude Modulation. *Journal of Communications Technology and Electronics*. 2017;62(4):344–353. (in Russ.) DOI:10.1134/S1064226917040015
19. Dvornikov S.V., Dvornikov S.S., Ivanov R.V., Gulidov A.A., Chikhonadskikh A.P. Protection of Structural Noise Radio Channel Frequency Shift Keying. *Information Technologies*. 2017;23(3):193–198. (in Russ.)
20. Khasyanova E.R., Sedov M.O. Experimental Study of Methods for Estimating and Compensating Errors in Quadrature Conversion of Signals with M-QAM Modulation. *Systems of Synchronization, Formation and Processing of Signals*. 2017;8(1): 119–122. (in Russ.)
21. Alekseev A.A., Aladinskii V.A., Zheleznyak V.K., Komarov V.F., Dvornikov S.V. Time-Frequency Processing of Acoustic Signals Applied to Reverberation Parameters Measurement. *Nauchnoe priborostroenie*. 2001;11(1):65–76. (in Russ.)
22. Xue M., Chen W., Zhu B., Pan S. High-resolution optical vector network analyzer employing optical double-sideband modulation and optical hilbert transform. *Electronics Letters*. 2019;55(6):337–339. DOI:10.1049/el.2018.5243

23. Wen J., Shi D., Jia Z., Shi Z., Li M., Zhu N.H., Li W. Accuracy-enhanced wideband optical vector network analyzer based on double-sideband modulation. *Journal of Lightwave Technology*. 2019;37(13):2920–2926.
24. Gao X., Huang S., Lei M., Zhang H., Qian J., Bai Y., Zheng Z. Chromatic diarrhea immune microwave photonic phase shifter based on double-sideband modulation. *Optics Letters*. 2019;44(18):4503–4506.
25. Paramonov A.A., Hoang V.Z. Noise immunity of digital information transmission in a radio communication system using DOFT signals with frequency hopping under the influence of noise interference in a part of the band. *Journal of Radio Electronics*. 2021;2:1. (in Russ.) DOI:10.30898/1684-1719.2021.2.8
26. Stetsenko G.A., Lomakin A.F., Statsenko L.G. Detection of Possible Intra-System Interference In The "Vladivostok" Zone of the SFN DVB-T2 Primorsky Krai. *Izvestiya SFedU. Engineering Science*. 2018;6(200):152–163. (in Russ.) DOI:10.23683/2311-3103-2018-6-152-163
27. Abdourahmane A. Advantages of optical orthogonal frequency division multiplexing in communications systems. *EUREKA: Physics and Engineering*. 2016;2:27–33. DOI:10.21303/2461-4262.2016.00058
28. Xiong F. *Digital Modulation Techniques*. Artech House Publishers; 2006.
29. Dvornikov S.V., Pshenichnikov A.V., Avanesov M.Yu. Model of Destructive Influence of Cognitive Character. *Information and Space*. 2018;2:22–29. (in Russ.)
30. Ovchinnikov A.A. The Problem of the LDPC-Codes Constructing on the Base of Euclidean Geometries. *Information and Control Systems*. 2005;1(14):32–40. (in Russ.)
31. Azarov A.I., Budarin E.V. Estimation the noise immunity of continuous phase modulation signals with full response based simulation model. *T-Comm*. 2021;15(1):52–56. DOI:10.36724/2072-8735-2021-15-1-52-56
32. Vitthaladevuni P.K., Alouini M.-S., Kieffer J.C. (2005). Exact BER computation for cross QAM constellations. *IEEE Transactions on Wireless Communications*. 2005;4(6):3039–3050. DOI:10.1109/TWC.2005.857997
33. Dvornikov S.V., Pshenichnikov A.V., Burykin D.A. Structural-Functional Model of a Signal Constellation with Increased Noise Immunity. *Information and Space*. 2015;2:4–7. (in Russ.)
34. Dvornikov S.V., Pshenichnikov A.V., Rusin A.A., Dvornikov A.S. Increased Noise Immunity Signal 16-QAM Constellation with Transformed. *Voprosy radioelektroniki. Seriya: Tekhnika teledeniia*. 2014;2:51–56. (in Russ.)
35. Dvornikov S.V., Manaenko S.S., Dvornikov S.S., Pogorelov A.A. Synthesis PSK wavelet-signals. *Information Technologies*. 2015;21(2):140–143. (in Russ.)

Список источников

1. Довбня В.Г., Коптев Д.С., Бабанин И.Г., Князев А.А. Оценка влияния значения динамического диапазона радио-приёмного устройства на помехоустойчивость приема сигналов с квадратурной амплитудной модуляцией // *T-Comm*. 2021. Т. 15. № 6. С. 65–69. DOI:10.36724/2072-8735-2021-15-6-65-69
2. Засенко В.Е., Просвирякова Л.В. Формирователь квадратурных составляющих комплексной огибающей сигнала с минимальной частотной модуляцией // *Вестник СибГУТИ*. 2020. № 2. С. 20–29.
3. Рабин А.В. Совместное применение ортогонального кодирования и квадратурной амплитудной модуляции // *Успехи современной радиоэлектроники*. 2020. Т. 74. № 9. С. 44–52. DOI:10.18127/j20700784-202009-05
4. Дворников С.В., Пшеничников А.В. Формирование спектрально-эффективных сигнальных конструкций в радиоканалах передачи данных контрольно-измерительных комплексов // *Известия высших учебных заведений. Приборостроение*. 2017. Т. 60. № 3. С. 221–228. DOI:10.17586/0021-3454-2017-60-3-221-228
5. Рюмшин К.Ю., Атакищев О.И., Амелёнков А.А., Журавлёв А.П. Алгоритм фазирования при демодуляции фазоманипулированных сигналов и сигналов с квадратурной амплитудной модуляцией // *Известия Института инженерной физики*. 2022. № 2(64). С. 35–39.
6. Дворников С.В., Бородин Е.Ю., Маджар Х., Махлуф Ю.Х. Частотно-временное оценивание параметров сигналов на основе функций огибающих плотности распределения их энергии // *Информация и космос*. 2007. № 4. С. 41–45.
7. Симонгауз В.И. Цифровая система вхождения в связь при приеме радиосигнала с квадратурной фазовой модуляцией // *Радиотехника*. 2020. Т. 84. № 1. С. 24–34. DOI:10.18127/j00338486-202001(02)-03
8. Rec. ITU-T G.992.3 (04/2009) Asymmetric digital subscriber line transceivers 2 (ADSL2)
9. Goldsmith A. *Wireless Communication*. Cambridge University Press, 2005. 644 p.
10. Al Safi A., Bazuin B. FPGA based implementation of BPSK and QPSK modulators using address reverse accumulators // *Proceedings of the 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON, New York, USA, 20–22 October 2016)*. IEEE, 2016. DOI:10.1109/UEMCON.2016.7777861
11. Ali M., Ahsan T., Armughan A., Bilal H., Farhan A., Rehan C., Mehr D. BER Reduction in QPSK // *Journal of Applied Environmental and Biological Sciences*. 2017. Vol. 7. Iss. 6. PP. 57–64.
12. Choi D.Y., Kim W.K., Kim J.H., Cho H. Performance of analog and digital modulation schemes under sweep jamming // *Proceedings of the 8th International Conference on Ubiquitous and Future Networks (ICUFN, Vienna, Austria, 05–08 July 2016)*. IEEE, 2016. PP. 13–15. DOI:10.1109/ICUFN.2016.7536970
13. Агиевич С.Н., Дворников С.В., Гусельников А.С. Описание сигналов в базисах функций сплайн – Виленкина – Кристенсона // *Контроль. Диагностика*. 2009. № 3. С. 52–57.
14. Куликов Г.В., Шамшура А.О., Печенин Е.А., Шаталов Е.В. Анализ помехоустойчивости приема сигналов с квадратурной амплитудной модуляцией на фоне частотно-манипулированной помехи // *Вестник Воронежского института ФСИИ России*. 2022. № 2. С. 9–15.
15. Прокис Д.Д. *Цифровая связь*. Пер. с англ. М.: Радио и связь. 2000. 797 с.
16. Феер К. *Беспроводная цифровая связь: Методы модуляции и расширения спектра*. Пер. с англ. М.: Радио и связь, 2000. 518 с.

17. Дворников С.В. Демодуляция сигналов на основе обработки их модифицированных частотно-временных распределений // Цифровая обработка сигналов. 2009. № 2. С. 7–11.
18. Бакулин М.Г., Григорьев В.А., Крейнделин В.Б., Лагутенко И.О. Синтез многомерных созвездий сигналов с квадратурной амплитудной модуляцией // Радиотехника и электроника. 2017. Т. 62. № 4. С. 344–353. DOI:10.7868/S003384 9417040015
19. Дворников С.В., Дворников С.С., Иванов Р.В., Гулидов А.А., Чихонадских А.П. Защита от структурных помех радиоканалов с частотной манипуляцией // Информационные технологии. 2017. Т. 23. № 3. С. 193–198.
20. Хасьянова Е.Р., Седов М.О. Экспериментальное исследование методов оценки и компенсации погрешностей квадратурного преобразования сигналов с модуляцией М-КАМ // Системы синхронизации, формирования и обработки сигналов. 2017. Т. 8. № 1. С. 119–122.
21. Алексеев А.А., Аладинский В.А., Железняк В.К., Комарович В.Ф., Дворников С.В. Применение методов частотно-временной обработки акустических сигналов для анализа параметров реверберации // Научное приборостроение. 2001. Т. 11. № 1. С. 65–76.
22. Xue M., Chen W., Zhu B., Pan S. High-resolution optical vector network analyser employing optical double-sideband modulation and optical hilbert transform // Electronics Letters. 2019. Vol. 55. Iss. 6. PP. 337–339. DOI:10.1049/el.2018.5243
23. Wen J., Shi D., Jia Z., Shi Z., Li M., Zhu N.H., Li W. Accuracy-Enhanced Wideband Optical Vector Network Analyzer Based on Double-Sideband Modulation // Journal of Lightwave Technology. 2019. Vol. 37. Iss. 13. PP. 2920–2926.
24. Gao X., Huang S., Lei M., Zhang H., Qian J., Bai Y., Zheng Z. Chromatic dispersion immune microwave photonic phase shifter based on double-sideband modulation // Optics Letters. 2019. Vol. 44. Iss. 18. PP. 4503–4506.
25. Парамонов А.А., Хоанг В.З. Помехоустойчивость передачи цифровой информации в системе радиосвязи сигналами ДОФТ с ППРЧ при воздействии шумовой помехи в части полосы // Журнал радиоэлектроники. 2021. № 2. С. 1. DOI:10.30898/1684-1719.2021.2.8
26. Стеценко Г.А., Ломакин А.Ф., Стаценко Л.Г. Выявление возможных внутрисистемных помех в зоне "Vladivostok" одночастотной сети DVB-T2 Приморского края // Известия ЮФУ. Технические науки. 2018. № 6(200). С. 152–163. DOI:10.23683/2311-3103-2018-6-152-163
27. Abdourahmane A. Advantages of optical orthogonal frequency division multiplexing in communications systems // EUREKA: Physics and Engineering. 2016. Iss. 2. PP. 27–33. DOI:10.21303/2461-4262.2016.00058
28. Xiong F. Digital Modulation Techniques. Artech House Publishers, 2006.
29. Дворников С.В., Пшеничников А.В., Аванесов М.Ю. Модель деструктивного воздействия когнитивного характера // Информация и космос. 2018. № 2. С. 22–29.
30. Овчинников А.А. К вопросу о построении LDPC-кодов на основе евклидовых геометрий // Информационно-управляющие системы. 2005. № 1(14). С. 32–40.
31. Azarov A.I., Budarin E.V. Estimation the noise immunity of continuous phase modulation signals with full response based simulation model // T-Comm. 2021. Vol. 15. Iss. 1. PP. 52–56. DOI:10.36724/2072-8735-2021-15-1-52-56
32. Vitthaladevuni P.K., Alouini M.-S., Kieffer J.C. (2005). Exact BER computation for cross QAM constellations // IEEE Transactions on Wireless Communications. 2005. Vol. 4. Iss. 6. PP. 3039–3050. DOI:10.1109/TWC.2005.857997
33. Дворников С.В., Пшеничников А.В., Бурыкин Д.А. Структурно-функциональная модель сигнального созвездия с повышенной помехоустойчивостью // Информация и космос. 2015. № 2. С. 4–7.
34. Дворников С.В., Пшеничников А.В., Русин А.А., Дворников А.С. Повышение помехоустойчивости сигналов КАМ-16 с трансформированными созвездиями // Вопросы радиоэлектроники. Серия: Техника телевидения. 2014. № 2. С. 51–56.
35. Дворников С.В., Манаенко С.С., Дворников С.С., Погорелов А.А. Синтез фазоманипулированных вейвлет-сигналов // Информационные технологии. 2015. Т. 21. № 2. С. 140–143.

Статья поступила в редакцию 19.12.2022; одобрена после рецензирования 14.02.2023; принята к публикации 15.02.2023.

The article was submitted 19.12.2022; approved after reviewing 14.02.2023; accepted for publication 15.02.2023.

Информация об авторе:

ДВОРНИКОВ
Сергей Сергеевич

кандидат технических наук, доцент института радиотехники, электроники и связи (институт 2) Санкт-Петербургского государственного университета аэрокосмического приборостроения, научный сотрудник научно-исследовательского отдела Военной академии связи имени Маршала Советского Союза С.М. Буденного,
 <https://orcid.org/0000-0001-7426-6475>

Научная статья

УДК 621.396

DOI:10.31854/1813-324X-2023-9-1-14-23



Численный анализ математической модели кластерной V2X-системы

Павел Владимирович Плотников✉, plotnikov.pv@sut.ru

Андрей Геннадьевич Владыко, vladuko@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация: В статье проводится анализ результатов численного моделирования информационных процессов в автомобильных самоорганизующихся сетях (VANETs). Приведен обзор работ, посвященных кластеризации и кэшированию данных при работе с Vehicle-to-Everything (V2X) системами. В качестве метрики выбрана L_1 -метрика из-за ее активного использования в городах с современной застройкой. Рассмотрены два подхода к описанию и оценке эффективности взаимодействия граничных устройств в традиционной конфигурации и с использованием кластерной схемы с общим кэшем. Построена математическая модель и проведен анализ ее эффективности. Показано, что внедрение новых стандартов IEEE 802.11bd позволит увеличить долю обслуживаемых устройств, тем самым будет сокращена общая задержка вычислений, что позволит повысить эффективность работы V2X-системы. Результаты исследования могут быть использованы при проектировании и развертывании автоматизированных систем управления дорожным движением в городах.

Ключевые слова: VANET, кластеризация, V2X-системы, численное моделирование

Ссылка для цитирования: Плотников П.В., Владыко А.Г. Численный анализ математической модели кластерной V2X-системы // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 14–23. DOI:10.31854/1813-324X-2023-9-1-14-23

Numerical Analysis of the Mathematical Model of a Cluster V2X-System

Pavel Plotnikov✉, plotnikov.pv@sut.ru

Andrei Vladyko, vladuko@sut.ru

The Bonch-Bruevich Saint Petersburg State University of Telecommunications, St. Petersburg, 193232, Russian Federation

Abstract: The article analyzes the results of numerical modeling of information processes in vehicular ad-hoc networks (VANETs). The review of works devoted to clustering and data caching schemes in Vehicle-to-Everything (V2X) systems is given. L_1 -metric was chosen as a metric because of its active use in cities with modern layout. Two approaches to the description and evaluation of the efficiency of interaction of boundary devices in a traditional configuration and using a cluster scheme with a shared cache are considered. A mathematical model is constructed and an analysis of its effectiveness is carried out. It is shown that the introduction of new IEEE 802.11bd standards will increase the percentage of serviced devices, thereby minimize the overall delay of computing, which will improve the efficiency of the V2X-system. The results of the study can be used in the design and deployment of automated traffic control systems in cities.

Keywords: VANET, clustering techniques, V2X-systems, numerical simulation

For citation: Plotnikov P., Vladiko A. Numerical Analysis of the Mathematical Model of a Cluster V2X-System. *Proc. of Telecom. Universities.* 2023;9(1):14–23 (in Russ.) DOI:10.31854/1813-324X-2023-9-1-14-23

Введение

Экспоненциальный рост мобильного трафика данных, в особенности мобильного видеопотока, оказывается достаточно серьезной проблемой при оптимизации взаимодействия внутри вычислительных динамических систем при граничных вычислениях. Компанией Cisco [1] было проведено исследование, по результатам которого сделан вывод, что каждый год глобальный мобильный трафик в среднем возрастает практически в 2 раза. При этом нет никаких причин полагать, что в дальнейшем рост не будет ускоряться. Стоит отметить, что с ростом числа компьютерных вычислений и увеличением объемов обрабатываемой информации возникает необходимость в осуществлении параллельных вычислений как с использованием новых алгоритмов, так и за счет расширения технических возможностей каналов связи. Не менее важным аспектом рассматриваемой проблемы является значительный рост потребления энергии при функционировании рассматриваемых систем. Рост скорости взаимодействия при минимизации задержек оказывает на это потребление значительное влияние. В этой связи требуется разрабатывать новый методический подход к анализу задержек вычислений с учетом энергетических затрат и возможностей модификации и модернизации каналов связи.

Одним из возможных подходов к решению рассматриваемой проблемы является использование облачных вычислений в мобильных коммуникационных средах. При этом часть расчетов переносится с физического устройства на некоторый удаленный сервер, что позволяет повысить скорость вычислений и снизить удельное энергопотребление. Несмотря на то, что в силу развития технологий появляются новые модернизированные стандарты сетей связи, существенную задержку вычислений необходимо учитывать и, по возможности, уменьшать. С этой целью были разработаны и успешно внедрены мобильные граничные вычислители (MEC, *аббр. от англ. Mobile Edge Computing*) [2].

Развитие MEC позволило разработать новый подход к анализу и оптимизации интеллектуальных транспортных систем (ИТС) [3–5]. В работе авторов [6, с. 7] отмечается: “Внедряя автомобильные граничные вычисления (VEC, *аббр. от англ. Vehicular Edge Computing*) в автотранспортные самоорганизующиеся сети (VANETs, *аббр. от англ. Vehicular Ad-hoc Networks*), поставщики услуг могут обеспечить сервисы со сверхмалыми задержками, поскольку инструменты граничных вычислений разворачивают ресурсы на стороне, близкой к пользовательскому оборудованию”. Взаимодействие внутри VANET между автомобилями (V2V,

аббр. от англ. Vehicle-to-Vehicle) может осуществляться для обмена данными о скорости и маршруте, а между автомобилями и граничными вычислителями или, например, элементами инфраструктуры (V2X, *аббр. от англ. Vehicle-to-Everything*) с целью разгрузки локальных вычислительных мощностей, а также управления светофорами или парковочными автоматами [7].

Необходимость в развитии V2X-систем определяется относительно небольшими вычислительными мощностями бортовых устройств транспортных средств (OBU, *аббр. от англ. On-Board Unit*). Для повышения эффективности взаимодействия и минимизации информационных потерь при взаимодействии OBU и MEC на практике используют придорожные вычислительные устройства (RSU, *аббр. от англ. Road-Side Unit*) с целью осуществления более стабильного взаимодействия. Сгенерированная задача на транспортном средстве (ТС) выгружается на RSU и в дальнейшем либо решается на нем, либо передается на ближайший MEC-сервер.

Сложность рассматриваемой задачи определяется ее динамическим характером, а также слабой предсказуемостью пространственной конфигурации системы даже на среднесрочных интервалах упреждения. Поэтому априорно неясно: каким образом и в каком порядке следует разгружать вычислительные задачи. Дополнительным ограничением является то, что MEC-серверы могут работать на границе сети радиодоступа, что затрудняет их использование. Дополнительным узким местом остается соединение и кэширование на уровне граничных устройств OBU – RSU [8].

Стоит отметить, что описанное взаимодействие вызывает дополнительные расходы в виде увеличенного энергопотребления. Задержка вычислений возникает при обработке и передаче контента при взаимодействии MEC-сервера, RSU и ТС. Повышенная интенсивность транспортного потока может вызвать следующий эффект: сеть может столкнуться с перегрузкой. Для снижения нагрузки на сеть применяют два основных подхода: (1) повышение неоднородности сети с учетом текущего трафика; (2) оптимизация граничных вычислений с использованием кэширования и кластеризации.

В данной работе предлагается новый подход к организации взаимодействия элементов системы ТС – RSU. Строится математическая модель и приводится алгоритм ее численного моделирования, производится сравнение с известной моделью [6]. Оценка эффективности производится путем вычисления доли необработанных запросов, сформированных ТС, обусловленной их мобильностью, средних энергопотребления и величины задержки передачи, и обработки сформированных запросов в

системе TC – RSU. Проведено сравнение традиционной и кластеризованной моделей. Результаты показывают, что каждая из предложенных моделей может быть эффективно реализована в мобильных узлах и позволит значительно сократить общее ожидаемое время обработки задач по совершенствованию организации и алгоритмического обеспечения функционирования V2X за счет объединения RSU в кластеры с общим кэшем.

Обзор литературы

В последнее время было выполнено достаточно много работ, посвященных анализу подходов к минимизации потребления энергии при ограничениях, накладываемых на величину задержки в рассматриваемых системах. В работах [9, 10] предложен новый подход к оптимальному распределению ресурсов в сети, основывающийся на использовании выпуклой оптимизации с целью минимизации взвешенного суммарного потребления вычислительной энергии при ограничениях на задержки вычислений.

Группой авторов в работе [11] предложен алгоритм разгрузки распределенных вычислений на основе построения модели, базирующийся на равновесии Нэша, а также проведен сравнительный анализ эффективности алгоритма с известными подходами к оптимизации по двум параметрам: потребленная энергия и время обработки. Численные результаты подтверждают, что предложенный алгоритм может обеспечить отличную производительность при разгрузке вычислений и хорошее масштабирование по мере увеличения числа пользователей. При этом предложенная модель не позволяет проводить анализ систем с мобильными пользователями, которые могут динамически менять свое положение в течение периода разгрузки вычислений.

В последние годы было проведено множество исследований, посвященных анализу подходов к кэшированию данных в мобильных сетях. Классическая схема кэширования с учетом популярности (PBCS, аббр. от англ. Popularity-Based Caching Scheme), подробно изученная в [12–15], впервые применялась в однородных системах, к которым можно отнести сотовую сеть, социальные беспроводные сети VANETs. В этих схемах RSU не взаимодействуют между собой и всегда заполняют свободное пространство в памяти наиболее популярным содержимым. Если OBU не может получить желаемый контент из локальной RSU, то запрос перенаправляется на MEC-сервер.

В работе [16] рассматривается многопоточная схема кэширования, так называемая сеть малой сотовой связи (от англ. Small Cell Network), которая поддерживает многоадресное формирование и рассылку запросов в рамках архитектуры сети. В этой схеме базовые станции макроэлементов (MBS, аббр.

от англ. Macro-Cell Base Station) и базовые станции малых элементов (SBS, аббр. от англ. Small Cell Base Station) собирают запросы с OBU в течение определенного периода сбора данных, при этом на SBS обрабатываются только те запросы, ответы на которые хранятся в кэш-памяти устройства, остальные – переадресуются на MBS. С базовых станций макроэлементов осуществляется формирование, обработка и взаимодействие с MEC-сервером. Эта схема с поддержкой многоадресной рассылки уменьшает время взаимодействия по доставке ресурсов при высокой задержке во взаимодействии с MEC-сервером. Дальнейшие исследования должны быть посвящены оптимизации процесса взаимодействия с удаленным сервером.

Схема кэширования под названием Фемтокэшинг (от англ. Femtocaching) предложена в работе [17]. Предполагается, что схема расположения RSU устроена так, что зоны покрытия базовых станций пересекаются. В этом случае OBU может быть обслужено любым из RSU, в зоне покрытия которого оно находится. Так, в случае отсутствия запрашиваемой информации, запрос от OBU будет перенаправлен на другой ближайший RSU. Данный подход позволяет предположить, что схема кластерного подхода к разделению RSU на группы может привести к получению оптимального решения по минимизации задержек при взаимодействии в системе OBU-RSU, максимальному проценту обслуженных устройств в сети, а также оптимальному расходованию энергии.

Подробный обзор применения кластерного подхода к решению задач в сетях VANETs приведен в более ранней публикации авторов [6, с. 10].

Постановка задачи

Пусть модель города задана в прямоугольной метрике (L_1 -метрика, манхэттенская модель мобильности). Расстояние между двумя точками на плоскости с координатами $A(x_1, y_1)$ и $B(x_2, y_2)$ в данной модели вычисляется по формуле:

$$d(A, B) = |x_2 - x_1| + |y_2 - y_1|.$$

Порядок использования данной модели рассматривался в работе авторов. Подробное описание модели приведено в [6, с. 7–8]. Здесь позволим себе привести лишь краткое описание обозначений и объектов изучения в форме таблицы 1.

Система городских автомобильных дорог образует сетку с горизонтальными и вертикальными элементами, при этом на каждой улице организовано двустороннее движение. OBU транспортных средств генерируют индивидуальный маршрут для перемещения от точки старта до определенной заранее точки прибытия. Элементы RSU расположены в середине каждого квартала между двумя соседними перекрестками.

ТАБЛИЦА 1. Некоторые обозначения

TABLE 1. Some designations

Модель	Символьное обозначение
Набор транспортных средств (шт.)	V
Набор RSU (шт.)	S
Максимальный объем кэш памяти s-ого RSU (байт)	Z_s
Диаметр зоны покрытия s-ого RSU (м.)	L_s
Скорость ТС на участке дороги (м/с)	$u_{\min} \leq u \leq u_{\max}$
Блок данных для обмена в системе OBU-RSU	$M = \{1, 2, \dots, m\}$
Максимальный объем отдельного элемента блока данных (байт)	C
Скорость обмена данными в системе OBU-RSU (байт/с)	α_s

Будем полагать, что скорость u ТС в каждой зоне покрытия RSU будет генерироваться случайно со средним значением μ и дисперсией σ^2 . Функция плотности распределения случайной величины u задается формулой [18]:

$$\varphi(u) = \frac{2}{\sigma\sqrt{2\pi}} e^{-\frac{(u-\mu)^2}{2\sigma^2}} \cdot \frac{1}{\operatorname{erf}\left(\frac{u_{\max}-\mu}{\sigma\sqrt{2}}\right) - \operatorname{erf}\left(\frac{u_{\min}-\mu}{\sigma\sqrt{2}}\right)},$$

где $\operatorname{erf}()$ – функция Лапласа.

Для проведения численного моделирования будем предполагать, что каждая i -я ячейка кортежа M может быть запрошена ТС с вероятностью, заданной по закону Зепфа (Zipf Distribution), вычисляемой по формуле [19]:

$$p(i) = \frac{i^{-A}}{\sum_{k=1}^m k^{-A}}, \quad (1)$$

где A – коэффициент асимметрии распределения и соответствует степени загрузки системы ТС.

Среднее значение объема запроса (в байтах), который необходимо обработать системе МЕС – RSU – OBU можно вычислить как математическое ожидание сформированной случайно величины:

$$D(i) = \sum_{k=1}^m C \cdot p(i), \quad (2)$$

где C – объем отдельного элемента блока данных.

«Отметим, что, так как местоположение и количество ТС в рассматриваемой модели динамически меняются во времени, с некоторой периодичностью необходимо обновлять данные в RSU, запрашивая их с МЕС-сервера. Пусть время обработки запроса от конкретного ТС по блоку данных i составляет $t_i^{(0)}$, если данные по этой ячейке памяти актуальны и $t_i^{(0)} + t_i^{(1)}$, где $t_i^{(1)}$ – время, требующееся на

обновление устаревших данных, если эти данные неактуальны и требуется их актуализация» [6, с. 8].

Будем считать, что RSU может обслуживать ТС последовательно, при этом каждое устройство дорожной инфраструктуры может одновременно обрабатывать до 2 запросов от ТС. Для поддержки приложений V2X в 2010 году IEEE разработала стандарт IEEE 802.11p. Однако системы, основанные на этом стандарте, не удовлетворяют требованиям к очень низкой задержке передачи данных, предъявляемым современными приложениями V2X. Новый стандарт IEEE 802.11bd имеет важное преимущество в виде технологии соединения каналов, которая позволяет передавать данные по двум смежным каналам одновременно. Это увеличивает скорость передачи данных и может снизить задержки и величину потери пакетов. В работе [20] проведена оценка эффективности вышеупомянутых стандартов из семейства IEEE 802.11, учитывающих задержки передачи данных и величину потери пакетов.

При этом если OBU покидает область покрытия RSU, то взаимодействие прекращается, ТС после этого может подключиться к следующему RSU в случае, если оно свободно. Можно считать, что RSU по окончании работы с каким-либо ТС может начать обслуживание следующего ТС мгновенно, то есть за нулевое время, без задержек. Переключение RSU на новое ТС обнуляет кэш, т. е. блоки данных, которые не были полностью обработаны в ходе информационного взаимодействия с предыдущим ТС, удаляются.

Таким образом, если считать скорость ТС на участке дороги, обслуживаемом RSU s равной u м/с, а зона покрытия этого участка имеет длину L_s метров, то максимальное число запросов, которые может обработать RSU от конкретного ТС, вычисляется по формуле [6, с. 8]:

$$k = \left\lfloor \frac{L_s}{u \cdot \alpha_s} \right\rfloor.$$

Введем функцию потерь при обработке RSU запросов ТС. Пусть ТС под номером i сформировало запрос $D(i)$, тогда потери при взаимодействии на участке длины L_s составят:

$$V(i) = \begin{cases} D(i) - C \cdot k, & C \cdot k < D(i) \\ 0, & C \cdot k \geq D(i) \end{cases}.$$

При этом, если часть запрашиваемой информации требует обновления, общее время взаимодействия будет ограничено сверху:

$$\sum_{i=1}^k (t_i^{(0)} + \gamma \cdot t_i^{(1)}) \leq \frac{L_s}{u},$$

где $\gamma = 1$, если данные устарели, и $\gamma = 0$, если данные не требуют актуализации, для каждой пары ТС – RSU.

Анализ энергетических затрат

Важным аспектом решения рассматриваемой задачи является величина энергетических затрат на обслуживание функционирования системы OBU – RSU. Стоит предположить, что с появлением кластеров может значительно возрасти число параллельных запросов между локальными граничными устройствами. Это обусловлено ростом числа вычислительных задач, решаемых на RSU. К обмену данными в системе OBU – RSU, а также взаимодействию в RSU – MEC добавятся взаимодействия внутри кластера, которому принадлежит RSU. При этом стоит ожидать увеличения количества вычислений и роста величины энергетических затрат на функционирование инфокоммуникационной сети.

Будем, как и ранее, считать, что каждое OBU имеет M независимых вычислительных задач, которые необходимо выполнить. Для решения каждой j -й задачи i -й парой OBU – RSU будем рассматривать кортеж $\{D_{ij}, c_{ij}, time_{ij}\}$, где D_{ij} – вычисляется по формуле (2), c_{ij} – общее число циклов работы процессора, необходимое для решения конкретной j -й задачи, $time_{ij}$ – допустимый срок выполнения j -й задачи на i -й паре OBU – RSU.

Можно выделить три типа выполнения вычислительных задач: локальное, кластерное и удаленное. В каждом из этих случаев энергетические затраты будут разными.

Рассмотрим локальное выполнение задачи. В этом случае все взаимодействия происходят непосредственно в паре OBU – RSU, т. е. все необходимые данные уже находятся в кэше RSU.

Потребляемая энергия может быть вычислена по формуле:

$$E_{ij}^L = \eta_i \cdot c_{ij},$$

где η_i – коэффициент, который обозначает энергию, потребляемую за один цикл работы процессора, и зависит от архитектуры вычислительной системы RSU.

Принимаем $\eta_i = 10^{-11}(f_i)^2$, где f_i – количество циклов работы процессора в секунду. В работе [21] приведены сведения о связи частоты процессора с числом выполняемых циклов за единицу энергетических затрат, величина f_i носит название Computing Frequency.

Отдельно рассматривается кластерное и удаленное решение вычислительных задач. Как результат, получены следующие формулы:

1) если рассматривать взаимодействие в системе OBU – RSU без кластерного разбиения, то общие затраты энергии для решения каждой j -й задачи i -й парой вычисляется по формуле:

$$E_{ij}^{nC} = \eta_i \cdot c_{ij} + (p_i^A \cdot T_{ij}^{down} + p_i^D \cdot T_{ij}^{offc}) \cdot \delta_{ij},$$

где p_i^A – мощность приема вычислительного устройства RSU; T_{ij}^{down} – время приема RSU; p_i^D – мощность передачи MEC; T_{ij}^{offc} – время передачи MEC; δ_{ij} – число, принимающее значение «1», если запрашиваемые данные хранятся в кэше RSU, и «0», если данные требуют обновления или отсутствуют;

2) если рассматривать взаимодействие в системе OBU – RSU с использованием разбиения RSU на кластеры с n элементами в каждом, с целью минимизации потерь данных при обслуживании OBU, то общие затраты энергии для решения каждой j -й задачи i -й парой вычисляются по формуле:

$$E_{ij}^C = \eta_i \cdot c_{ij} + nE_0 + (p_i^A \cdot T_{ij}^{down} + p_i^D \cdot T_{ij}^{offc}) \cdot \delta_{ij},$$

где E_0 – энергетические затраты, расходуемые на осуществление одного запроса о наличии данных внутри кластера.

Общие расходы ресурсов на выполнение каждой j -й вычислительной задачи i -й парой OBU – RSU в терминах потребления энергии могут быть определены так:

$$E = \sum_{i,j} ((1 - \beta) E_{ij}^{nC} + \beta E_{ij}^C),$$

где $\beta = 0$, если выбрана бескластерная модель и $\beta = 1$, если используется кластеризация.

В силу того, что в работе [6], было показано, что с укрупнением кластеров, т. е. уменьшением их количества, процент обслуженных OBU растет, введем понятие средних затрат энергии на кластер E/n , где n – число элементов кластера, или величина, характеризующая среднюю расходуемую энергию, приходящуюся на кластер.

Объединяя результаты анализа задачи оптимизации, сформулируем экстремальную задачу следующим образом:

$$\begin{cases} \min_n \frac{E}{n} \\ \min_m \frac{\sum_i V(i)}{\sum_i D(i)} \\ D(i) \leq \frac{L_s}{u_i} \cdot \alpha_s \end{cases}$$

В данной статье вопросы энергетики затрагиваются только в постановочной форме. Более детальный анализ этого аспекта, авторы планируют привести в последующих публикациях.

Общее описание модели

Опишем динамическую систему городского движения. Будем полагать, что планировочная схема улично-дорожной сети является прямоугольной (рисунок 1). Зона покрытия каждой RSU – квартал между двумя соседними перекрестками (на рисунке для RSU использовано обозначение ).

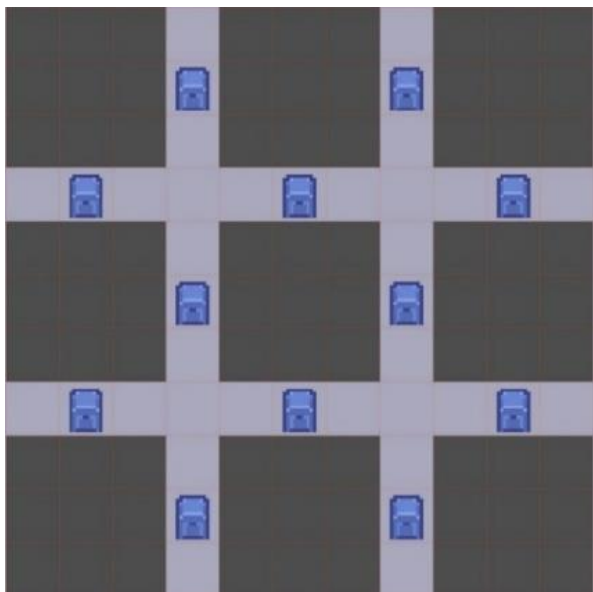


Рис. 1. Модель городской сети

Fig. 1. Scheme of Road Network

В ходе моделирования генерируется случайный поток ТС. Система RSU обслуживает запросы, поступающие от элементов динамической системы в порядке очереди поступления запросов. В случае, если запрос ТС к RSU не был обработан: ТС покинуло зону покрытия прервав взаимодействие, контакт между ТС и RSU так и не был настроен, то данный запрос будет считаться потерей данных при обслуживании. При этом будем считать, что ранее намеченный OBU ТС маршрут остается неизменным, и осуществляется попытка подключения к следующему RSU на пути следования. После нахождения свободного RSU ТС начинает взаимодействие с ним.

Некоторые дополнительные упрощения, позволяющие построить работоспособную модель, детально описаны в [6, с. 8–9], поэтому мы не будем здесь на них останавливаться. В качестве оценки эффективности работы системы будем вычислять процент необработанных запросов, сформированных на начальном этапе при одноканальном и двухканальном подключении ТС к RSU. В качестве дополнительной характеристики для анализа результатов можно подсчитывать среднюю величину энергозатрат на выполнение одного запроса.

Как в работе [6], приведем некоторые дополнительные допущения. Во-первых, не ставится задача нахождения оптимального расположения RSU. Во-вторых, скорость ТС не зависит от скорости движения потока. В-третьих, ТС не перестраивает свой маршрут, опираясь на информацию, полученную от RSU.

Важным и принципиальным отличием от результатов, полученных в работе [6], можно считать, что:

1) каждое ТС формирует запрос случайно по формуле (1);

2) моделирование проводится в увеличенной области со значительно большим числом обслуживаемых ТС;

3) количество блоков информации, которое запрашивает каждое ТС, принимает значение из большего диапазона;

4) RSU может одновременно взаимодействовать с двумя OBU.

Результаты численного моделирования

Численное моделирование проводилось с использованием авторской программы [22], реализованной на языках программирования Python и GDScript по средствам кроссплатформенного механизма Godot Engine. Возможный вариант дорожной сети представлен на рисунке 2. Каждое ТС начинает свой маршрут с ячейки, обозначенной на рисунке знаком , такое положение позволяет наглядно отследить движение ТС и изменение количества отправляемых запросов. При моделировании на большей области число стартовых позиций задается случайно в диапазоне от 1 до 10. RSU обозначены на схеме синими блоками (см. рисунке 1 – ). Конечная точка маршрута каждого ТС генерируется отдельно и расположена на границе, приведенной на рисунке 2, области.

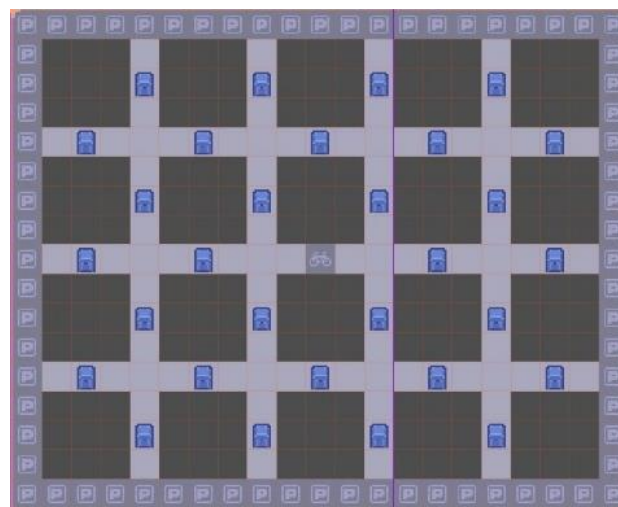


Рис. 2. Моделируемая дорожная сеть

Fig. 2. Model of Road Network

Для проведения численных расчетов примем:

$$V = 800, \quad m = 20, \quad L_s = 200, \quad k_1^{vi} = 1, \quad k_2^{vi} = 12,$$

$$t_i^{(0)} = 0,1 \text{ c}, \quad t_i^{(1)} = 1 \text{ c}, \quad F = 3, \quad T = 10 \text{ c}.$$

Для получения более точной оценки процента необработанных запросов проведем моделирование 10 раз и найдем среднее значение процента необработанных запросов. Результаты численного моделирования показывают, что при генерировании потока ТС 11 и более раз, процент необработанных запросов, поступающих от ТС, меняется не-

значительно. Десяти итераций достаточно, для получения необходимой точности при оценке эффективности рассматриваемого подхода.

Результаты численного моделирования представлены на рисунке 3.

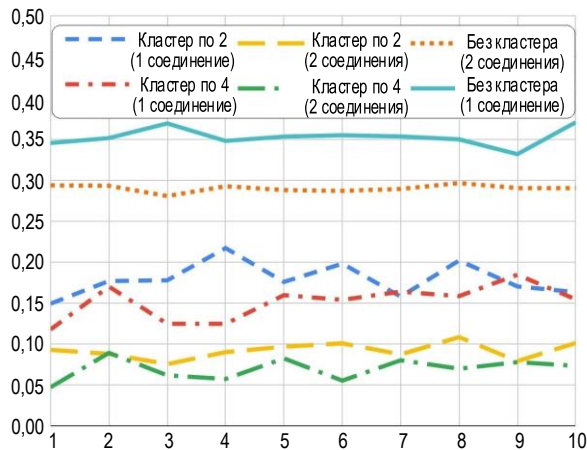


Рис. 3. Средний процент потерь на 10 итерациях

Fig. 3. Average Percentage of Losses on 10 Iterations

На рисунке 3 приведены результаты подсчета среднего числа необработанных запросов при обслуживании ТС: без разбиения граничных устройств на кластеры, с делением на кластеры по 2 и 4 элемента RSU в каждом, в двух вариантах взаимодействия. По горизонтальной оси указан порядковый номер итерации численного моделирования с $V = 800$ ТС, по вертикальной – процент необработанных запросов при взаимодействии в системе ТС – RSU. Как видно из представленных графиков, объединение RSU в кластеры позволяет получить значительный выигрыш в величине процента успешно обработанных запросов. Этот результат подтверждает выводы, сделанные авторами в [6]. При этом чем больше элементов объединяется в один кластер, тем выше эффективность управления системой.

Следует отметить, что технические характеристики современных средств коммуникации и связи не позволяют объединить все RSU в одну общую структуру, вследствие чего необходимо кластерное деление в соответствии с пространственным местоположением устройств граничных вычислений. Из представленных графиков видно, что передача данных по двум смежным каналам одновременно позволяет существенно понизить процент необработанных запросов, сгенерированных ТС. При этом использование кластерного подхода существенно снижает величину потерь в каждом из рассматриваемых случаев.

Приведем графики с результатами численного моделирования в системе ТС – RSU в каждом из двух вариантов взаимодействия: прием и передача данных по одному (рисунок 4а) и по двум смежным каналам одновременно (рисунок 4б).

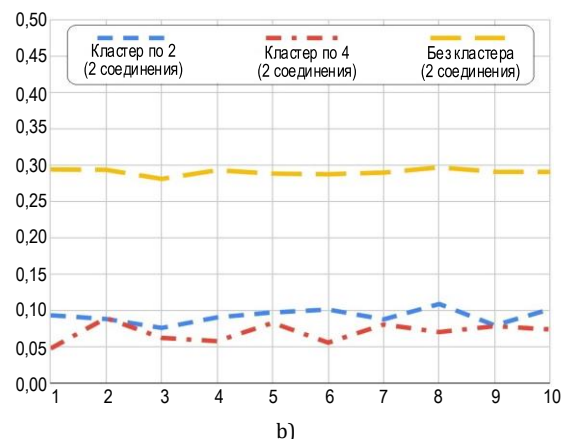
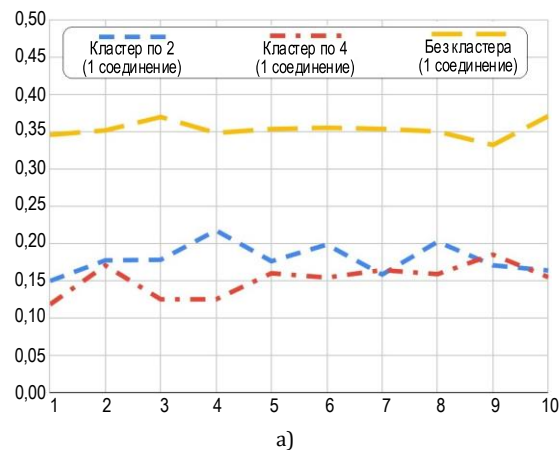


Рис. 4. Средний процент потерь: 1 канал (а) и 2 канала подключения (б)

Fig. 4. Average Percentage of Losses: 1 Connection (a) and 2 Connection Channels (b)

Для качественного сравнения результатов проведем подсчет среднего процента потерь блоков данных по 10 генерациям случайного потока ТС и выборочной дисперсии этих потерь. Сравнительный анализ рассматриваемых параметров в различных условиях приведен в таблице 2.

ТАБЛИЦА 2. Результаты численного моделирования потока ТС в дорожной сети

TABLE 2. The Results of Numerical Simulation of Vehicle Flow in the Road Network

Модель	Выборочное среднее процента потерь, %	Значение выборочной дисперсии
Без кластеров, одно соединение	35,28	1,29
Кластеры по 2, одно соединение	17,88	4,47
Кластеры по 4, одно соединение	15,11	4,66
Без кластеров, два соединения	29,02	0,20
Кластеры по 2, два соединения	9,22	1,07
Кластеры по 4, два соединения	6,97	1,82

Можно отметить, что при использовании бескластерной модели выигрыш от использования новой двухканальной схемы оказывается не столь значительным: потери становятся в среднем на 6 % меньше.

При этом использование любой из рассмотренных схем кластеризации позволяет практически вдвое сократить процентное значение величины потерь. В этой связи стоит комплексно подходить к анализу и построению модели с целью ее эффективного функционирования.

Дополнительно стоит отметить, что значение выборочной дисперсии, характеризующая разброс значений относительно среднего, оказывается значительно меньшим при использовании стандарта IEEE 802.11bd. Это позволяет сделать вывод, что результаты, полученные при использовании вышеупомянутой схемы, являясь более устойчивыми к внешним факторам. Использование схемы с двумя каналами одновременного взаимодействия ТС и RSU оказывается более стабильным инструментом для реализации взаимодействия элементов динамической системы.

Несмотря на то, что использование новых модернизированных стандартов сетей связи и кластеризация позволяют снизить величину потерь данных при моделировании системы ТС – RSU, структурное и функциональное усложнение приводит к повышению энергопотреблению. В этой связи необходимо находить баланс в числе кластеров, основываясь на задачах, поставленных перед системой.

Выводы

В предыдущей статье авторов [6] на основе теоретических рассуждений и моделирования было доказано, что кластеризация является эффективным способом повышения быстродействия и сокращения потерь в сетях VANETs. Эти результаты были подтверждены приведенным численным моделированием. В то же время этот вывод был получен для частного случая конфигурации системы – применительно к одноканальным устройствам обмена данными.

Появление новых технических решений, связанных с внедрением промышленного стандарта IEEE

802.11bd, который подразумевает двухканальную работу [23], вынуждает более осторожно подходить к приведенному выводу. Новые технические решения дают новые возможности для формирования информационно-алгоритмического обеспечения V2X-систем и могут привести к необходимости корректировки схем их функционирования.

В частности, в некоторых случаях (см. результаты моделирования, представленные в данной статье) может оказаться, что переход к использованию двухканальных устройств обмена данными дает больший выигрыш в производительности, в сравнении с кластеризацией на одноканальных устройствах (в статье [6] доказывались преимущества кластеризации). Задача синтеза оптимальной по потерям системы становится менее определенной, т. к. в ее решении возникают ветвления. В зависимости от численных значений параметров, которыми описывается моделируемая система, может оказаться, что более эффективным решением является как использование двухканальных устройств, так и кластеризация.

Определение граничных условий (пороговых значений значимых параметров системы), позволяющих провести оптимизацию на произвольных наборах исходных данных, которые адекватно отражают реальные задачи управления потоком ТС в городах, является направлением дальнейших исследований. Несмотря на то, что подобные разработки активно ведутся в последние годы [24], выявленные в нашем исследовании новые обстоятельства актуализируют проведение дальнейших изысканий в указанном направлении.

Вторым направлением дальнейших исследований является более глубокое рассмотрение вопросов энергопотребления в различных конфигурациях рассматриваемой системы. В данной публикации эти вопросы изложены в постановочном плане, без учета стоимости энергетических затрат, их пространственного и временного распределения. Между тем, это распределение, в реальных задачах управления дорожным трафиком, может оказаться весьма значимым. Следствием этого может явиться необходимость динамической реконфигурации стационарной части системы, в части формирования состава кластеров.

Список источников

1. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020. White Paper. San Jose: Cisco, 2016.
2. Abbas N., Zhang Y., Taherkordi A., Skeie T. Mobile Edge Computing: A Survey // *IEEE Internet of Things Journal*. 2018. Vol. 5. Iss. 1. PP. 450–465. DOI:10.1109/JIOT.2017.2750180
3. Brehon-Grataloup L., Kacimi R., Beylot A.L. Mobile edge computing for V2X architectures and applications: A survey // *Computer Networks*. 2022. Vol. 206. P. 108797. DOI:10.1016/j.comnet.2022.108797
4. Vladyko A., Khakimov A., Muthanna A., Ateya A.A., Koucheryavy A. Distributed Edge Computing to Assist Ultra-Low-Latency VANET Applications // *Future Internet*. 2019. Vol. 11. Iss. 6. P. 128. DOI:10.3390/fi11060128
5. Vladyko A., Elagin V., Spirkina A., Muthanna A., Ateya A.A. Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications // *Electronics*. 2022. Vol. 11. Iss. 2. P. 173. DOI:10.3390/electronics11020173

6. Плотников П.В., Владыко А.Г. Минимизация задержек при взаимодействии граничных устройств с использованием кластеризации в сетях VANETs // Труды учебных заведений связи. 2022. Т. 8. № 2. С. 6–13. DOI:10.31854/1813-324X-2022-8-2-6-13
7. Аль-Свейти М.А.М., Волков А.Н., Мутханна А.С.А. Проблемы и требования для реализации технологии V2X // Информационные технологии и телекоммуникации. 2020. Т. 8. № 3. С. 20–26. DOI:10.31854/2307-1303-2020-8-3-20-26
8. Dziyaudhin R.A., Niyato D., Luong N.C., Izhar M.A.M., Hadhari M., Daud S. Computation Offloading and Content Caching Delivery in Vehicular Edge Computing: A Survey // Computer Networks. 2021. Vol. 197. P. 108228. DOI:10.1016/j.comnet.2021.108228
9. You C., Huang K., Chae H., Kim B.H. Energy-Efficient Resource Allocation for Mobile-Edge Computation Offloading // IEEE Transactions on Wireless Communications. 2017. Vol. 16. Iss. 3. PP. 1397–1411. DOI:10.1109/TWC.2016.2633522
10. Ren J., Yu G. He Y., Li G.Y. Collaborative Cloud and Edge Computing for Latency Minimization // IEEE Transactions on Vehicular Technology. 2019. Vol. 68. Iss. 5. PP. 5031–5044. DOI:10.1109/TVT.2019.2904244
11. Chen X., Jiao L., Li W., Fu X. Efficient Multi-User Computation Offloading for Mobile-Edge Cloud Computing // IEEE/ACM Transactions on Networking. 2016. Vol. 24. Iss. 5. PP. 2795–2808. DOI:10.1109/TNET.2015.2487344
12. Bernardini C., Silverston T., Festor O. MPC: Popularity-based caching strategy for content centric networks // Proceedings of the International Conference on Communications (ICC, Budapest, Hungary, 09–13 June 2013). IEEE, 2013. PP. 3619–3623. DOI:10.1109/ICC.2013.6655114
13. Perabathini B., Baştuğ E., Kountouris M., Debbah M., Conte A. Caching at the edge: A green perspective for 5G networks // Proceedings of the International Conference on Communication Workshop (ICCW, London, UK, 08–12 June 2015). IEEE, 2015. PP. 2830–2835. DOI:10.1109/ICCW.2015.7247608
14. Mahmood A., Casetti C., Chiasserini C.F., Giaccone P., Harri J. Mobility-aware edge caching for connected cars // Proceedings of the 12th Annual Conference on Wireless On-demand Network Systems and Services (WONS, Cortina d'Ampezzo, Italy, 20–22 January 2016). IEEE, 2016. PP. 1–8.
15. Garetto M., Leonardi E., Traverso S. Efficient analysis of caching strategies under dynamic content popularity // Proceedings of the Conference on Computer Communications (INFOCOM, Hong Kong, China, 26 April 2015–01 May 2015). IEEE, 2015. PP. 2263–2271. DOI:10.1109/INFOCOM.2015.7218613
16. Poularakis K., Iosifidis G., Sourlas V., Tassioulas L. Exploiting Caching and Multicast for 5G Wireless Networks // IEEE Transactions on Wireless Communications. 2016. Vol. 15. Iss. 4. PP. 2995–3007. DOI:10.1109/TWC.2016.2514418
17. Golrezaei N., Molisch A.F., Dimakis A.G., Caire G. Femtocaching and device-to-device collaboration: A new architecture for wireless video distribution // IEEE Communications Magazine. 2013. Vol. 51. Iss. 4. PP. 142–149. DOI:10.1109/MCOM.2013.6495773
18. Abuelenin S.M., Abul-Magd A.Y., Empirical study of traffic velocity distribution and its effect on VANETs connectivity // Proceedings of the International Conference on Connected Vehicles and Expo (ICCVE, Vienna, Austria, 03–07 November 2014). IEEE, 2014. PP. 391–395. DOI:10.1109/ICCVE.2014.7297577
19. Ma J., Wang J., Fan P. A Cooperation-Based Caching Scheme for Heterogeneous Networks // IEEE Access. 2017. Vol. 5. PP. 15013–15020. DOI:10.1109/ACCESS.2016.2644980
20. Torgunakov V., Loginov V., Khorov E. A Study of Channel Bonding in IEEE 802.11bd Networks // IEEE Access. 2022. Vol. 10. PP. 25514–25533. DOI:10.1109/ACCESS.2022.3155814
21. Zhu Z., Zhang M., Hao W. Chapter 6 – Artificial intelligence technology in the Internet of things. Intelligent Sensing and Communications for Internet of Everything. Academic Press; 2022. p.245–297. DOI:10.1016/B978-0-32-385655-3.00010-2
22. Плотников П.В., Тамбовцев Г.И., Владыко А.Г. Программный модуль моделирования взаимодействия граничных устройств в сети VANET. Свидетельство о регистрации программы для ЭВМ № RU 2022669558 от 07.10.2022. Оpubл. 21.10.2022.
23. Торгунаков В.А., Логинов В.А., Хоров Е.М., Ляхов А.И. Алгоритм адаптивного выбора конкурентного окна в сетях IEEE 802.11bd // Информационные процессы. 2022. Т. 22. № 4. С. 373–383. DOI:10.53921/18195822_2022_22_4_373
24. Елькин Д.М., Вяткин В.В. На пути к интернету вещей в управлении транспортными потоками: обзор существующих методов управления дорожным движением // Известия ЮФУ. Технические науки. 2019. № 5. С. 100–113. DOI: 10.23683/2311-3103-2019-5-100-113

References

1. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020. White Paper. San Jose: Cisco; 2016.
2. Abbas N., Zhang Y., Taherkordi A., Skeie T. Mobile Edge Computing: A Survey. IEEE Internet of Things Journal. 2018;5(1): 450–465. DOI:10.1109/JIOT.2017.2750180
3. Brehon-Grataloup L., Kacimi R., Beylot A.L. Mobile edge computing for V2X architectures and applications: A survey. Computer Networks. 2022; Vol. 206:108797. DOI:10.1016/j.comnet.2022.108797
4. Vladiko A., Khakimov A., Muthanna A., Ateya A.A., Koucheryavy A. Distributed Edge Computing to Assist Ultra-Low-Latency VANET Applications. Future Internet. 2019; 11(6):128. DOI:10.3390/fi11060128
5. Vladiko A., Elagin V., Spirkina A., Muthanna A., Ateya A.A. Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications. Electronics. 2022;11(2):173. DOI:10.3390/electronics11020173
6. Plotnikov P., Vladiko A. Minimizing delays in the interaction of edge devices using clustering in VANETs. Proc. of Telecom. Universities. 2022;8(2):6–13. (in Russ.) DOI:10.31854/1813-324X-2022-8-2-6-13
7. Al-Sweity M.A.M., Volkov A., Muthanna A. Challenges and Requirements for Implementing V2X Technology // Telecom IT. 2020;8(3):20–26. (In Russ.) DOI:10.31854/2307-1303-2020-8-3-20-26
8. Dziyaudhin R.A., Niyato D., Luong N.C., Izhar M.A.M., Hadhari M., Daud S. Computation Offloading and Content Caching Delivery in Vehicular Edge Computing: A Survey. Computer Networks. 2021;197:108228. DOI:10.1016/j.comnet.2021.108228
9. You C., Huang K., Chae H., Kim B.H. Energy-Efficient Resource Allocation for Mobile-Edge Computation Offloading. IEEE Transactions on Wireless Communications. 2017;16(3):1397–1411. DOI:10.1109/TWC.2016.2633522

10. Ren J., Yu G. He Y., Li G.Y. Collaborative Cloud and Edge Computing for Latency Minimization. *IEEE Transactions on Vehicular Technology*. 2019;68(5):5031–5044. DOI:10.1109/TVT.2019.2904244
11. Chen X., Jiao L., Li W., Fu X. Efficient Multi-User Computation Offloading for Mobile-Edge Cloud Computing. *IEEE/ACM Transactions on Networking*. 2016;24(5):2795–2808. DOI:10.1109/TNET.2015.2487344
12. Bernardini C., Silverston T., Festor O. MPC: Popularity-based caching strategy for content centric networks. *Proceedings of the International Conference on Communications, ICC, 09–13 June 2013, Budapest, Hungary*. IEEE; 2013. p.3619–3623. DOI:10.1109/ICC.2013.6655114
13. Perabathini B., Baştuğ E., Kountouris M., Debbah M., Conte A. Caching at the edge: A green perspective for 5G networks. *Proceedings of the International Conference on Communication Workshop, ICCW, 08–12 June 2015, London, UK*. IEEE; 2015. p.2830–2835. DOI:10.1109/ICCW.2015.7247608
14. Mahmood A., Casetti C., Chiasserini C.F., Giaccone P., Harri J. Mobility-aware edge caching for connected cars. *Proceedings of the 12th Annual Conference on Wireless On-demand Network Systems and Services, WONS, 20–22 January 2016, Cortina d'Ampezzo, Italy*. IEEE; 2015. p.1–8.
15. Garetto M., Leonardi E., Traverso S. Efficient analysis of caching strategies under dynamic content popularity. *Proceedings of the Conference on Computer Communications, INFOCOM, 26 April 2015–01 May 2015, Hong Kong, China*. IEEE; 2015. p.2263–2271. DOI:10.1109/INFOCOM.2015.7218613
16. Poularakis K., Iosifidis G., Surlas V., Tassioulas L. Exploiting Caching and Multicast for 5G Wireless Networks. *IEEE Transactions on Wireless Communications*. 2016;15(4):2995–3007. DOI:10.1109/TWC.2016.2514418
17. Golrezaei N., Molisch A.F., Dimakis A.G., Caire G. Femtocaching and device-to-device collaboration: A new architecture for wireless video distribution. *IEEE Communications Magazine*. 2013;51(4):142–149. DOI:10.1109/MCOM.2013.6495773
18. Abuelenin S.M., Abul-Magd A.Y., Empirical study of traffic velocity distribution and its effect on VANETs connectivity. *Proceedings of the International Conference on Connected Vehicles and Expo, ICCVE, 03–07 November 2014, Vienna, Austria*. IEEE; 2014. p.391–395. DOI:10.1109/ICCV.2014.7297577
19. Ma J., Wang J., Fan P. A Cooperation-Based Caching Scheme for Heterogeneous Networks. *IEEE Access*. 2017;5:15013–15020. DOI:10.1109/ACCESS.2016.2644980
20. Torgunakov V., Loginov V., Khorov E. A Study of Channel Bonding in IEEE 802.11bd Networks. *IEEE Access*. 2022;10:25514–25533. DOI:10.1109/ACCESS.2022.3155814
21. Zhu Z., Zhang M., Hao W. Chapter 6 – Artificial intelligence technology in the Internet of things. *Intelligent Sensing and Communications for Internet of Everything*. Academic Press; 2022. p.245–297. DOI:10.1016/B978-0-32-385655-3.00010-2
22. Plotnikov P., Tamboltsev G., Vladyko A. Software Module for Modeling the Interaction of Edge Devices in VANET. Patent RF, no 2022669558, 07.10.2022. (in Russ.)
23. Torgunakov V.A., Loginov V.A., Khorov E.M., Lyakhov A.I. Algorithm for adaptive selection of a competitive window in IEEE 802.11bd networks. *Information processes*. 2022;22(4):373–383. (in Russ.) DOI:10.53921/18195822_2022_22_4_373
24. Elkin D.M., Vyatkin V.V. On the way to the Internet of things in traffic management: a review of existing methods of traffic management. *Izvestiya SFU. Technical science*. 2019;5:100–113. DOI:10.23683/2311-3103-2019-5-100-113

Статья поступила в редакцию 30.01.2023; одобрена после рецензирования 13.02.2023; принята к публикации 15.02.2023.

The article was submitted 30.01.2023; approved after reviewing 13.02.2023; accepted for publication 15.02.2023.

Информация об авторах:

ПЛОТНИКОВ
Павел Владимирович

кандидат физико-математических наук, доцент кафедры высшей математики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0001-8869-6142>

ВЛАДЫКО
Андрей Геннадьевич

кандидат технических наук, доцент, декан факультета фундаментальной подготовки Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0002-8852-5607>

Научная статья

УДК 621.3.011.1

DOI:10.31854/1813-324X-2023-9-1-24-33



Математическая модель несимметричного вибратора с вынесенной точкой питания. Часть 1. Общий подход к построению математической модели

- ✉ Олег Вениаминович Попов¹, ov.popov@mail.ru
Андрей Витальевич Тумашов¹, ice47reg@yandex.ru
Георгий Николаевич Борисов¹, georgiiborisov@gmail.com
Константин Олегович Коровин², korovin.ko@sut.ru

¹ООО «Специальный Технологический Центр»,
Санкт-Петербург, 195220, Российская Федерация

²Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация: В работе предложена методика раздельного вычисления реактивной составляющей входного сопротивления, сопротивления излучения и сопротивления потерь малых, по сравнению с длиной волны, нормально разомкнутых антенн. Построена развернутая эквивалентная схема несимметричного вибратора с вынесенной точкой питания. Получены интегральные соотношения, определяющие сопротивление излучения и электродвижущую силу эквивалентного генератора. Разложение активной части входного сопротивления на две составляющие, одна из которых характеризует излучаемую мощность, а другая – тепловые потери, позволяет успешно решать как задачу определения коэффициента согласования по сопротивлению, так и коэффициента полезного действия антенны. Полученные результаты могут быть полезны при проектировании антенн и энергетических расчетах радиолиний.

Ключевые слова: коэффициент трансформации, комплексная емкость, сопротивление излучения, входное сопротивление антенны, несимметричный вибратор

Ссылка для цитирования: Попов О.В., Тумашов А.В., Борисов Г.Н., Коровин К.О. Математическая модель несимметричного вибратора с вынесенной точкой питания. Часть 1. Общий подход к построению математической модели // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 24–33. DOI:10.31854/1813-324X-2023-9-1-24-33

Mathematical Model of the Unbalanced Monopole Feed. Part 1. General Approach to Building a Mathematical Model

- ✉ Oleg Popov¹, ov.popov@mail.ru
Andrey Tumashov¹, ice47reg@yandex.ru
Georgy Borisov¹, georgiiborisov@gmail.com
Konstantin Korovin², korovin.ko@sut.ru

¹Special Technology Center LLC,
St. Petersburg, 195220, Russian Federation

²The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Abstract: *The paper proposes a method for separate calculation of the reactive component of the input impedance, radiation resistance and loss resistance small, in comparison with the wavelength of normally open antennas. A detailed equivalent circuit of the Unbalanced Monopole with Shunt Feed (UMSF). Integral relations are obtained that determine the radiation resistance and the electromotive force of an equivalent generator. The decomposition of the active part of the input resistance into two components, one of which characterizes the radiated power, and the other - thermal losses, allows us to successfully solve both the problem of determining the resistance matching coefficient and the antenna efficiency. The results obtained can be useful in the design of antennas and energy calculations of radio links.*

Keywords: *transformation ratio, complex capacitance, radiation resistance, antenna input impedance, unbalanced monopole*

For citation: Popov O., Tumashov A., Borisov G., Korovin K. Mathematical Model of the Unbalanced Monopole Feed. Part 1. General Approach to Building a Mathematical Model. *Proc. of Telecom. Universities*. 2023;9(1):24–33. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-24-33

Введение

Поскольку в настоящее время математическое моделирование используется для исследования самых разных объектов, процессов и явлений, единого, всеобъемлющего определения математической модели на сегодняшний день не существует. В соответствии с одним из определений, математическая модель – это «эквивалент» объекта, отражающий в математической форме важнейшие его свойства [1]. Применительно к антеннам это определение можно конкретизировать следующим образом: математическая модель представляет собой совокупность аналитических выражений, связывающих геометрические размеры антенны с ее электрическими характеристиками.

В нижней части ВЧ-диапазона и на более низких частотах широко используются антенны, размеры которых много меньше длины волны. При построении математических моделей таких антенн широко используются методы электростатики, позволяющие найти комплексную емкость антенны. Сопротивление комплексной емкости считается входным сопротивлением антенны, несмотря на то, что вещественная составляющая электростатического сопротивления определяется только тепловыми потерями и никак не связана с процессом излучения. Тем не менее, ввиду малости сопротивления излучения, такой подход дает достаточную для практики точность при определении коэффициента согласования антенны с фидерным трактом по сопротивлению. [2–6].

Наряду с коэффициентом согласования по сопротивлению, весьма важной характеристикой антенны, необходимой для энергетического расчета радиолинии, является коэффициент полезного действия (КПД) [2, 3, 7]. Строгое решение задачи о КПД малых антенн сопряжено с серьезными трудностями, обусловленными необходимостью отделения мощности, рассеиваемой токами, наводимыми в полупроводящей земле ближним полем антенны [2–5, 7] от мощности, идущей на создание электромагнитного поля в дальней зоне. Однако, поскольку

точные электрические характеристики подстилающей поверхности, как правило, неизвестны, приближенная оценка КПД в ряде случаев является вполне достаточной. Часто полагают, что входное сопротивление антенны представляет собой последовательное соединение комплексной емкости с сопротивлением излучения [2–4, 8, 9]. Такая модель является физически обоснованной, поскольку при уменьшении частоты сопротивление излучения стремится к нулю, а входное сопротивление – к электростатическому.

Поскольку практически все ВЧ- и более низкочастотные антенны по типу исполнения относятся к проволочным, для построения математической модели малогабаритной нормально разомкнутой антенны необходимо разработать две методики:

- определения комплексной емкости моделируемой антенны;
- вычисления сопротивления излучения малогабаритной нормально разомкнутой проволочной антенны произвольной конструкции.

При этом, если порядок решения первой задачи достаточно подробно освещен в литературе [2, 4, 5, 10, 11], то разработка общего подхода к решению второй представляет практический интерес. В качестве примера малогабаритной нормально разомкнутой проволочной антенны в данной работе рассматривается несимметричный вибратор с вынесенной точкой питания (НВВТП). Его конструкция схематично представлена на рисунке 1.

Сопротивление излучения, как и, практически все характеристики проволочных антенн, связаны с распределением токов по их проводникам [2], которые можно разделить на две группы:

- 1) непосредственно участвующие в процессе излучения (приема) электромагнитных волн (ЭМВ); на рисунке 1 изображены сплошными линиями;
- 2) не излучающие (не принимающие) электромагнитные волны (ЭМВ), но влияющие на распределение токов по излучающим (принимающим) ЭМВ проводникам и, т. образом, влияющие на характеристики антенны (изображены пунктиром).

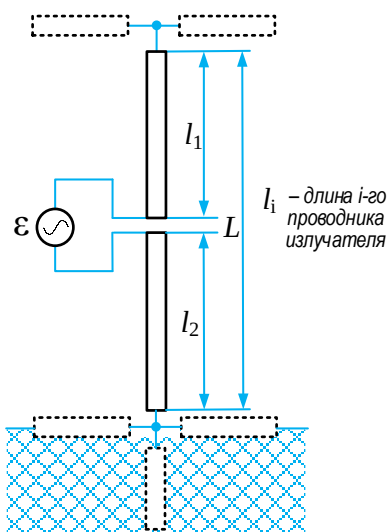


Рис. 1. Схема конструкции НВВТП в общем виде

Fig. 1. General Design of the Unbalanced Monopole with Shunt Feed

Проводники первой группы будем называть излучателем, а второй – корректором распределения тока. В первом приближении можно считать, что поле излучения создается только токами, протекающими по вертикальным проводникам антенны, расположенным в воздухе. Эти проводники образуют излучатель НВВТП. Все остальные проводники образуют корректор распределения тока. Для определения сопротивления излучения можно воспользоваться хорошо зарекомендовавшим себя методом наведенных электродвижущих сил (ЭДС) [2–4], ограничившись рассмотрением только излучателя

НВВТП, но учитывая при этом влияние на распределение тока по излучателю всех остальных проводников и подстилающей поверхности.

Анализ основных закономерностей распределения тока по проводникам излучателя НВВТП

Согласно допущению, принятому в методе наведенных ЭДС, ток, протекающий по проводникам антенны, считается сосредоточенным вдоль осей проводников [2–4]. При этом распределения токов вдоль проводников считаются известными и описываются соотношениями теории линий [4, 8, 9]. Как правило, достаточную точность дает предположение о совпадении распределения токов вдоль проводников антенны с распределением вдоль нагруженной линии без потерь. Согласно работе [4], при совмещении начала координат с точкой пересечения вертикальной осью излучателя НВВТП подстилающей поверхности распределение тока вдоль вертикальных проводников можно представить в виде выражения (1), где $L = l_1 + l_2$ – общая длина излучателя НВВТП; I_a – амплитуда тока на зажимах антенны; $j_{\Sigma}^0(\xi)$ – безразмерная функция распределения тока по излучателю НВВТП, нормированная к току на зажимах I_a ; $k = 2\pi/\lambda$ – волновое число; λ – длина волны; l_i – длина i -го проводника; ξ – вертикальная координата; $\hat{Z}_{hi} = Z_{hi}/\rho_i$ – нагрузка на конце i -го проводника, нормированная к его волновому сопротивлению; Z_{hi} – нагрузка на конце i -го проводника:

$$I(\xi) = I_a j_{\Sigma}^0(\xi) = I_a \begin{cases} \frac{\cos k(L - \xi) + i \hat{Z}_{h1} \sin k(L - \xi)}{\cos k l_1 + i \hat{Z}_{h1} \sin k l_1} & l_2 \leq \xi \leq L \\ \frac{\cos k \xi + i \hat{Z}_{h2} \sin k \xi}{\cos k l_2 + i \hat{Z}_{h2} \sin k l_2} & 0 \leq \xi \leq l_2 \end{cases} \quad (1)$$

Волновые сопротивления проводников излучателя НВВТП определяются через погонную статическую емкость, рассчитываемую по методу среднего потенциала, и описываются выражениями, приведенными в [4], где a_i – радиус i -го проводника:

$$\rho_1 = 60 \left[\ln \frac{l_1}{a_1} - 1 - \frac{L + l_2}{l_2} \ln \frac{L}{L + l_2} \right],$$

$$\rho_2 = 60 \left\{ \ln \frac{l_2}{a_2} - 1 - \frac{1}{2} \left[\left(1 - \frac{l_2}{l_1} \right) \ln \frac{L}{L + l_2} - \frac{l_2}{l_1} \ln \frac{4l_2}{L + l_2} \right] \right\}.$$

Легко заметить, что распределение тока по каждому проводнику излучателя описывается двумя вещественными гармоническими функциями. Будем в дальнейшем называть эти функции базовыми, а токи с единичной амплитудой в пучности, распределенные по закону базовой функции – базовыми токами (БТ).

Соотношение (1) можно представить в более компактном виде:

$$j_{\Sigma}^0(\xi_k) = \begin{cases} j_1^0(\xi_k) = n_{c1} j_{c1}^0(\xi_k) + n_{s1} j_{s1}^0(\xi_k) & l_{k2} \leq \xi_k \leq L_k \\ j_2^0(\xi_k) = n_{c2} j_{c2}^0(\xi_k) + n_{s2} j_{s2}^0(\xi_k) & 0 \leq \xi_k \leq l_{k2} \end{cases} \quad (2)$$

где

$$n_{ci} = \frac{1}{\cos kl_i + i \hat{Z}_{hi} \sin kl_i}, \quad (3)$$

$$n_{si} = i \frac{\hat{Z}_{hi}}{\cos kl_i + i \hat{Z}_{hi} \sin kl_i}, \quad (4)$$

$$j_{c1}^0(\xi_k) = \begin{cases} 0 & 0 \leq \xi_k \leq l_{k2} \\ \cos(L_k - \xi_k) & l_{k2} \leq \xi_k \leq L_k \end{cases}, \quad (5)$$

$$j_{s1}^0(\xi_k) = \begin{cases} 0 & 0 \leq \xi_k \leq l_{k2} \\ \sin(L_k - \xi_k) & l_{k2} \leq \xi_k \leq L_k \end{cases}, \quad (6)$$

$$j_{c2}^0(\xi_k) = \begin{cases} \cos(\xi_k) & 0 \leq \xi_k \leq l_{k2} \\ 0 & l_{k2} \leq \xi_k \leq L_k \end{cases}, \quad (7)$$

$$j_{s2}^0(\xi_k) = \begin{cases} \sin(\xi_k) & 0 \leq \xi_k \leq l_{k2} \\ 0 & l_{k2} \leq \xi_k \leq L_k \end{cases}. \quad (8)$$

В соотношениях (2–8) введены обозначения: $j_i^0(\xi_k)$ – функция распределения тока по i -му проводнику излучателя НВВТП; $j_{c1}^0(\xi_k)$, $j_{s1}^0(\xi_k)$, $j_{c2}^0(\xi_k)$, $j_{s2}^0(\xi_k)$ – базовые функции; n_{ci} – коэффициент трансформации тока на зажимах (КТТЗ) НВВТП к косинусному БТ i -го проводника излучателя; n_{si} – КТТЗ НВВТП к синусному БТ i -го проводника излучателя; $L_k = kL$ – суммарная электрическая длина проводников излучателя НВВТП; $l_{ki} = kl_i$ – электрическая длина i -го проводника излучателя НВВТП; $\xi_k = k\xi$ – электрическая координата точки наблюдения.

В выражениях (2–8) геометрические размеры, с целью сокращения числа параметров, заменены электрическими, измеряемыми в радианах.

Из (3) и (4) видно, что КТТЗ к БТ, в общем случае, являются комплексными величинами. Кроме того, легко заметить, что при $\xi_k = l_{k2}$ из соотношений (2–8) следует:

$$j_i^0(l_{k2}) = n_{ci} \cos l_{ki} + n_{si} \sin l_{ki} = 1. \quad (9)$$

Из (9) можно сделать вывод, что функция распределения тока по излучателю НВВТП $j_{\Sigma}^0(\xi_k)$ обладает двумя важными свойствами: сохраняет непрерывность в точке питания НВВТП; из четырех КТТЗ к БТ, введенных в (2), независимыми являются только два, т. к. из (9) следует:

$$n_{si} = \frac{1 - n_{ci} \cos l_{ki}}{\sin l_{ki}}. \quad (10)$$

Таким образом, распределение токов по излучателю НВВТП, в общем случае полностью определяется двумя комплексными числами, т. е. в каждом плече излучателя НВВТП должен быть известен хотя бы один КТТЗ к БТ. Для их определения требуется выявить связь КТТЗ с конструктивным исполнением антенны. Решение этой задачи следует начать с установления связи между входным сопротивлением неизлучающего НВВТП и функцией распределения тока по излучателю.

Поскольку распределения токов в проводниках излучателя совпадают с распределениями в нагруженных линиях передачи без потерь, каждому проводнику можно поставить в соответствие такую линию. При этом входное сопротивление неизлучающего НВВТП будет представлять собой последовательное соединение двух нагруженных линий [4].

$$Z_{\text{вх}} = Z_{\text{вх1}} + Z_{\text{вх2}}, \quad (11)$$

где $Z_{\text{вх1}}$, $Z_{\text{вх2}}$ – входные сопротивления линий, соответствующие, соответственно, верхнему и нижнему проводнику излучателя НВВТП.

Входные сопротивления нагруженных линий без потерь будут [12, 13]:

$$Z_{\text{вх}i} = \rho_i \frac{\hat{Z}_{hi} \cos l_{ki} + i \sin l_{ki}}{\cos l_{ki} + i \hat{Z}_{hi} \sin l_{ki}}. \quad (12)$$

Легко заметить, что, если конечные нагрузки будут чисто мнимыми или будут отсутствовать ($\hat{Z}_{hi} \rightarrow \infty$), входное сопротивление, определяемое соотношениями (11, 12), будет чисто мнимым. Это объясняется тем, что при их выводе проводники излучателя описываются линиями без потерь. Такой прием обычно используется для определения реактивной составляющей входного сопротивления диполя [2–4, 8, 9, 12]. Затем к реактивной составляющей добавляется сопротивление излучения, найденное иным способом. Применительно к НВВТП, соотношения (11) и (12), несмотря на то, что не содержат сопротивления излучения, будут комплексными, поскольку характеризуют не только запасаемую энергию, а и тепловые потери в полупроводящей подстилающей поверхности.

Соотношения (3) и (4) совместно с (12) позволяют установить связь между входным сопротивлением i -го проводника излучателя и соответствующими КТТЗ к БТ:

$$Z_{\text{вх}i} = -i \rho_i n_{si} \cos l_{ki} + i \rho_i n_{ci} \sin l_{ki}. \quad (13)$$

Так как КТТЗ связаны между собой соотношением (10), выражение (13) можно преобразовать к виду:

$$Z_{\text{вх}i} = -i \rho_i \frac{\cos l_{ki} - n_{ci}}{\sin l_{ki}}. \quad (14)$$

Подставляя (14) в (11), получим:

$$Z_{\text{вх}} = -i \left(\rho_1 \frac{\cos l_{k1} - n_{c1}}{\sin l_{k1}} + \rho_2 \frac{\cos l_{k2} - n_{c2}}{\sin l_{k2}} \right). \quad (15)$$

Если НВВТП не содержит верхней нагрузки, то $Z_{\text{н1}} \rightarrow \infty$. Легко заметить, что в этом случае из (3) следует, что $n_{c1} = 0$. В этом случае (15) преобразуется к виду:

$$Z_{\text{вх}}^0 = -i \left(\rho_1 \text{ctgl}_{k2} + \rho_2 \text{ctgl}_{k2} - |n_{c2}| \rho_2 \frac{\cos \phi_{c2}}{\sin l_{k2}} \right) - |n_{c2}| \rho_2 \sin \phi_{c2} / \sin l_{k2}, \quad (16)$$

где $Z_{\text{вх}}^0$ – входное сопротивление НВВТП без верхней нагрузки; $|n_{c2}|$ и ϕ_{c2} – модуль и аргумент КТТЗ к косинусному БТ нижнего плеча НВВТП, соответственно.

Входное сопротивление неизлучающего НВВТП можно трактовать как сопротивление комплексной емкости. Комплексная емкость двух изолированных групп проводников, имеющих между собой электрический контакт, определяется с помощью методик, изложенных в [2, 4, 10, 11, 14, 15].

Пусть $\tilde{C}_0$ – комплексная емкость НВВТП без верхней нагрузки, определенная электростатическим методом. Тогда:

$$Z_{\text{вх}}^0 = \frac{1}{i\omega \tilde{C}_0} = R_c^0 + i X_c^0, \quad (17)$$

где

$$R_c^0 = -\text{Im}(\tilde{C}_0) / (\omega |\tilde{C}_0|^2), \quad (18)$$

$$X_c^0 = -\text{Re}(\tilde{C}_0) / (\omega |\tilde{C}_0|^2). \quad (19)$$

Соотношения (17–19) преобразовывают (16) в систему уравнений, определяющую модуль и аргумент коэффициента трансформации n_{c2} .

Приравнивая вещественные и мнимые части соотношений (16) и (17), получим:

$$|n_{c2}| \sin \phi_{c2} = -\frac{\sin l_{k2}}{\rho_2} R_c^0, \quad (20)$$

$$|n_{c2}| \cos \phi_{c2} = \frac{\sin l_{k2}}{\rho_2} [\rho_1 \text{ctgl}_{k1} + \rho_2 \text{ctgl}_{k2} + X_c^0]. \quad (21)$$

Легко показать, что решение системы будет:

$$\phi_{c2} = \arctg \frac{-R_c^0}{\rho_1 \text{ctgl}_{k1} + \rho_2 \text{ctgl}_{k2} + X_c^0}, \quad (22)$$

$$|n_{c2}| = \frac{\sin l_{k2}}{\rho_2} \sqrt{[\rho_1 \text{ctgl}_{k1} + \rho_2 \text{ctgl}_{k2} + X_c^0]^2 + (R_c^0)^2}. \quad (23)$$

Таким образом, при отсутствии верхней нагрузки распределение тока по проводникам излучателя НВВТП полностью определяется соотношениями (2), (17), (22), (23) и (10).

Если НВВТП содержит верхнюю нагрузку, то $n_{c1} \neq 0$. В этом случае, как следует из (15), справедливо соотношение:

$$Z_{\text{вх}} - Z_{\text{вх}}^0 = i n_{c1} \rho_1 / \sin l_{k1}, \quad (24)$$

где $Z_{\text{вх}}$ – входное сопротивление неизлучающего НВВТП с верхней нагрузкой.

Очевидно, что $Z_{\text{вх}}$ можно рассматривать как сопротивление комплексной емкости НВВТП с верхней нагрузкой. В этом случае:

$$Z_{\text{вх}} = \frac{1}{i\omega \tilde{C}} = R_c + i X_c, \quad (25)$$

где $R_c = -\text{Im}(\tilde{C}) / (\omega |\tilde{C}|^2)$; $X_c = -\text{Re}(\tilde{C}) / (\omega |\tilde{C}|^2)$; $\tilde{C}$ – комплексная емкость НВВТП с верхней нагрузкой.

Подставляя в (24) соотношения (17) и (25) и приравнивая вещественные и мнимые части, получим систему уравнений:

$$\left. \begin{aligned} |n_{c1}| \sin \phi_{c1} &= -\frac{\sin l_{k1}}{\rho_1} (R_c - R_c^0) \\ |n_{c1}| \cos \phi_{c1} &= \frac{\sin l_{k1}}{\rho_1} (X_c - X_c^0) \end{aligned} \right\} \quad (26)$$

Решение системы (26), будет:

$$\phi_{c1} = \arctg \frac{R_c^0 - R_c}{X_c - X_c^0}, \quad (27)$$

$$|n_{c1}| = \frac{\sin l_{k1}}{\rho_1} \sqrt{(R_c - R_c^0)^2 + (X_c - X_c^0)^2}. \quad (28)$$

Соотношения (22, 23, 27, 28) совместно с (10) и (2) описывают распределение тока по проводникам излучателя НВВТП с учетом как конструктивных особенностей, так и параметров подстилающей поверхности.

В таблице 1 приведены значения комплексной емкости НВВТП при $l_1 = l_2 = 1$ м, $\lambda = 100$ м, $\varepsilon = 4$, $\sigma = 0,01$ см/м. Радиусы проводников: излучателя – 50 мм; верхней нагрузки – 4 мм; противовесов – 2 мм. Длина заземлителя: 0,4 м. Число проводников как нагрузки, так и противовесов равно шести.

ТАБЛИЦА 1. Комплексная емкость НВВТП [Ф]

ТАБЛИЦА 1. Complex capacity of UMSF [Ф]

Длины противовесов (м)	Длины проводников верхней нагрузки (м)		
	0	0,5	1
0	$1,76 \cdot 10^{-11} - i5,09 \cdot 10^{-13}$	$3,072 \cdot 10^{-11} - i1,813 \cdot 10^{-12}$	$5,008 \cdot 10^{-11} - i5,139 \cdot 10^{-12}$
3	$1,743 \cdot 10^{-11} - i2,457 \cdot 10^{-13}$	$3,014 \cdot 10^{-11} - i8,608 \cdot 10^{-13}$	$4,865 \cdot 10^{-11} - i2,38 \cdot 10^{-12}$

На рисунке 2 представлены модули функций распределения тока по проводникам излучателя при различных длинах проводников нагрузки L_A и противовесов L_D .

Видно, что верхняя нагрузка НВВТП существенно выравнивает распределение тока по верхнему проводнику излучателя. Влияние противовесов на функцию распределения тока при установке НВВТП на влажной почве незначительно, однако противовесы, как видно из таблицы 1, существенно снижают уровень тепловых потерь (мнимую составляющую комплексной емкости).

Поскольку, как установлено, распределение тока по излучателю НВВТП, в общем случае, представляет собой линейную комбинацию четырех базовых токов, разработку методики расчета сопротивления излучения следует начать с оценки их взаимного влияния и построения развернутой схемы НВВТП.

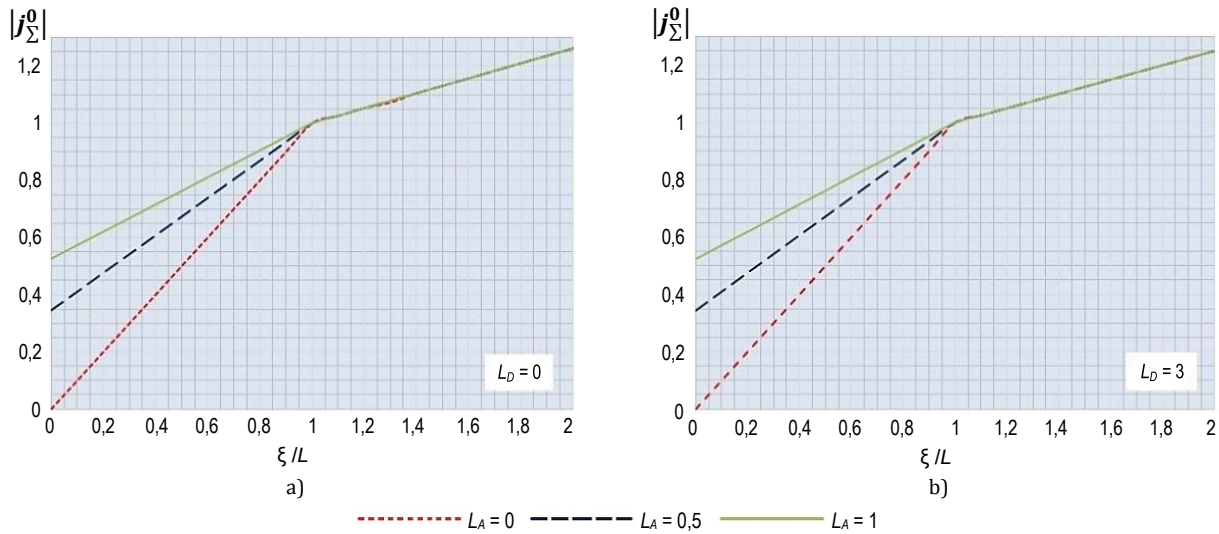


Рис. 2. Модуль функции распределения тока по излучателю НВВТП для а) $L_D = 0$ и б) $L_D = 3$
 Fig. 2. Absolute Value of the Current Distribution Function over UMSF element а) $L_D = 0$ and б) $L_D = 3$

Построение развернутой эквивалентной схемы НВВТП

Сопротивление излучения любой проволочной антенны определяется распределением токов по проводникам, участвующим в процессе излучения ЭМВ. Установить связь между сопротивлением излучения и функцией распределения тока можно, воспользовавшись методом наведенных ЭДС [2–4, 16–19 и др.], в основе которого лежит теорема Пойнтинга. Согласно этой теореме, мощность, выделяемая в объеме V , ограниченном замкнутой поверхностью S , определяется [2, 3, 12, 20]:

$$P_a = \frac{1}{2} \int_V \frac{|\bar{j}|^2}{\sigma} dV + \frac{i\omega}{2} \times \times \int_V [\mu_a |\bar{H}|^2 - \varepsilon_a |\bar{E}|^2] dV + \frac{1}{2} \oint_S [\bar{E} \bar{H}^*] \bar{n} dS, \quad (29)$$

где $\bar{j}$ – вектор плотности тока; $\bar{E}$ – напряженность электрического поля, созданного в объеме V ; $\bar{H}$ – напряженность магнитного поля, созданного в объеме V ; $\bar{n}$ – единичный вектор внешней нормали к поверхности S ; σ – удельная проводимость среды.

Первое слагаемое в правой части уравнения (29) определяет мощность тепловых потерь в объеме V . Второе слагаемое есть умноженная на $i\omega$ разность между усредненными за период колебания энергиями магнитного и электрического полей. Третье слагаемое представляет собой мощность, выносимую за пределы объема V .

Пусть поверхность S совпадает с поверхностью проводников излучателя НВВТП. Тогда, если эти проводники идеальные, тепловые потери и запасенная в объеме V энергия будут отсутствовать, а выделяемая в нем мощность будет равна мощно-

сти, передаваемой антенной в фидерный тракт. Соотношение (30) в этом случае можно представить в виде:

$$\frac{1}{2} U_{\text{фТ}} I_{\text{фТ}}^* = \frac{1}{2} \oint_S [\bar{E} \bar{H}^*] \bar{n} dS, \quad (30)$$

где $U_{\text{фТ}}$ – напряжение на входе фидерного тракта; $I_{\text{фТ}}$ – ток на входе фидерного тракта.

Воспользовавшись правилом перестановки смешанного произведения векторов, и считая, что вся энергия за пределы объема V выносится через боковые поверхности, получим:

$$U_{\text{фТ}} I_{\text{фТ}}^* = \oint_S [\bar{H}^* \bar{n}] \bar{E} dS = - \int_0^{l_2} \int_0^{2\pi} \bar{J}_2^*(\varphi, z) \bar{E}_2 a_2 d\varphi dz - \int_{l_2}^L \int_0^{2\pi} \bar{J}_1^*(\varphi, z) \bar{E}_1 a_1 d\varphi dz, \quad (31)$$

где $\bar{J}_i(\varphi, z)$ – распределение поверхностной плотности тока по i -му проводнику; $\bar{E}_i$ – напряженность электрического поля на поверхности i -го проводника; a_i – радиус i -го проводника.

В (31) учтено, что на идеально проводящей поверхности справедливо соотношение [12, 18, 20]:

$$[\bar{H}^* \bar{n}] = -\bar{J}^*. \quad (32)$$

Если вектор напряженности магнитного поля в выражении (31) содержит только φ -ю составляющую, то $\bar{J}_i^*(\varphi, z) = J_i^*(\varphi, z) \bar{z}^0$. Следовательно, считая, что напряженность электрического поля в поперечном сечении проводника постоянна, после интегрирования выражения (31) по φ получим:

$$U_{\Phi T} I_{\Phi T}^* = -\frac{1}{k} \int_0^{l_{k2}} I_2^*(z_k) \bar{E}_2 \bar{z}^0 dz_k - \frac{1}{k} \int_{l_{k2}}^{L_k} I_1^*(z_k) \bar{E}_1 \bar{z}^0 dz_k. \quad (33)$$

В выражении (33) введена новая переменная $z_k = kz$, а также учтено, что:

$$\int_0^{2\pi} \bar{J}_i^*(\phi, z) a_i d\phi = \left[\int_0^{2\pi} J_i^*(\phi, z) a_i d\phi \right] \bar{z}^0 = I_i^*(z) \bar{z}^0, \quad (34)$$

где $I_i(z)$ – распределение тока по длине i -го проводника излучателя НВВТП.

Как следует из (1) и (2), функцию $I_i(z_k)$ в выражении (33) можно представить в виде:

$$I_i(z_k) = I_a [n_{ci} j_{ci}^0(z_k) + n_{si} j_{si}^0(z_k)]. \quad (35)$$

Напряженности электрических полей на поверхностях проводников излучателя НВВТП можно представить в виде суммы [12]:

$$\bar{E}_i = \bar{E}_0 e^{-i \bar{k} \bar{r}_i} + \bar{E}_i \{ I_1(\xi) \} + \bar{E}_i \{ I_2(\xi) \}, \quad (36)$$

где $\bar{E}_0 e^{-i \bar{k} \bar{r}_i}$ – напряженность поля приходящей плоской волны на поверхности i -го проводника;

$\bar{k} = 2\pi \bar{n}_b / \lambda$ – волновой вектор приходящей волны; $\bar{n}_b$ – нормаль к фронту приходящей плоской волны, совпадающая с направлением распространения; $\bar{r}_i$ – радиус-вектор точки наблюдения находящейся на поверхности i -го проводника; $\bar{E}_i \{ \}$ – линейный интегро-дифференциальный оператор, определяющий напряженность электрического поля на поверхности i -го проводника, создаваемую током, указанным в скобках $\{ \}$; $\bar{E}_i \{ I_1(\xi) \}$, $\bar{E}_i \{ I_2(\xi) \}$ – напряженности поля на поверхности i -го проводника, создаваемые током, протекающим по оси верхнего и нижнего плеча излучателя НВВТП, соответственно.

Поскольку напряжение на входе фидерного тракта связано с его входным сопротивлением соотношением:

$$U_{\Phi T} = I_{\Phi T} Z_{\Phi T} = -I_a Z_{\Phi T}. \quad (37)$$

Формулу (33) с учетом (35–37) можно записать в виде выражения (38), где $p = c1, s1, c2, s2$ – обобщенный индекс базовой функции; $\bar{r}_0$ – радиус-вектор точки пересечения оси излучателя НВВТП с горизонтальной плоскостью, проходящей через середину зазора между смежными торцами верхнего и нижнего проводников; $\int_{l_{ki}}$ – означает интегрирование по длине i -го проводника;

$$i = \begin{cases} 1 & \text{при } p = c1, s1; \\ 2 & \text{при } p = c2, s2 \end{cases}.$$

$$\begin{aligned} -I_a Z_{\Phi T} &= \frac{1}{k} \sum_{v=c,s} \sum_{i=1,2} \left[n_{vi}^* \bar{E}_0 e^{-i \bar{k} \bar{r}_0} \bar{z}^0 \int_{l_{ki}} j_{vi}^0(z_k) e^{-i \bar{k} (\bar{r}_i - \bar{r}_0)} dz_k + \right. \\ &\quad \left. + I_a n_{vi}^* \sum_{v'=c,s} \sum_{i'=1,2} n_{v'i'} \int_{l_{ki}} j_{vi}^0(z_k) \bar{E}_i \{ j_{v'i'}^0(z_k) \} \bar{z}^0 dz_k \right] = \\ &= \frac{1}{k} \sum_p n_p^* \left[\bar{E}_0 e^{-i \bar{k} \bar{r}_0} \bar{z}^0 \int_{l_{ki}} j_p^0(z_k) e^{-i \bar{k} (\bar{r}_i - \bar{r}_0)} dz_k + I_a \sum_{p'} n_{p'} \int_{l_{ki}} j_p^0(z_k) \bar{E}_i \{ j_{p'}^0(z_k) \} \bar{z}^0 dz_k \right] \end{aligned} \quad (38)$$

Учитывая размерность интегралов в (38), обозначим:

$$\varepsilon_p = -\frac{1}{k} \bar{E}_0 e^{-i \bar{k} \bar{r}_0} \bar{z}^0 \int_{l_{ki}} j_p^0(z_k) e^{-i \bar{k} (\bar{r}_i - \bar{r}_0)} dz_k, \quad (39)$$

$$z_{p p'} = \frac{1}{k} \int_{l_{ki}} j_p^0(z_k) \bar{E}_i \{ j_{p'}^0(z_k) \} \bar{z}^0 dz_k, \quad (40)$$

где ε_p – ЭДС базового тока p ; $z_{p p'} = r_{p p'} + i x_{p p'}$ – взаимное сопротивление базового тока $p p'$.

С учетом сделанных обозначений, соотношение (38) можно представить следующим образом:

$$\varepsilon = I_a (Z_{\Phi T} + Z_{ii}), \quad (41)$$

где

$$\varepsilon = \sum_p n_p^* \varepsilon_p \quad (42)$$

$$Z_{ii} = \sum_p \sum_{p'} n_p^* n_{p'} z_{p p'}, \quad (43)$$

ε – ЭДС эквивалентного генератора НВВТП; Z_{ii} – входное сопротивление излучателя НВВТП.

Соотношения (42) и (43) в ряде случаев удобно представить в матричном виде:

$$\varepsilon = \langle N^* \varepsilon_{BT} \rangle, \quad (44)$$

$$Z_{ii} = \langle N^* | Z_{BT} | N \rangle, \quad (45)$$

где $\langle N^* = |n_{c1}^* n_{s1}^* n_{c2}^* n_{s2}^*|$ – комплексно-сопряженная матрица-строка КТТЗ к БТ; ϵ_{BT} – матрица-столбец ЭДС БТ; $|Z_{BT}|$ – матрица взаимных сопротивлений БТ.

Следует отметить, что сопротивление Z_{ii} получено путем анализа закона сохранения энергии в объеме проводников излучателя НВВТП. Поскольку при этом считалось, что тепловые потери в проводниках отсутствуют, активная составляющая этого сопротивления является сопротивлением излучения и никак не связана с тепловыми потерями в подстилающей поверхности.

Учитывая, что из теоремы взаимности следует:

$$Z_{pp'} = Z_{p'p},$$

соотношения (43) и (45) в развернутом виде будут:

$$\begin{aligned} Z_{ii} = & |n_{c1}|^2 z_{c1c1} + |n_{s1}|^2 z_{s1s1} + |n_{c2}|^2 z_{c2c2} + \\ & + |n_{s2}|^2 z_{s2s2} + (n_{c1}^* n_{s1} + n_{c1} n_{s1}^*) z_{c1s1} + \\ & + (n_{c1}^* n_{c2} + n_{c1} n_{c2}^*) z_{c1c2} + \\ & + (n_{c1}^* n_{s2} + n_{c1} n_{s2}^*) z_{c1s2} + \\ & + (n_{s1}^* n_{c2} + n_{s1} n_{c2}^*) z_{s1c2} + \\ & + (n_{s1}^* n_{s2} + n_{s1} n_{s2}^*) z_{s1s2} + \\ & + (n_{c2}^* n_{s2} + n_{c2} n_{s2}^*) z_{c2s2}. \end{aligned} \quad (46)$$

Видно, что сопротивление излучателя представляет собой сумму всех взаимных сопротивлений базовых токов, умноженных на вещественные числа. Это значит, что сопротивление излучения

определяется только вещественными составляющими взаимных базовых токов:

$$R_{\Sigma} = \text{Re}(Z_{ii}) = \sum_p \sum_{p'} n_p^* n_{p'} r_{pp'}. \quad (47)$$

Соотношение (47) можно представить в матричной форме:

$$R_{\Sigma} = \langle N^* \text{Re} | Z_{BT} | N \rangle = \langle N^* | R_{BT} | N \rangle, \quad (48)$$

где $|R_{BT}|$ – вещественная составляющая матрицы $|Z_{BT}|$.

Как известно [2, 3, 16, 17, 19, 21], приемная антенна представляет собой эквивалентный генератор, характеризующийся ЭДС и внутренним сопротивлением. Входное сопротивление малых по сравнению с длиной волны антенн, как указывалось ранее, фактически является последовательным соединением комплексной емкости с сопротивлением излучения. Комплексная емкость характеризует реактивную составляющую входного сопротивления и тепловые потери. Сопротивление излучения в этом случае должно совпадать с внутренним сопротивлением эквивалентного генератора ЭДС. Эквивалентная схема НВВТП, представленная таким образом, изображена на рисунке 3а. Для доказательства чистоты активного характера внутреннего сопротивления эквивалентного генератора на рис. 3б представлена эквивалентная схема излучателя в развернутом виде, иллюстрирующем соотношение (44) и (48).

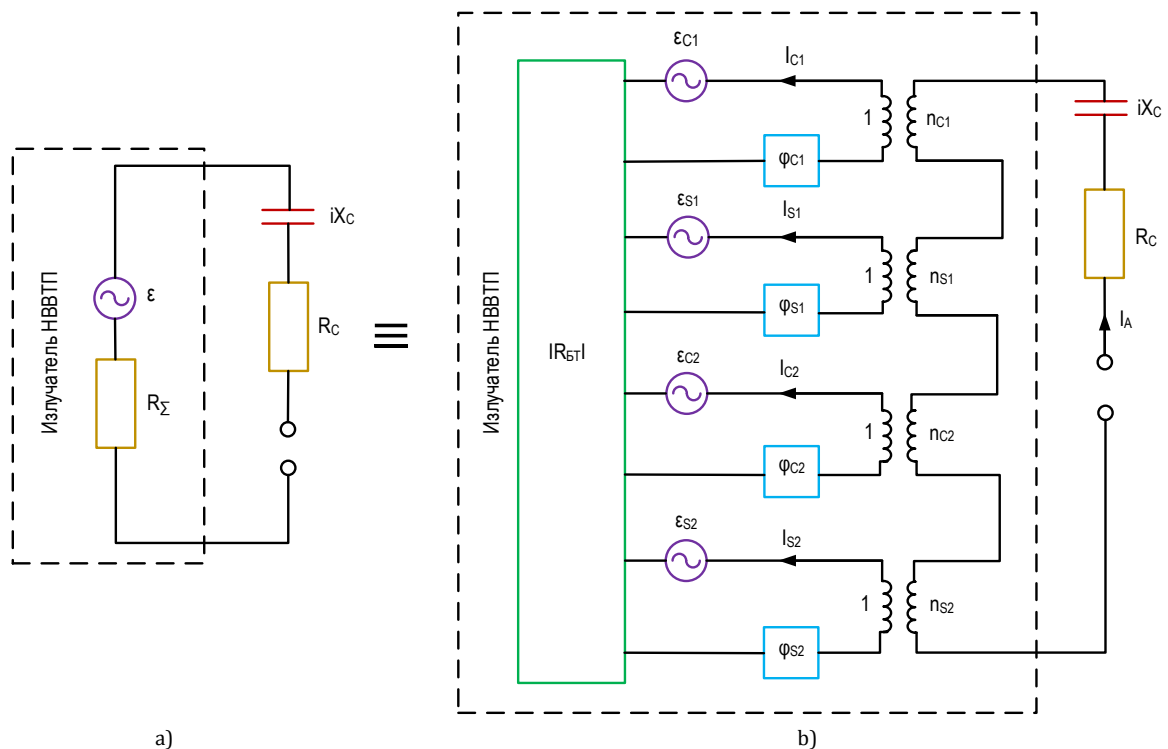


Рис. 3. Эквивалентные схемы НВВТП

Fig. 3. Equivalent Circuits of UMSF

Каждому БТ на рисунке 3b поставлен в соответствие эквивалентный генератор ЭДС ε_p . Внутренним сопротивлением всех эквивалентных генераторов служит восьмиполюсник, описываемый матрицей взаимных сопротивлений, состоящей из активных элементов. Численные значения этих элементов определяются интегро-дифференциальным соотношением (40). Комплексным коэффициентам трансформации на развернутой эквивалентной схеме поставлены в соответствие идеальные трансформаторы в совокупности с фазовращателями. Входные зажимы трансформаторов соединены последовательно, преобразуя активный эквивалентный восьмиполюсник в эквивалентный генератор ЭДС, параметры которого связаны с параметрами развернутой эквивалентной схемы соотношениями (44) и (48).

Как следует из эквивалентной схемы, входное сопротивление НВВТП будет:

$$Z_a = R_\Sigma + R_c + i X_c. \quad (49)$$

Легко заметить, что практически все параметры развернутой эквивалентной схемы в той или иной степени связаны с комплексной емкостью НВВТП. Таким образом, первоочередной задачей при построении математической модели НВВТП является установление связи между геометрическими раз-

мерами антенны и ее комплексной емкостью с учетом электрических параметров подстилающей поверхности.

Заключение

В конструкции НВВТП выделены проводники, непосредственно участвующие в создании ЭМП в дальней зоне. Показано, что ток, протекающий по этим проводникам, является линейной комбинацией четырех токов, распределенных по гармоническому закону. Эти элементарные токи предложено называть базовыми. Получены аналитические выражения, связывающие амплитуды БТ с комплексной емкостью НВВТП. Показано, что сопротивление излучения определяется вещественными составляющими матрицы взаимных сопротивлений эквивалентного восьмиполюсника с БТ на входах. Получены интегральные соотношения, определяющие элементы этой матрицы. Построена развернутая эквивалентная схема НВВТП и показано, что для построения математической модели достаточно преобразования интегральных соотношений к виду, пригодному для инженерных расчетов.

Установлено, что одним из важнейших параметров малых, по сравнению с длиной волны антенн является комплексная емкость, что делает задачу ее определения одной из главных при разработке математических моделей.

Список источников

1. Самарский А.А., Михайлов А.А. Математическое моделирование: Идеи. Методы. Примеры. М.: Физматлит, 2001. 320 с.
2. Гавеля Н.П., Истрашкин А.Д., Муравьев Ю.К., Серков В.П. Антенны. Ч. I. Л.: ВКАС, 1963. 633 с.
3. Серков В.П. Распространение радиоволн и антенные устройства. Л.: ВАС, 1981.
4. Муравьев Ю.К. Справочник по расчету проволочных антенн. Л.: ВАС, 1978.
5. Бесчастнов Н.С., Конторович М.И. О потерях в земле при использовании корпуса передатчика в качестве противовеса // Труды ВКАС. 1944. № 3.
6. Конторович М.И. О расчете емкости антенны по методу Хоу // Труды ВКАС. 1943. № 2.
7. Калинин А.И., Черенкова Е.Л. Распространение радиоволн и работа радиолиний. М.: Связь, 1971. 439 с.
8. Зернов Н.В., Карпов В.Г. Теория радиотехнических цепей. Л.: Энергия: Ленингр. отд-ние, 1972. 816 с.
9. Корбанский И.Н. Антенны: учебное пособие для вузов. М.: Энергия, 1973. 363 с.
10. Русин Ю.С. Метод приближенного расчета электрической емкости // Электричество. 1960. № 11. С. 48.
11. Иосель Ю.Я., Кочанов Э.С., Струнский М.Г. Расчет электрической емкости. Л.: Энергоиздат: Ленингр. отд-ние, 1981. 288 с.
12. Емелин Б.Ф. Нерегулярные волноводы и резонаторы. Л.: ВКАС, 1959. 219 с.
13. Белецкий А.Ф. Основы теории линейных электрических цепей. М.: Связь, 1967. 608 с.
14. Фихманас Р.Ф., Фридберг П.Ш. Метод Хоу расчета емкости тел и его связь с вариационными принципами // Журнал технической физики. 1970. Т. 40.
15. Попов О.В., Тумашов А.В., Борисов Г.Н. Методика расчета сопротивления потерь заземленных несимметричных вибраторов с вынесенной точкой питания // Успехи современной радиоэлектроники. 2021. Т. 75. № 4. С. 71-79.
16. Вершков М.В. Судовые антенны. Л.: Судостроение, 1972. 424 с.
17. Фрадин А.З. Антенно-фидерные устройства: учебн. пособие для вузов связи. М.: Связь, 1977. 440 с.
18. Кисунько Г.В. Электродинамика полых систем. Л.: ВКАС, 1949. 424 с.
19. Марков Г.Т., Чаплин А.Ф. Возбуждение электромагнитных волн. М.: Радио и связь, 1983. 295 с.
20. Гольдштейн Л.Д., Зернов Н.В. Электромагнитные поля и волны. М.: Изд-во «Советское радио», 1971.
21. Белоцерковский Г.Б. Антенны. М.: Государственное научно-техническое издательство ОБОРОНГИЗ, 1962.

References

1. Samarsky A.A., Mikhailov A.A. *Math Modeling: Ideas. Methods. Examples*. Moscow: Fizmatlit Publ.; 2001. 320 p. (in Russ.)
2. Gavelya N.P., Istrashkin A.D., Muravyov Yu.K. *Antennas. Part I*. Leningrad: Military Academy of Communications Publ.; 1963. 633 p. (in Russ.)

3. Serkov V.P. *Radio Wave Propagation and Antenna Devices*. Leningrad: Military Academy of Telecommunications Publ.; 1981. (in Russ.)
4. Muravyov Yu.K. *Handbook for the Calculation of Wire Antennas*. Leningrad: Military Academy of Telecommunications Publ.; 1978. (in Russ.)
5. Beschastnov N.S., Kontorovich M.I. On Loss in the Ground when Assembling the Mechanism as a Counterweight. *Trudy VKAS*. 1944;3. (in Russ.)
6. Kontorovich M.I. On the calculation of the capacitance of the antenna by the Howe method. *Trudy VKAS*. 194;2. (in Russ.)
7. Kalinin A.I., Cherenkova E.L. *Propagation of Radio Waves and the Operation of Radio Links*. Moscow: Sviaz Publ.; 1971. 439 p. (in Russ.)
8. Zernov N.V., Karpov V.G. *Theory of Radio Circuits*. Leningrad: Energiia Publ.; 1972. 816 p. (in Russ.)
9. Korbansky I.N. *Antennas*. Moscow: Energiia Publ.; 1973. 336 p. (in Russ.)
10. Rusin Yu.S. Approximate Capacitance Measurement Method. *Elektrichestvo*. 1960;11(48) (in Russ.)
11. Iossel Yu.Ya., Kochanov E.S., Strunsky M.G. *Capacity Calculation*. Leningrad: Energoizdat Publ.; 1981. 288 p. (in Russ.)
12. Emelin B.F. *Irregular Waveguides and Resonators*. Leningrad: Military Academy of Communications Publ.; 1959. 219 p. (in Russ.)
13. Beletsky A.F. *Fundamentals of the Theory of Linear Mathematical Circuits*. Moscow: Sviaz Publ.; 1967. 608 p. (in Russ.)
14. Fikhmanas R.F., Fridberg P.Sh. Method for Calculating the Capacity of Bodies and its Connection with Variational Principles. *Technical Physics*. 1970;40. (in Russ.)
15. Popov O.V., Tumashov A.V., Borisov G.N. Method for Calculating the Loss Asymmetric Vibrators with a Remote Power Point. *Journal Achievements of Modern Radioelectronics*. 2021;75(4):71–79. DOI:10.18127/j20700784-202104-10.
16. Vershkov M.V. *Ship Antennas*. Leningrad: Sudostroenie Publ.; 1972. 424 p. (in Russ.)
17. Fradin A.Z. *Antenna-Feeder Devices*. Moscow: Sviaz Publ.; 1977. 440 p. (in Russ.)
18. Kisunko G.V. *Electrodynamics of Hollow Systems*. Leningrad: Military Academy of Communications Publ.; 1949. 426 p. (in Russ.)
19. Markov G.T., Chaplin A.F. *Excitation of Electromagnetic Waves*. Moscow: Radio i sviaz Publ.; 1983. 295 p. (in Russ.)
20. Goldstein L.D., Zernov N.V. *Electromagnetic Fields and Waves*. Moscow: Sovetskoe radio Publ.; 1971. (in Russ.)
21. Belotserkovsky G.B. *Antennas*. Moscow: State Scientific and Technical Publishing House OBORONGIZ, 1962. (in Russ.)

Статья поступила в редакцию 30.01.2023; одобрена после рецензирования 13.02.2023; принята к публикации 14.02.2023.

The article was submitted 30.01.2023; approved after reviewing 13.02.2023; accepted for publication 14.02.2023.

Информация об авторах:

ПОПОВ
Олег Вениаминович

кандидат технических наук, доцент, ведущий научный сотрудник ООО «Специальный технологический центр»,
 <https://orcid.org/0000-0002-5315-2679>

ТУМАШОВ
Андрей Витальевич

аспирант кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
 <https://orcid.org/0000-0003-2656-0463>

БОРИСОВ
Георгий Николаевич

инженер ООО «Специальный технологический центр»,
 <https://orcid.org/0000-0002-3275-251X>

КОРОВИН
Константин Олегович

кандидат физико-математических наук, доцент, заведующий кафедрой радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
 <https://orcid.org/0000-0001-7979-3725>

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

**2.2.6 – Оптические
и оптико-электронные приборы
и комплексы**

**2.2.13 – Радиотехника, в том числе системы
и устройства телевидения**

**2.2.14 – Антенны, СВЧ-устройства
и их технологии**

**2.2.15 – Системы, сети и устройства
телекоммуникаций**

2.2.16 – Радиолокация и радионавигация

Научная статья

УДК 621.372.632

DOI:10.31854/1813-324X-2023-9-1-35-40



Реализация алгоритма начальной синхронизации демодулятора сигналов с прямым расширением спектра на основе быстрого преобразования Фурье. Часть 2. Оценивание несущей частоты

Ефим Александрович Брусин, brusin.ea@sut.ru

АО «Российский институт радионавигации и времени»,
Санкт-Петербург, 192012, Российская Федерация
Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация: Сигналы с прямым расширением спектра широко распространены в современных системах связи и навигации. Зачастую для каналов связи, в которых используются такие сигналы, характерны значительные по отношению к информационным скоростям принимаемых сигналов изменения несущей частоты. В частности, для каналов связи с существенным доплеровским смещением. Поэтому оценивание несущей частоты играет ключевую роль при решении задачи начальной синхронизации демодуляторов сигналов с прямым расширением спектра. В первой части статьи были представлены основные подходы к решению задачи начальной синхронизации. В данной части работы предложен алгоритм оценивания несущей частоты, основанный на анализе сечения функции неопределенности принимаемого сигнала в плоскости задержки. Оценивание несущей частоты осуществляется на основе быстрого преобразования Фурье с использованием итеративной процедуры дихотомического поиска. Приведены результаты анализа его эффективности; дисперсии оценок, полученные при реализации предложенного алгоритма оценивания, сопоставляются с границей Крамера – Рао.

Ключевые слова: прямое расширение спектра, оценивание несущей частоты, быстрое преобразование Фурье, дихотомический поиск, граница Крамера – Рао

Ссылка для цитирования: Брусин Е.А. Реализация алгоритма начальной синхронизации демодулятора сигналов с прямым расширением спектра на основе быстрого преобразования Фурье. Часть 2. Оценивание несущей частоты // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 35–40. DOI:10.31854/1813-324X-2023-9-1-35-40

Direct Sequence Spread Spectrum Signal's Demodulator Acquisition Implementation Based on Fast Fourier Transform. Part 2. Carrier Frequency Estimation

Ефим Брусин, brusin.ea@sut.ru

Russian Institute of Radionavigation and Time,
St. Petersburg, 192012, Russian Federation
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Abstract: Signals with direct spread spectrum are widespread in modern communication and navigation systems. Often for communication channels in which such signals are used, significant changes in the carrier frequency in relation to the information speeds of the received signals are characteristic. In particular, for communication channels with significant Doppler shift. Therefore, estimation of the carrier frequency plays a key role in solving the problem of initial synchronization of demodulators of signals with direct spectral broadening. In the first part of the paper, the main approaches to solving the initial synchronization problem were presented. In this part of the paper an algorithm for estimating the carrier frequency based on the analysis of the received signal uncertainty function cross section in the delay plane was proposed. The carrier frequency estimation is based on the fast Fourier transform using an iterative dichotomous search procedure. The results of its efficiency analysis are presented; the variance of the estimates obtained in the implementation of the proposed estimation algorithm are compared with the Cramer-Rao boundary.

Keywords: direct sequence spread spectrum signals, frequency estimation, Fast Fourier Transform, dichotomous search, Cramer-Rao bound

For citation: Brusin E. Direct Sequence Spread Spectrum Signal's Demodulator Acquisition Implementation Based on Fast Fourier Transform. Part 2. Carrier Frequency Estimation. *Proc. of Telecom. Universities*. 2023;9(1):35–40. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-35-40

Алгоритм начальной синхронизации демодулятора сигналов с прямым расширением спектра на основе БПФ предложен в работе [1]. В ней обсуждается синхронизация как по несущей частоте, так и по задержке. Предложенный в [1] алгоритм обеспечивает достаточно «грубое» оценивание несущей частоты. Для реализации собственно захвата демодулятора могут использоваться, например, методы, основанные на применении схем частотной автоподстройки [2]. В то же время интерес представляют подходы, которые бы обеспечили оценивание с дисперсией, достаточной для непосредственного перехода к демодуляции.

Известно, что для практической реализации демодулятора сигнала с прямым расширением спектра начальное смещение по частоте несущего колебания должно быть порядка единиц процентов от частоты следования информационных символов [3]:

$$(\sigma_f T_b)^2 \sim 10^{-3}, \quad (1)$$

где T_b – длительность информационного символа.

То есть необходимо разработать алгоритм оценивания, который бы обеспечил указанную дисперсию оценки.

Интересный подход к оцениванию несущей частоты сигналов с прямым расширением спектра изложен в работе [4]. Однако результаты, представленные в ней, не дают полного представления об эффективности предложенного алгоритма оценивания.

Таким образом, несмотря на значительное количество работ по проблеме начальной синхронизации демодуляторов сигналов с прямым расширением спектра, представляется, что проблемы оценивания несущей частоты принимаемого сигнала освещены недостаточно полно. В связи с этим основными задачами второй части работы являются разработка алгоритма оценивания не-

сущей частоты сигнала с прямым расширением спектра и анализ эффективности алгоритма методами компьютерного моделирования. При разработке собственно процедуры оценивания будем опираться на алгоритм начальной синхронизации, предложенный в [1].

Алгоритм оценивания

Как и в [1], будем рассматривать принимаемый сигнал двухпозиционной фазовой модуляции (ФМ-2) в виде:

$$\begin{aligned} \tilde{s}_k(t; b_k) = & s_k(t - \tau_k) \cdot B_k(t - \tau_k) \times \\ & \times \cos(2\pi(f_0 + f)t + \varphi_k) + n_\tau(t), \end{aligned}$$

где τ_k – задержка в канале; f – смещение частоты несущего колебания относительно заданного номинального значения; φ_k – фаза несущей частоты; $n_\tau(t)$ – отсчеты шума.

Для анализа эффективности алгоритма оценивания нормированную дисперсию оценки $(\sigma_f T_b)^2$ сопоставим с границей Крамера – Рао [5]:

$$D\{\hat{f}\} \approx \frac{1}{(2\pi T_{rms})^2 q^2}, q \gg 1, \quad (2)$$

где q^2 – отношение сигнал-шум; T_{rms} – среднеквадратичная длительность сигнала, характеризующая длительность сигнала во времени.

На практике полученная по результатам моделирования нормированная дисперсия оценок сравнивается с нормированной границей, для получения которой проведем простые преобразования. В первом приближении будем полагать, что среднеквадратичная длительность сигнала равна длительности информационного символа:

$$T_{rms} \sim T_b.$$

Приведем отношение сигнал/шум к соответствующему отношению на чип:

$$q^2 = q_s^2 N_l,$$

где N_l – длина расширяющей спектр последовательности; q_s^2 – отношение сигнал/шум на чип.

Границу (2) перепишем в виде:

$$D\{\hat{f}\} \approx \frac{1}{4\pi^2 T_b^2 q_s^2 N_l}.$$

Отсюда для нормированной границы Крамера – Рао оценки несущей частоты принимаемого сигнала можно записать:

$$CRLB(\hat{f}) \cdot T_b^2 \approx \frac{1}{4\pi^2 N_l E_s/N_0}. \quad (3)$$

В [1] приведена полученная по результатам моделирования зависимость нормированной дисперсии оценки несущей частоты для длины БПФ, равной 32768, что соответствует длительности интервала наблюдения $K = 8$. Моделирование проводилось для следующего сигнала: длительность информационного символа $T_b = 50$ мкс (что соответствует информационной скорости 20 кбит/с), вид модуляции ФМ-2, диапазон поиска по несущей частоте ± 40 кГц, $N_l = 2046$. Шаг сетки по несущей частоте $\Delta f T_b = 0,25$. В результате для $K = 8$ была получена нормированная дисперсия $(\sigma_f T_b)^2 \sim 10^{-2}$, что на порядок больше необходимой дисперсии оценки в соответствии с условием (1). Очевидное решение задачи повышения точности оценивания – уменьшение шага сетки частот. Для иллюстрации этого подхода на рисунке 1 представлены зависимости нормированных дисперсий оценки для $\Delta f T_b = 0,25$ и $\Delta f T_b = 0,125$.

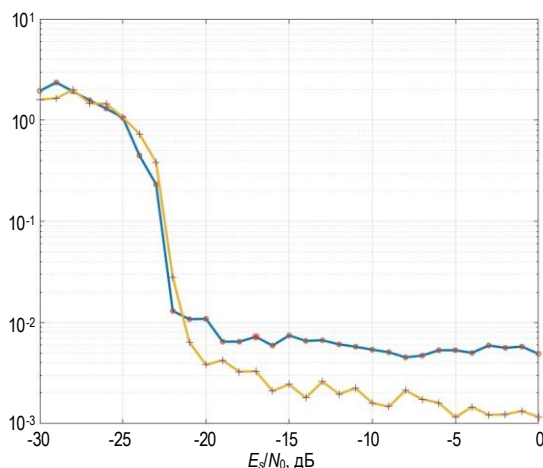


Рис. 1. Дисперсии оценок

Fig. 1. Estimation Variance

Следует отметить, что даже при $\Delta f T_b = 0,125$ полученная дисперсия недостаточна для захвата демодулятора. При этом количество вычислений БПФ практически удвоилось. Дальнейшее повышение точности оценивания потребует существенного увеличения объема вычислений. По-

этому для решения задачи оценивания несущей частоты предлагается другой подход.

Рассмотрим функцию неопределенности $\bar{\rho}(m, l)$, вычисленную в соответствии с алгоритмом, предложенным в [1]. В качестве иллюстрации на рисунке 2 представлена реализация функции $\bar{\rho}(m, l)$ для $E_s/N_0 = -10$ дБ, $L_f = 12$, частотной неопределенности ± 40 кГц, $K = 8$ и $\Delta f T_b = 0,25$.

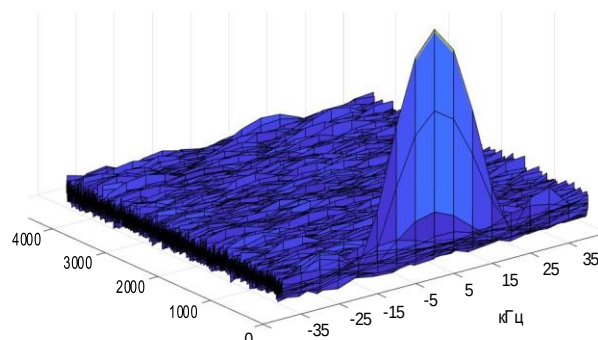


Рис. 2. Функция неопределенности

Fig. 2. Ambiguity Function

Выделим сечение функции неопределенности при $l = L_f$:

$$F(m) = \bar{\rho}(m, L_f). \quad (4)$$

Рассматриваемое сечение $F(m)$ фактически является срезом функции неопределенности $\bar{\rho}(m, l)$ в плоскости задержки. В качестве иллюстрации на рисунке 3а представлена реализация сечения функции неопределенности, полученная в ходе моделирования; -40 кГц на рисунке соответствует $m = -8$, а $+40$ кГц соответствует $m = +8$. Зависимость получена для нулевого смещения частоты несущего колебания относительно заданного номинального значения ($f = 0$) при отношении сигнал/шум на чип, равном -10 дБ.

При смещении несущей частоты принимаемого сигнала будут смещаться соответствующие сечения. Так, на рисунке 3б показаны реализации функции (4) при разных смещениях сигнала по несущей частоте: 0 и ± 5 кГц. Функцию (4) можно трактовать как дискретный спектр фрагмента сигнала. В таком случае задача оценивания тождественна задаче нахождения максимума этого спектра. Фактически оценивание несущей частоты сводится к нахождению максимума сечения функции неопределенности $\bar{\rho}(m, L_f)$ в плоскости частоты.

Подобная задача возникает при оценивании частоты синусоидального сигнала [6], которая сводится уже к нахождению максимума периодограммы, для чего разработан ряд алгоритмов. В частности, предлагается итеративная процедура дихотомического поиска [7], которая обеспечивает асимптотически эффективную оценку несущей частоты гармонического сигнала. Для нахождения макси-

муна сечения функции неопределенности предлагается использовать указанный метод дихотомического поиска, трансформировав его с учетом специфики принимаемого сигнала.

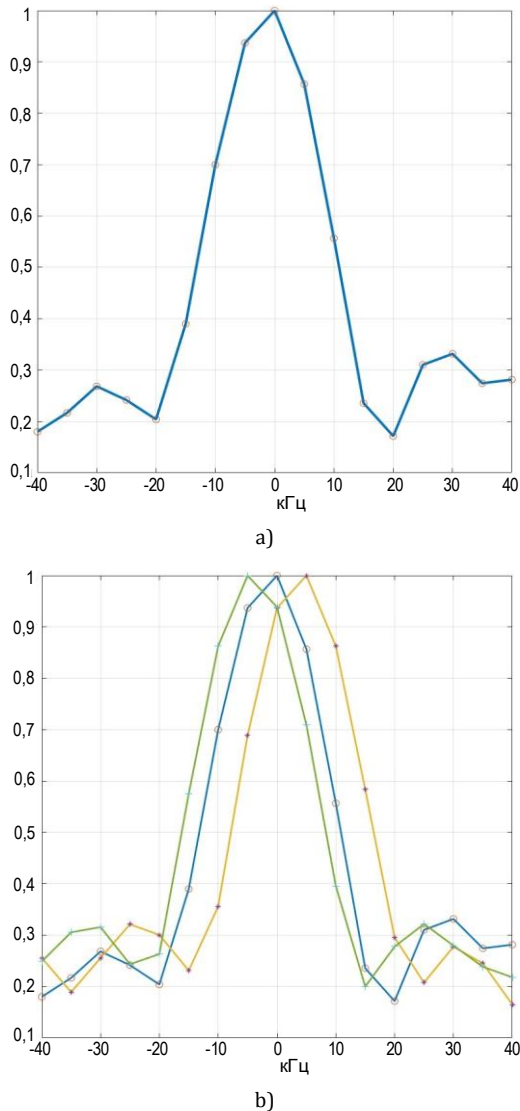


Рис. 3. Сечение функции неопределенности

Fig. 3. Ambiguity Function Section

Суть процедуры оценивания состоит в следующем. Вычисляем функцию неопределенности и находим оценку несущей частоты и смещение по отношению к опорной расширяющей последовательности в соответствии с алгоритмом, предложенном в [1]:

$$\{M_f, L_f\} = \arg \left\{ \max_{m,l} \bar{\rho}(m, l) \right\},$$

где $m = -M/2, \dots, -1, 0, 1, \dots, M/2$; $l = 0, 1, \dots, N_l - 1$.

В результате получаем искомую позицию по отношению к опорной расширяющей последовательности L_f и оценку смещения несущей частоты принимаемого сигнала относительно заданного номинального значения:

$$\hat{f} = M_f \cdot \Delta f. \quad (5)$$

В соответствии с L_f выделяем сечение функции неопределенности:

$$F(m) = \bar{\rho}(m, L_f).$$

После этого запускается итеративная процедура дихотомического поиска. Начальное значение итеративной процедуры – оценка (5):

$$\hat{f}_{c0} = \hat{f}.$$

Далее включается собственно дихотомический поиск. Суть процесса дихотомического поиска состоит в последовательном вычислении прямых и обратных преобразований Фурье.

Рассмотрим частоты

$$f_i^+ = f_{i-1}^+ + \frac{1}{2^i} \Delta f, \quad i = 1, 2, \dots, M_i$$

и

$$f_i^- = f_{i-1}^- - \frac{1}{2^i} \Delta f, \quad i = 1, 2, \dots, M_i,$$

где M_i – число итераций; $f_0^+ = f_0^- = \hat{f}_{c0}$.

Вычисляются преобразования Фурье вида:

$$S_l^+ = \sum_{n=0}^{N-1} \tilde{s}_k(t_n; b_k) \cdot e^{-j2\pi(f_0 + f_i^+)t_n} \cdot e^{-j\frac{2\pi n l}{N}}$$

и

$$S_l^- = \sum_{n=0}^{N-1} \tilde{s}_k(t_n; b_k) \cdot e^{-j2\pi(f_0 + f_i^-)t_n} \cdot e^{-j\frac{2\pi n l}{N}},$$

где $l = 0, 1, \dots, N-1$.

Затем вычисляются обратные преобразования Фурье вида:

$$s_l^+ = \frac{1}{N} \sum_{n=0}^{N-1} S_l^+ \cdot \hat{R}_n \cdot e^{j\frac{2\pi n l}{N}}$$

и

$$s_l^- = \frac{1}{N} \sum_{n=0}^{N-1} S_l^- \cdot \hat{R}_n \cdot e^{j\frac{2\pi n l}{N}}.$$

Далее проводятся усреднения вида:

$$\langle |s_m^+| \rangle = \frac{1}{K} \sum_{k=0}^{K-1} |s_{m+2kN_l}^+|$$

и

$$\langle |s_m^-| \rangle = \frac{1}{K} \sum_{k=0}^{K-1} |s_{m+2kN_l}^-|.$$

где $m = 0, 1, \dots, 2N_l - 1$.

Если $\langle |s_{L_f}^+| \rangle > \langle |s_{L_f}^-| \rangle$, то $\hat{f}_{ci} = f_i^+$, в противном случае $\hat{f}_{ci} = f_i^-$.

И наконец, при $i = M_i$, в заключение итеративной процедуры оценка смещения несущей частоты имеет вид:

$$\hat{f}_{c1} = \hat{f}_{c0} + \hat{f}_{cM_i}.$$

Таким образом, предлагаемый алгоритм оценивания является двухэтапной процедурой.

На первом этапе с использованием методов преобразования Фурье строится функция неопределенности принимаемого сигнала. Определяются смещение принимаемого сигнала по отношению к началу заданной расширяющей последовательности L_f и «грубая» оценка несущей частоты:

$$\{M_f, L_f\} = \arg \left\{ \max_{m,l} \bar{\rho}(m, l) \right\},$$

$$\hat{f}_{c0} = M_f \cdot \Delta f,$$

где Δf – шаг сетки по несущей частоте.

«Точная» оценка несущей частоты $\hat{f}_{c1}$ осуществляется с использованием итеративной процедуры дихотомического поиска.

Для определения эффективности оценок, обеспечиваемых предложенным алгоритмом, было проведено компьютерное моделирование процедуры оценивания. Отношение сигнал/шум на чип в ходе моделирования изменялось от -30 до 0 дБ с шагом 1 дБ. При каждом E_s/N_0 проводилось 100 попыток реализации алгоритма начальной синхронизации, включая оценивание смещения принимаемого сигнала относительно заданной расширяющей и собственно оценивание несущей частоты.

В ходе моделирования вычислялись вероятность обнаружения и нормированные дисперсии оценок несущей частоты:

$$P_d = \frac{1}{N_p} \sum_{i=0}^{N_p-1} P_i,$$

$$(\sigma_f T_b)^2 = \frac{1}{N_p} \sum_{i=0}^{N_p-1} [(\hat{f}_{c0} - f) \cdot T_b]^2 \text{ и } (\sigma_{f1} T_b)^2 =$$

$$= \frac{1}{N_p} \sum_{i=0}^{N_p-1} [(\hat{f}_{c1} - f) \cdot T_b]^2,$$

где N_p – количество попыток реализации алгоритма начальной синхронизации; $P_i = 1$, если $L_f = \tilde{L}_f$ и $P_i = 0$, если $L_f \neq \tilde{L}_f$; $\tilde{L}_f$ – правильное, априорно известное значение смещения временной позиции на приеме. Дисперсия вычислялась для различного количества итераций. Результаты моделирования иллюстрируют зависимости, представленные на рисунках 4 и 5.

На рисунке 4 представлена зависимость вероятности обнаружения от отношения сигнал/шум на чип для $L_f = 12$. Результаты реализации процедуры оценивания для количества итераций 2, 4 и 6 при

$L_f = 12$ представлены на рисунке 5. На рисунке также приведены нормированная граница (3) и дисперсия оценки в соответствии с правилом (5).

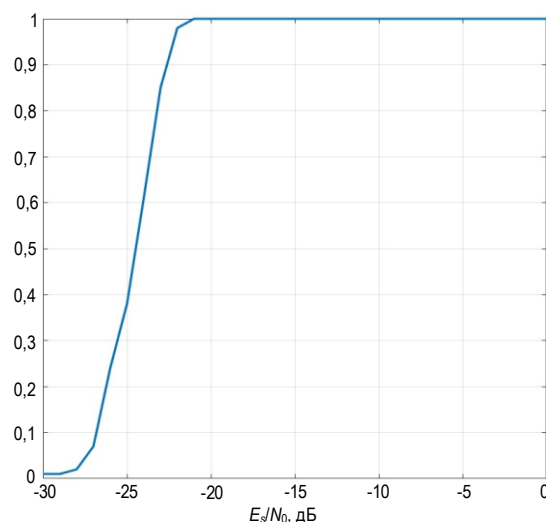


Рис. 4. Вероятность обнаружения

Fig. 4. Detection Probability

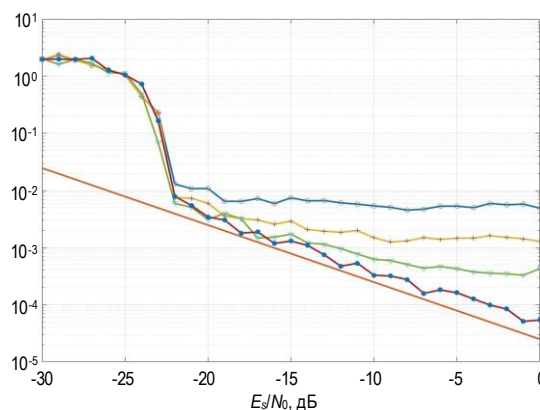


Рис. 5. Дисперсии оценок от количества итераций

Fig. 5. Estimation Variance VS Iteration Numbers

Заметим, что с увеличением числа итераций дисперсия оценки приближается к границе (3) и уже при $M_i = 6$ очень незначительно проигрывает нижней границе Крамера – Рао.

Выводы

Предложен двухэтапный алгоритм оценивания несущей частоты сигнала с прямым расширением спектра. На первом этапе с использованием методов преобразования Фурье строится функция неопределенности принимаемого сигнала. На втором этапе осуществляется поиск максимума сечения функции неопределенности.

Фактически предложенный алгоритм оценивания является развитием традиционного подхода к начальной синхронизации, основанного на методах анализа в частотной области с использованием преобразования Фурье. То есть обеспечивает совместную оценку несущей частоты и задержки.

Для реализации собственно захвата демодулятора в основном используются схемы частотной автоподстройки. Существенным отличием предлагаемого подхода является точное оценивание несущей частоты с применением итеративной процедуры дихотомического поиска.

В плане практической реализации затраты на процедуру дихотомического поиска сводятся к вычислению двух прямых и двух обратных БПФ на каждую итерацию. Например, для четырех итераций требуется дополнительное вычисление 16 преобразований Фурье. Представляется, что эти дополнительные вычислительные затраты не столь значительны. В свою очередь, использование итеративной процедуры даже с 4 итерациями позволяет в наиболее значимом в практическом плане диапазоне отношения сигнал/шум на чип получить

точность оценки несущей частоты, достаточную для «прямого» захвата демодулятора.

Предложенная процедура оценивания позволяет получить требуемую точность оценок при относительно небольших интервалах наблюдения. Так, в рассматриваемом случае приведены результаты для длительности интервала наблюдения $K = 8$.

Следует особо подчеркнуть, что разработанный алгоритм оценивания обеспечивает дисперсии оценок, весьма близкие к границе Крамера – Рао. Например, в диапазоне отношений сигнал/шум на чип от -20 до -10 дБ при использовании итеративной процедуры с 6 итерациями дисперсии оценок проигрывают границе не более 2 дБ. То есть предложенный алгоритм обеспечивает асимптотически эффективное оценивание. А для практической реализации демодулятора достаточно 4 итераций.

Список источников

1. Брусин Е.А. Реализация алгоритма начальной синхронизации демодулятора сигналов с прямым расширением спектра на основе быстрого преобразования Фурье. Часть 1. Постановка задачи и подход к решению // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 21–27. DOI:10.31854/1813-324X-2022-8-4-21-27
2. Перова А.И., Харрисова В.Н. ГЛОНАСС. Принципы построения и функционирования. М.: Радиотехника, 2010. 800 с.
3. COM-1418 DIRECT SEQUENCE SPREAD-SPECTRUM DEMODULATOR 22 Mchip/s. URL: <https://www.comblock.com/download/com1418.pdf> (дата обращения 23.01.2023)
4. DeLeon P.L., Scaife B.J. Spread-Spectrum Carrier Estimation with Unknown Doppler Shift. 1993. URL: <https://ntrs.nasa.gov/citations/20000014441> (дата обращения 23.01.2023)
5. Ipatov V.P. Spread Spectrum and CDMA: Principles and Applications. John Wiley & Sons Ltd., 2005.
6. Rife D., Boorstin R. Single tone Parameter Estimation From Discrete-Time Observations // IEEE Transactions on Information Theory. 1974. Vol. 20. Iss. 5. PP. 591–598. DOI:10.1109/TIT.1974.1055282
7. Zakharov Y.V., Tozer T.C. Frequency estimator with dichotomous search of periodogram peak // Electronics Letters. 1999. Vol. 35. Iss. 19. PP. 1608–1609.

References

1. Brusin E. Direct Sequence Spread Spectrum Signal's Demodulator Acquisition Implementation Based on Fast Fourier Transform. Part 1. Problem Statement and Solution Approach. *Proc. of Telecom. Universities*. 2022;8(4):21–27. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-21-27
2. Perova A.I., Harrisova V.N. *GLONASS. Principles of Construction and Functioning*. Moscow: Radiotekhnika Publ.; 2010. 800 p. (in Rus.)
3. COM-1418 DIRECT SEQUENCE SPREAD-SPECTRUM DEMODULATOR 22 Mchip/s. URL: <https://www.comblock.com/download/com1418.pdf> [Accessed 23rd January 2023]
4. DeLeon P.L., Scaife B.J. Spread-Spectrum Carrier Estimation with Unknown Doppler Shift. 1993. URL: <https://ntrs.nasa.gov/citations/20000014441> [Accessed 23rd January 2023]
5. Ipatov V.P. *Spread Spectrum and CDMA: Principles and Applications*. John Wiley & Sons Ltd.; 2005.
6. Rife D., Boorstin R. Single tone Parameter Estimation From Discrete-Time Observations. *IEEE Transactions on Information Theory*. 1974;20(5):591–598. DOI:10.1109/TIT.1974.1055282
7. Zakharov Y.V., Tozer T.C. Frequency estimator with dichotomous search of periodogram peak. *Electronics Letters*. 1999;35(19):1608–1609.

Статья поступила в редакцию 23.09.2022; одобрена после рецензирования 02.11.2022; принята к публикации 19.01.2023.

The article was submitted 23.09.2022; approved after reviewing 02.11.2022; accepted for publication 19.01.2023.

Информация об авторе:

БРУСИН
Ефим Александрович

кандидат технических наук, руководитель проектного направления АО «Российский институт радионавигации и времени», доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
 <https://orcid.org/0000-0002-6742-2705>

Научная статья

УДК 004.725.5

DOI:10.31854/1813-324X-2023-9-1-41-51



Эффективное частотно-территориальное планирование сетей IEEE 802.11 как задача «замощения» плоской зоны покрытия регулярными структурами. Часть 3. Решения задачи выбора частотной конфигурации для случая с 8 каналами

Антон Сергеевич Викулов, vikulov.as@sut.ru

¹Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация: При решении задачи частотно-территориального планирования сетей беспроводного доступа сети стандарта IEEE 802.11 необходимо выбрать частотные каналы для точек доступа таким образом, чтоб выбранная конфигурация соответствовала их минимальному негативному взаимному влиянию. В работе рассмотрено покрытие плоскости как ее «замощение», т. е. максимально плотное заполнение, группами зон покрытия точек доступа, которые в спектральном смысле соответствуют частотным кластерам. Задавая каждой из точек доступа частотный канал, можно получить множество возможных конфигураций, каждая из которых соответствует возможному решению задачи частотно-территориального планирования. При решении актуальных проектных задач в диапазоне 5 ГГц, наиболее часто необходимо принимать во внимание частотные планы с использованием 8 и более каналов. Основываясь на ранее предложенных модели и методе, в данной работе получены решения задачи поиска наилучшей конфигурации в частотных кластерах, состоящих из 8 точек доступа, а также показаны их характеристики в привязке к их геометрии.

Ключевые слова: беспроводная сеть доступа, IEEE 802.11, помеха, мотивная единица, «замощение» плоскости, частотный кластер, частотное планирование, проектирование, частотная конфигурация

Ссылка для цитирования: Викулов А.С. Эффективное частотно-территориальное планирование сетей IEEE 802.11 как задача «замощения» плоской зоны покрытия регулярными структурами. Часть 3. Решения задачи выбора частотной конфигурации для случая с 8 каналами // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 41–51. DOI:10.31854/1813-324X-2023-9-1-41-51

Effective Channel Planning of IEEE 802.11 Networks as a Plane Tessellation Problem. Part 3. Solutions of Best Channel Configuration Selection Problem for Eight-Channel Case

Anton Vikulov, vikulov.as@sut.ru

¹The Bonch-Bruевич Saint-Petersburg State University of Telecommunications, St. Petersburg, 193232, Russian Federation

Abstract: When solving the problem of channel planning of IEEE 802.11 wireless access networks, it is necessary to allocate channels for access points so that the selected channel configuration provides minimum negative mutual influence. We will consider the covering of the plane "tessellation", i.e. the densest filling, by coverage areas of access points groups, which in the spectral sense correspond to channel clusters. By assigning a channel to each of the access points, we obtain a set of possible configurations, each of which corresponds to a possible solution of the channel planning problem. When solving actual design problems in the 5 GHz band, it is often necessary to take into account channel plans that include 8 or more channels. Based on the previously proposed model and method, in this paper, solutions to the problem of finding the best channel configuration for clusters consisting of 8 access points are obtained, and their characteristics are shown in relation to their geometry.

Keywords: wireless access network, IEEE 802.11, interference, cluster, cell unit, plane tessellation, channel planning, channel configuration

For citation: Vikulov A. Effective Channel Planning of IEEE 802.11 Networks as a Plane Tessellation Problem. Part 3. Solutions of Best Channel Configuration Selection Problem for Eight-Channel Case. *Proc. of Telecom. Universities*. 2023;9(1):41–51. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-41-51

Введение

Без решения задачи частотно-территориального планирования сетей IEEE 802.11 [1], включая последнее дополнение [2], невозможен процесс проектирования сколько-нибудь сложной распределенной беспроводной инфраструктуры. Среди подходов к проектированию можно отметить как руководства («мануалы») компаний-производителей оборудования [3–7], так и монографии [8–10]. Среди них интерес представляет подход, при котором рассматривается «замоещение» [11] плоскости зонами покрытия точек доступа (ТД), формирующих регулярную структуру [12].

Такая регулярная структура может быть описана путем задания мотивной (элементарной) единицы «замоещения» и в общем случае косоугольного базиса, задающего трансляционную симметрию в плоской решетке. Мотивная единица в плоском случае – группа зон покрытия ТД, связанная с каждым из узлов решетки. Путем трансляционного переноса мотивной единицы может быть получена вся структура «замоещения» плоскости [12]. В спектральном смысле частотно-территориального планирования мотивная единица соответствует частотному кластеру [13], понятию, широко используемому в планировании сотовых сетей. Отметим, что, говоря о мотивной единице, мы акцентируем внимание на геометрии структуры «замоещения».

Располагая в мотивной единице ТД стандарта IEEE 802.11, работающие на различных каналах, мы можем изучить взаимное влияние между ТД таким образом, что получим возможность учитывать эффекты межканальных помех, и, следовательно, выбирать наилучшие частотные конфигурации. Под последней будем понимать отдельные возможные решения задачи выбора частотных каналов для каждой из ТД в мотивной единице.

Ранее были предложены модель [14] учета межканальных помех для такого подхода, а также метод [15] выбора наилучшей частотной конфигура-

ции для выбранной мотивной единицы «замоещения». Кроме того, в работе [15] были выполнены расчеты для задачи частотного планирования при размере частотного кластера, равного 3 и 4. Случаи для малого числа каналов характеризуются в целом отсутствием в явном виде лучших решений (кроме нескольких вырожденных сценариев), поскольку все возможные частотные конфигурации являются эквивалентными с точки зрения их характеристик. В случае же большего размера частотного кластера M , становится возможен выбор предпочтительных конфигураций (или групп конфигураций), а потому такая задача представляет практический интерес.

В работе [11] были рассмотрены наиболее актуальные для современных сетей IEEE 802.11 частотные планы и показано, что случай с числом каналов M , равным восьми, имеет особое значение. Это связано с тем, что при «замоещении» плоскости зонами покрытия ТД с координационным числом N , равным 4, возможно построить структуру из двух «слоев» [12]. При этом мотивная единица каждого из «слоев» будет содержать 8 ТД. Поскольку это хорошо соотносится с размещением в спектре доступных в РФ каналов частотного диапазона 5 ГГц (две группы по 8 каналов), случай с $M = 8$ представляет особый интерес.

Данная работа в развитие исследований [14] и [15] посвящена рассмотрению частотных планов, предполагающих использование 8 каналов IEEE 802.11ах, шириной 20 МГц (каналы типа HE20), что является особенно актуальным для планирования радиопокрытия в частотном диапазоне 5 ГГц.

Модель оценки межканальных помех и метод выбора наилучшей частотной конфигурации

Применим модель межканальных помех, подробно изложенную в работе [14] ранее. Имея в мотивной единице «замоещения» плоскости M точек доступа, работающих каждая на своем канале, получим $M!$ возможных частотных конфигураций, т. е.

их число определяется возможными перестановками из M . Поставим каждой ТД в соответствие некоторую центральную частоту канала наперед заданного типа и определим через матрицу-вектор F_n , где n – номер ТД в мотивной единице.

Матрица возможных частотных конфигураций H , будет содержать все возможные перестановки вектора F :

$$H = \begin{pmatrix} F_{1,1} & F_{1,2} & \dots & F_{1,M!} \\ F_{2,1} & F_{2,2} & \dots & F_{2,M!} \\ \dots & \dots & \dots & \dots \\ F_{M,1} & F_{M,2} & \dots & F_{M,M!} \end{pmatrix} \text{ (МГц)}. \quad (1)$$

При построении матрицы воспользуемся алгоритмом генерации перестановок, предложенным в работе [16]. При необходимости будем также пользоваться порядковыми номерами перестановок, генерируемыми согласно данному алгоритму. Т.е. каждая возможная частотная конфигурация из их общего числа $M!$ для мотивной единицы будет однозначно задаваться столбцом матрицы H . Схема выбора решения [15] имеет вид: исходные данные → расчет матрицы возможных решений → вариационный ряд решений → поиск оптимального решения → экстраполяция решения.

Исходными данными для этой задачи являются следующие параметры: радиус R (м) ячейки покрытия, формируемой ТД беспроводной локальной вычислительной сети (БЛВС); модель затухания сигнала $L(f, d)$, определяющая затухание распространяемого сигнала L (дБ) как функцию от частоты сигнала f (МГц) и расстояния до источника d (м); тип решетки «замощения» и ее базис; мотивная единица структуры; координационное число структуры «замощения» N ; размер частотного кластера M , равный числу ТД в мотивной единице; матрица H возможных частотных конфигураций общим числом $M!$; вероятность занятости канала Q ; шумовой порог NF (аббр. от англ. Noise Floor), равный 10^{-9} мВт (–90 дБм); требуемый уровень мощности принимаемого сигнала в ячейке P_T ; уровень мощности излучения всех ТД P_{rad} .

На втором шаге при расчете матрицы SNR (аббр. от англ. Signal-to-Noise Ratio, отношения сигнал/шум), содержащей множество m возможных частотных конфигураций, будем следовать модели, предложенной в работе [14]. Расчет выполняется для всех возможных частотных конфигураций мотивной единицы заданной структуры и размера для нескольких различных размеров сетки D . Параметр D в модели определяет размер рассматриваемой области. С его ростом свойства рассматриваемой области последовательно приближаются к свойствам бесконечной плоскости.

При этом сами значения SNR рассчитываются согласно формуле:

$$SNR_{n,m} = 10 \log_{10} \frac{\int_{F_T-A}^{F_T+A} S_{Tw}(f) df}{\int_{F_T-A}^{F_T+A} W_{Iw}(f) df} \text{ (дБ)}, \quad (2)$$

где n – номер вершины; m – номер решения; A – полуширина центральной части спектральной максимума сигнала, МГц; F_T – центральная частота рассматриваемого канала, МГц.

Суммарный спектр всех межканальных помех W_{Iw} (мВт) от ячеек той же БЛВС рассчитывается согласно выражению [14]:

$$W_{Iw}(f) = NF + Q \sum_{i=-D}^D \sum_{j=-D}^D \sum_{k=1}^M U \times S_{Iw}(H_{k,m}, d_{ij}(n), f) \quad (3)$$

при

$$U = \begin{cases} 1, & k \neq n \\ 0, & k = n \end{cases}$$

где U – функция-индикатор межканальных помех; NF – шумовой порог (мВт); Q – вероятность занятости частотного канала; i, j – координаты в системе трансляционной симметрии; D – размер сетки; S_{Iw} – спектральная маска канала заданного типа; H – матрица возможных $m \in [0, M!]$ частотных конфигураций для заданной мотивной единицы, содержащей n ТД; $\vec{d}_{ij}(n)$ – расстояние до отдельной ТД, создающей помеху; f – частота.

Маска сигнала задается согласно:

$$S_{Tw}(f) = 10^{\frac{P_T + S(f-F_T)}{10}} \text{ (мВт)}, \quad (4)$$

где P_T – требуемый уровень приема сигнала на входе радиомодуля клиентского устройства (дБм); примем его равным –60 дБм.

Маска канала помехи задается в виде:

$$S_{Iw}(f) = 10^{\frac{P_{rad} + G_t + S(f-F_l) - L(H,d)}{10}} \text{ (мВт)}, \quad (5)$$

где $S(f - F_l)$ – спектральная маска сигнала-помехи (дБм); $S(f - F_T)$ – спектральная маска полезного сигнала (дБм); P_{rad} – уровень мощности излучения источника сигнала на выходе радиомодуля, создающего помеху (дБм), примем его равным 14 дБм; G_t – коэффициент усиления передающей антенны ТД-помехи в направлении целевой ТД; F_l – центральная частота канала-помехи (МГц); $L(F, d)$ – среднее затухание мощности сигнала в зависимости от частоты сигнала F и расстояния от его источника, определяемого длиной вектора $\vec{d}_{ij}(n)$.

После построения вариационных рядов, при выборе наилучшего решения будем руководствоваться следующими требованиями к такой частотной конфигурации мотивной единицы с позиции значения SNR для состоящих в ней ТД:

- среднее SNR для всех ТД – максимальное;
- условие для SNR – максимум;

- третье по величине SNR – максимальное (для случая равномерного размещения каналов на непрерывном участке спектра);
- минимальное SNR – не ниже допустимого.

Для найденного на пятом шаге решения выполним экстраполяцию на большие D с целью найти значения параметров лучшего замощения на бесконечной плоскости.

Экстраполяцию (в данном случае для среднего SNR в отдельном решении) выполним экспоненциальной функцией вида:

$$\max\langle SNR_{n,m} \rangle = z_1 \cdot e^{-(D-z_2)} + \langle SNR_{n,m} \rangle_{\infty} \text{ (дБ)}, \quad (6)$$

где z_1 и z_2 – некоторые определяемые подбором коэффициенты, $\langle SNR_{n,m} \rangle_{\infty}$ – горизонтальная асимптота функции (6) при больших D .

Рассматриваемыми параметрами возможных решений являются: среднее и минимальное SNR для всех ТД мотивной единицы. Кроме того, справочно приведем значение для третьей по величине SNR точки доступа в мотивной единице.

Постановка задачи

В работе [12] ранее были построены некоторые возможные регулярные структуры, возникающие при «замощении» плоскости. Поскольку в данной работе мы рассматриваем случай с 8-канальными частотными планами, то здесь нас будут интересовать три случая: одна структура с числом элементов на минимальном расстоянии от заданного (координационным числом) $N = 4$ и две структуры с $N = 6$. С позиции выбора частотного плана, в данном случае мы рассмотрим только один вариант с 8 каналами HE20, соответствующих поддиапазонам UNII-1 и UNII-2, т. е. каналы с номерами: 36, 40, 44, 48, 52, 56, 60, 64. Обратим внимание, что в данном частотном плане каналы расположены последовательно, а расстояния в спектре между центральными частотами смежных каналов идентичны.

Матрица-вектор F , содержащая центральные частоты каналов частотного плана:

$$F = (5180 \ 5200 \ 5220 \ 5240 \ 5260 \ 5280 \ 5320).$$

Матрицу H , содержащую все $M! = 40320$ возможных решений, приводить далее не будем ввиду ее большого размера.

С целью проверить, что лучшее решение не зависит от выбранной модели затухания, рассмотрим две модели затухания сигнала: в случае наличия препятствий [10] и в случае их отсутствия [11]. Отметим, что расстояние между двумя ближайшими ТД равно $2R$, где R – радиус зоны покрытия ТД. Примем R равным 10 м.

Кроме того, с целью сравнить значения выполним расчеты также для двух различных значений

вероятности занятости Q в БЛВС: 0,1 – для умеренно нагруженной БЛВС и 0,5 для случая высокой нагрузки трафиком.

SNR для всех случаев, рассмотренных ниже, равен 30 дБ (при требуемом уровне приема равном –60 дБм и шумовом пороге равном –90 дБм). Примем коэффициент усиления всех антенн равным 2 дБ. Отклонения в меньшую сторону от указанного значения и будут в нашем случае определяться частотной конфигурацией и геометрией решения.

Далее рассмотрим подробно результаты расчетов для трех структур «замощения».

Решения для случая $M = 8, N = 4$

Для случая «замощения» с координационным числом 4 «замощение» плоскости, базис и мотивная единица приведены на рисунке 1, где здесь и далее: красным показана мотивная единица и векторы трансляционной симметрии в косоугольной системе координат; зеленым – ортонормированная система координат.

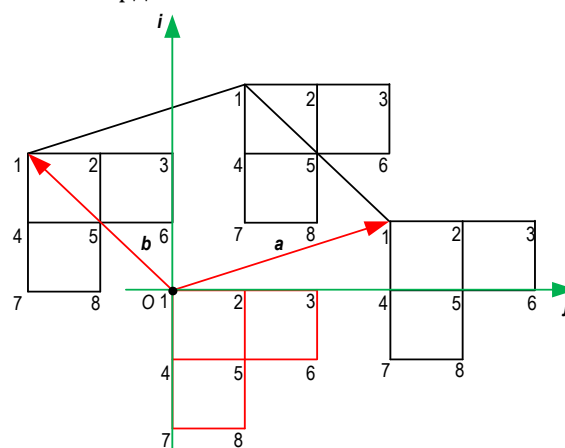


Рис. 1. Трансляционная симметрия и мотивная единица для случая $M = 8, N = 4$

Fig. 1. Translation Symmetry and Cell Unit for $M = 8, N = 4$

Матрица перехода между системами координат имеет вид:

$$C = \begin{pmatrix} 6R & -4R \\ 2R & 4R \end{pmatrix}.$$

Матрицу, содержащую все множество трансляций, т. е. задающую координаты вершин мотивной единицы в косоугольной системе координат, можно записать в виде (7).

С целью большей иллюстративности приведем вариационные ряды решений для двух моделей затухания сигнала – ITU-R P.1238 и ITU-R P.525 при высокой нагрузке ($Q = 0,5$), поскольку в этом случае ввиду большего взаимного влияния смежных каналов, преимущество наилучшего решения будет более заметным. Они приведены на рисунке 2.

$$d = \begin{pmatrix} 0+i & \frac{1}{4}+i & \frac{1}{2}+i & -\frac{1}{4}+i & 0+i & \frac{1}{4}+i & -\frac{1}{2}+i & -\frac{1}{4}+i \\ 0+j & -\frac{1}{8}+j & -\frac{1}{4}+j & -\frac{3}{8}+j & -\frac{1}{2}+j & -\frac{5}{8}+j & -\frac{3}{4}+j & -\frac{7}{8}+j \end{pmatrix}. \quad (7)$$

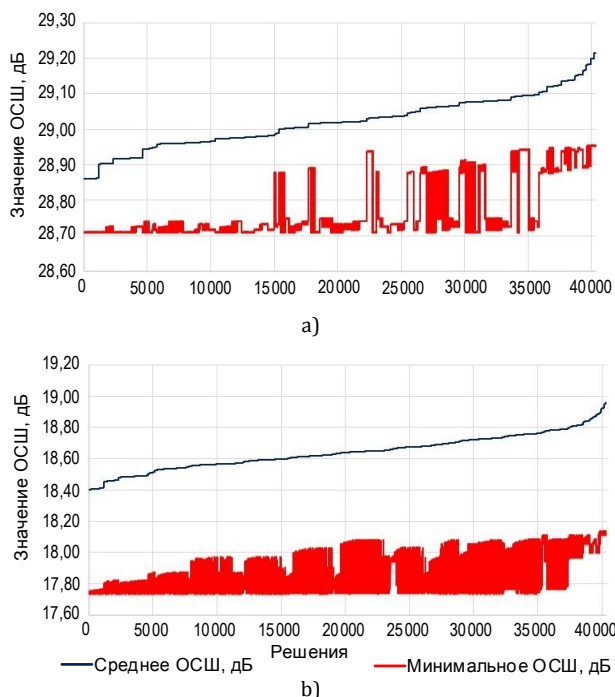


Рис. 2. Вариационный ряд для среднего и минимального SNR в случае $M = 8, N = 4$ для моделей затухания ITU-R P.525 (a) и ITU-R P.1238 (b) при $Q = 0,5, D = 3$

Fig. 2. Variational Series for Average and Minimum SNR for $M = 8, N = 4, Q = 0,5, D = 3$, ITU-R P.525 (a) and ITU-R P.1238 (b) Models

Отметим, что лучшее решение с точки зрения среднего SNR одновременно является лучшим с точки зрения минимального SNR. Из расчетов видно, что лучшее решение ожидаемо не зависит как от выбранной модели затухания, так и от нагрузки. При этом общий вид вариационного ряда для решений в двух рассмотренных моделях затухания сигнала-помехи идентичен и похож на S-образную функцию. При этом некоторая «ступенчатость» вариационного ряда для случая сильного затухания объясняется очень небольшой разницей в абсолютных значениях по параметрам наилучшего решения. Во всех приведенных ниже результатах значения округлены с точностью до 0,01 дБ.

Во всех случаях при $D = 3$ лучшим решением является № 28811. При $D = 0$ лучшим решением является № 16456. Соответствующие им частотные конфигурации (в МГц) приведены в таблице 1.

Отметим, что здесь и далее номера решения указываются по порядку их генерации алгоритмом, приведенным в работе [16]. Указанным решениям соответствуют частотные конфигурации мотивной единицы (рисунки 3 и 4). При этом числами показаны номера каналов диапазона 5 ГГц.

ТАБЛИЦА 1. Решения для «замошения» $M = 8, N = 4$

TABLE 1. Solutions for Tessellation with $M = 8, N = 4$

№ решения	ТД	1	2	3	4	5	6	7	8
16456	Канал	64	44	52	40	56	36	60	48
	Частота	5320	5220	5260	5200	5280	5180	5300	5240
28811	Канал	60	40	48	52	64	56	44	36
	Частота	5300	5200	5240	5260	5320	5280	5220	5180

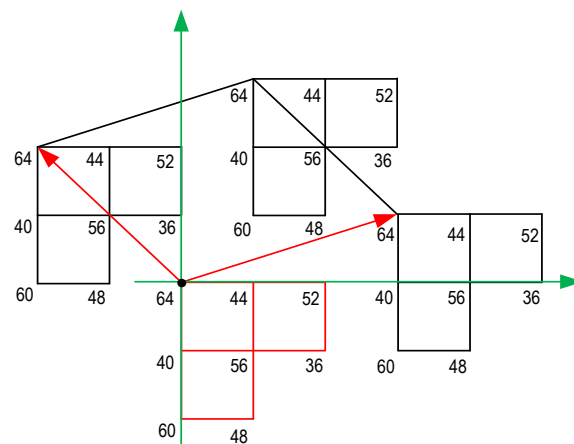


Рис. 3. Решение № 16456 ($D = 0$)

Fig. 3. Solution № 16456, $D = 0$

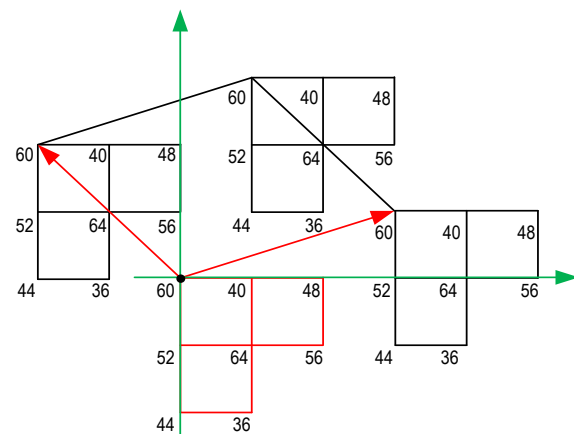


Рис. 4. Решение № 28811 ($D = 3$)

Fig. 4. Solution № 28811, $D = 3$

На рисунке 3 видно, что в рамках частотной конфигурации № 16456 в мотивной единице нет ни одной ТД, имеющей смежные точки, работающие на смежном канале, однако в рамках трансляций решение не является наилучшим. В то же время решение на рисунке 4 наилучшее именно с точки зрения учета трансляций. Теперь рассмотрим влияние размера сетки D на вариационный ряд решений для среднего SNR. Соответствующие графики приведены на рисунке 5.

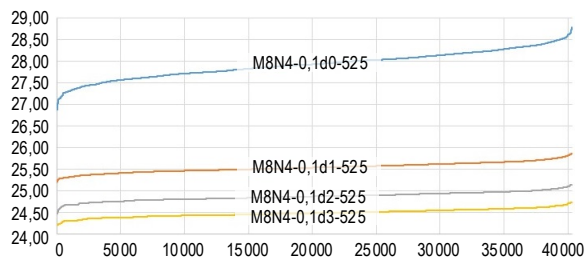


Рис. 5. Вариационные ряды для среднего SNR в случае $M = 8$, $N = 4$, модель затухания ITU-R P.525, $Q = 0,1$

Fig. 5. Variational Series for Average SNR for $M = 8$, $N = 4$, $Q = 0,1$, ITU-R P.525 Model

Обратим внимание, что с увеличением D последовательно снижаются значения SNR для решений и повышается точность расчетов. Можно ожидать, что возможна экстраполяция решений на большие D . При этом вид вариационных рядов для различных D одинаков.

В таблице 2 приведены результаты расчетов лучших решений для указанных условий. Приведены среднее, минимальное, а также значение SNR для третьего по величине узла.

ТАБЛИЦА 2. Результаты расчетов для $M = 8$, $N = 4$

TABLE 2. Calculation Results for $M = 8$, $N = 4$

L	Q	D	$\langle \text{SNR} \rangle$	$\text{Min}(\text{SNR})$	$\text{SNR}(3)$
1238	0,1	0	29,97	29,95	29,98
		1	29,85	29,79	29,85
		2	29,84	29,78	29,83
		3	29,83	29,77	29,83
		∞	29,81	29,75	–
1238	0,5	0	29,84	29,75	29,89
		1	29,29	29,05	29,29
		2	29,24	28,98	29,23
		3	29,21	28,96	29,21
		∞	29,13	28,85	–
525	0,1	0	28,79	28,37	29,02
		1	25,87	25,33	25,64
		2	25,14	24,53	24,86
		3	24,73	24,12	24,43
		∞	24,30	23,85	–
525	0,5	0	25,86	24,84	26,44
		1	20,52	19,63	20,15
		2	19,50	18,67	19,11
		3	18,96	18,14	18,54
		∞	18,36	17,17	–

Экстраполяция параметров лучшего решения экспоненциальной функцией на бесконечное D также показывает хорошую сходимость для всех рассмотренных случаев и представлена в таблице выше значениями при $D = \infty$.

Далее будем рассматривать мотивные единицы, возможные при «замощениях» с координационным числом $N = 6$ для двух структур.

Решения для случая $M = 8$, $N = 6$. Структура № 1

Для структуры № 1 при замощении с координационным числом 6, «замощение» плоскости, базис и мотивная единица приведены на рисунке 6.

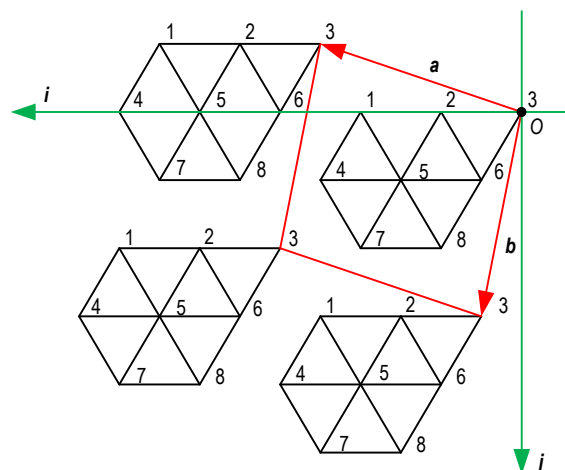


Рис. 6. Трансляционная симметрия и мотивная единица для случая $M = 8$, $N = 6$. Структура № 1

Fig. 6. Translation Symmetry and Cell Unit for $M = 8$, $N = 6$. Structure № 1

Матрица перехода между системами координат имеет вид:

$$C = \begin{pmatrix} 5R & R \\ -R\sqrt{3} & 3R\sqrt{3} \end{pmatrix}.$$

Матрица, содержащая все множество трансляций, т. е. задающая координаты вершин мотивной единицы в косоугольной системе координат, имеет вид (8).

Выполним расчеты матрицы решений и построим вариационные ряды, содержащие минимальное и среднее SNR. Ряды для двух рассматриваемых моделей затухания приведены на рисунке 7.

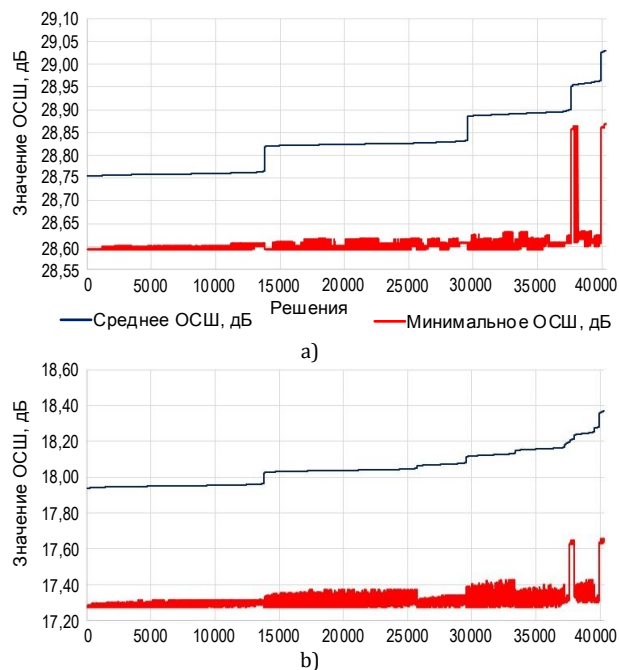


Рис. 7. Вариационный ряд для среднего и минимального SNR в случае $M = 8$, $N = 6$ (структура № 1) для моделей затухания ITU-R P.525 (a) и ITU-R P.1238 (b) при $Q = 0,5$, $D = 3$

Fig. 7. Variational Series for Average and Minimum SNR for $M = 8$, $N = 6$, $Q = 0,5$, $D = 3$, ITU-R P. 525 (a) and ITU-R P.1238 (b) Models. Structure № 1

$$d = \begin{pmatrix} \frac{6}{8} + i & \frac{3}{8} + i & 0 + i & \frac{7}{8} + i & \frac{1}{2} + i & \frac{1}{8} + i & \frac{5}{8} + i & \frac{2}{8} + i \\ \frac{2}{8} + j & \frac{1}{8} + j & 0 + j & \frac{5}{8} + j & \frac{1}{2} + j & \frac{3}{8} + j & \frac{7}{8} + j & \frac{6}{8} + j \end{pmatrix}. \quad (8)$$

Во всех случаях при $D = 3$ лучшим решением является № 37457. Соответствующая частотная конфигурация приведена в таблице 3.

ТАБЛИЦА 3. Решение для «замощения» $M = 8, N = 6$, структура № 1

TABLE 3. Solution for Tessellation with $M = 8, N = 6$, Structure № 1

№ решения	ТД	1	2	3	4	5	6	7	8
37457	Канал	36	56	48	52	44	64	60	40
	Частота	5180	5280	5240	5260	5220	5320	5300	5200

Указанному решению соответствует частотная конфигурация мотивной единицы, показанная на рисунке 8. Отметим, что в ней нет ТД, имеющих более одной соседней точки, работающей на смежном канале.

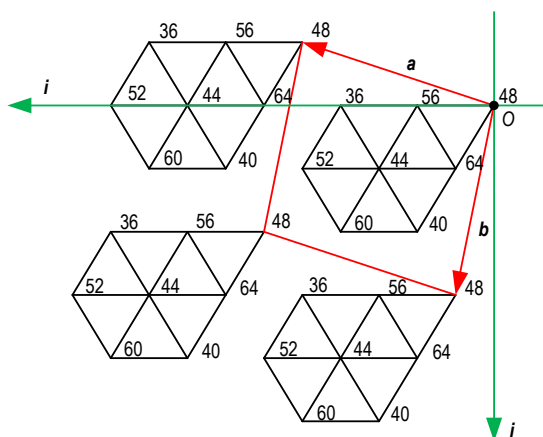


Рис. 8. Решение № 37457, структура № 1

Fig. 8. Solution №3 7457. Structure № 1

Теперь рассмотрим влияние размера сетки D на вариационный ряд решений для среднего SNR. Соответствующие графики приведены на рисунке 9.

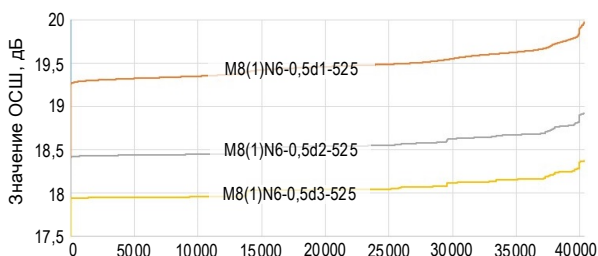


Рис. 9. Вариационные ряды для среднего SNR в случае $M = 8, N = 6$, структура № 1, модель затухания ITU-R P.525, $Q = 0,5$

Fig. 9. Variational Series for Average SNR for $M = 8, N = 6, Q = 0,5$, ITU-R P.525 Model. Structure № 1

Для большей наглядности, на рисунке выше не приведен вариационный ряд для $D = 0$. Обратим внимание, что с увеличением D последовательно

повышается точность расчетов и можно ожидать, что возможна экстраполяция решения на большие D . При этом вид вариационных рядов для различных D также одинаков.

В данном случае особенное внимание необходимо обратить на тот факт, что можно выделить группу из нескольких лучших решений, количеством 384 шт. На вариационных рядах их хорошо видно в правой части диаграммы. На рисунке 10 для большей наглядности приведена крайняя правая часть вариационного ряда среднего SNR для $D = 3$ (см. рисунок 9) в порядке от лучшего решения к худшим.

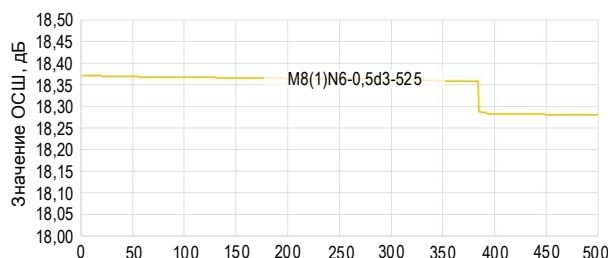


Рис. 10. Группа лучших решений в случае $M = 8, N = 6$, структура № 1, модель затухания ITU-R P.525, $Q = 0,5$

Fig. 10. Best Solutions for $M = 8, N = 6, Q = 0,5$, ITU-R P.525 Model. Structure № 1

Наличие убывания графика на рисунке 10 на участке до решения № 384 объясняется тем, что рассматриваемая сетка «замощения» представляет собой параллелепипед, а не круг. Т. е. с точки зрения произвольно взятой ТД в мотивной единице имеет место неизотропность (неравноценность) направлений на плоскости. С ростом D эта разница последовательно снижается и обратится в ноль на бесконечности. В таблице 4 приведены результаты расчетов лучших решений для указанных условий. Приведен ряд SNR: среднее ($\langle SNR \rangle$), минимальное ($\text{Min}(SNR)$), а также для третьего по величине узла ($SNR(3)$). Обратим внимание, что лучшее решение по поиску частотной конфигурации обладает одновременно и максимальным средним SNR и максимальным минимальным SNR среди возможных.

Экстраполяция экспоненциальной функцией параметров лучшего решения на бесконечное D показывает хорошую сходимость для всех рассмотренных случаев и представлена в таблице 4 значениями при $D = \infty$. Подбор параметров экспоненциальной функции (6) осуществлялся методом наименьших квадратов.

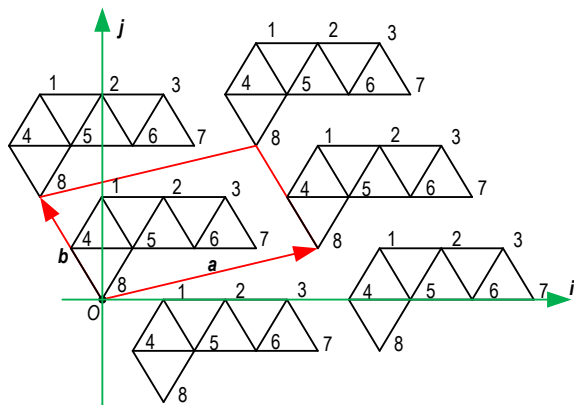
Теперь рассмотрим структуру замощения, также соответствующую случаю $M = 8$ и $N = 6$, но с иной геометрией мотивной единицы (Структура №2).

ТАБЛИЦА 4. Результаты расчетов для $M = 8, N = 6$, структура № 1TABLE 4. Calculation Results for $M = 8, N = 6$, Structure № 1

L	Q	D	$\langle SNR \rangle$	$\text{Min}(SNR)$	$SNR(3)$
1238	0,5	0	29,79	29,78	29,84
		1	29,14	28,96	29,00
		2	29,05	28,90	28,92
		3	29,03	28,87	28,90
		∞	28,93	28,74	–
525	0,1	0	28,67	28,44	28,79
		1	25,54	24,98	25,05
		2	24,70	24,19	24,26
		3	24,28	23,73	23,83
		∞	24,01	23,41	–
525	0,5	0	25,57	24,98	25,88
		1	19,98	19,30	19,34
		2	18,92	18,21	18,31
		3	18,37	17,65	17,78
		∞	17,73	17,05	–

Решения для случая $M = 8, N = 6$. Структура № 2

Для структуры № 2 при замощении с координатным числом 6, замощение плоскости, базис и мотивная единица приведены на рисунке 11.

Рис. 11. Трансляционная симметрия и мотивная единица для случая $M = 8, N = 6$. Структура № 2Fig. 11. Translation Symmetry and Cell Unit for $M = 8, N = 6$. Structure № 2

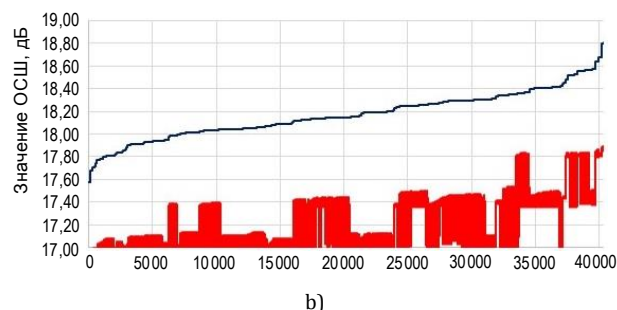
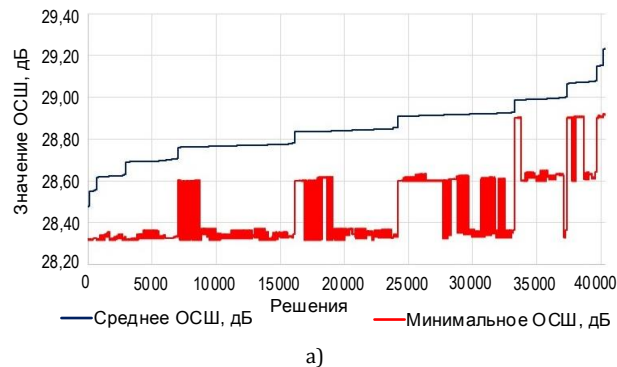
Матрица перехода между системами координат имеет вид:

$$C = \begin{pmatrix} 7R & -2R \\ R\sqrt{3} & 2R\sqrt{3} \end{pmatrix}.$$

Матрица, содержащая все множество трансляций, т. е. задающая координаты вершин мотивной единицы в косоугольной системе координат, имеет вид (9).

$$d = \begin{pmatrix} \frac{1}{4} + i & \frac{1}{2} + i & \frac{3}{4} + i & 0 + i & \frac{1}{4} + i & \frac{1}{2} + i & \frac{3}{4} + i & 0 + i \\ \frac{7}{8} + j & \frac{6}{8} + j & \frac{5}{8} + j & \frac{1}{2} + j & \frac{3}{8} + j & \frac{2}{8} + j & \frac{1}{8} + j & 0 + j \end{pmatrix}. \quad (9)$$

Выполним расчеты матрицы SNR и построим вариационные ряды, содержащие для каждого решения минимальное и среднее SNR . Ряды для двух рассматриваемых моделей затухания приведены на рисунке 12.

Рис. 12. Вариационный ряд для среднего и минимального SNR в случае $M = 8, N = 6$, структура № 2 для моделей затухания ITU-R P.1238 (а) и ITU-R P.525 (б) при $Q = 0,5, D = 3$
Fig. 12. Variational Series for Average and Minimum SNR for $M = 8, N = 6, Q = 0,5, D = 3$, ITU-R P.1238 (a) and ITU-R P.525 (b) Models. Structure № 2

Во всех случаях при $D = 3$ лучшим решением является № 28811. Соответствующая ему частотная конфигурация, приведена в таблице 5.

ТАБЛИЦА 5. Решение для «замощения» $M = 8, N = 6$, структура № 2TABLE 5. Solution for Tessellation with $M = 8, N = 6$, Structure № 2

№ решение	ТД	1	2	3	4	5	6	7	8
6225	Канал	36	56	48	60	44	64	40	52
	Частота	5180	5280	5240	5300	5220	5320	5200	5260

Указанному решению соответствует конфигурация мотивной единицы, показанная на рисунке 13. Решения обладают теми же свойствами, что и в ранее рассмотренном случае для $N = 6$.

Теперь рассмотрим влияние размера сетки D на вариационный ряд решений для среднего SNR . Соответствующие графики приведены на рисунке 14.

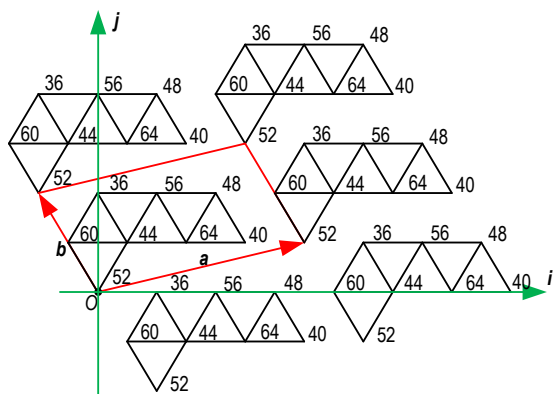


Рис. 13. Решение № 6225, структура № 2

Fig. 13. Solution № 6225. Structure № 2

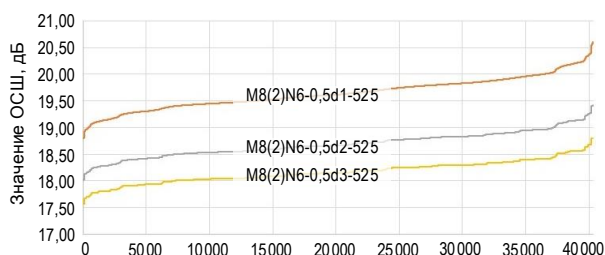


Рис. 14. Вариационные ряды для среднего SNR в случае $M = 8$, $N = 6$, структура № 2, модель затухания ITU-R P.525, $Q = 0,5$

Fig. 14. Variational Series for Average SNR for $M = 8$, $N = 6$, $Q = 0,5$, ITU-R P.525 Model. Structure № 2

Аналогично, на рисунке выше не приведен вариационный ряд для $D = 0$.

Отметим, что можно выделить группу из нескольких лучших решений, количеством 128 шт. На вариационных рядах они хорошо видны в правой части диаграммы. На рисунке 15 для большей наглядности приведена крайняя правая часть вариационного ряда среднего SNR для $D = 3$ (см. рисунок 14) в порядке от лучшего решения к худшим.

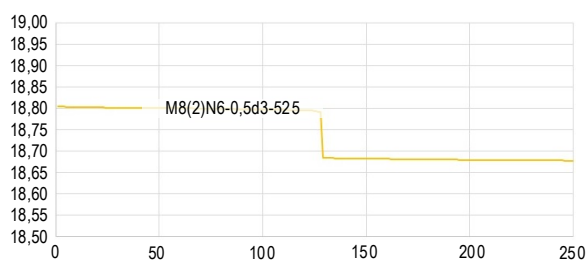


Рис. 15. Группа лучших решений в случае $M = 8$, $N = 6$, структура № 2, модель затухания ITU-R P.525, $Q = 0,5$

Fig. 15. Best Solutions for $M = 8$, $N = 6$, $Q = 0,5$, ITU-R P.525 Model. Structure № 2

Наличие убывания графика на рисунке 15 на участке до решения № 128 аналогично предыдущему случаю объясняется тем, что с точки зрения произвольно взятой ТД в мотивной единице имеет место неизотропность (неравноценность) направлений на плоскости.

В таблице 6 приведены результаты расчетов лучших решений для указанных условий.

ТАБЛИЦА 6. Результаты расчетов для $M = 8$, $N = 6$, структура № 2

TABLE 6. Calculation Results for $M = 8$, $N = 6$, Structure № 2

L	Q	D	$\langle SNR \rangle$	$\text{Min}(SNR)$	$SNR(3)$
1238	0,5	0	29,85	29,78	29,87
		1	29,34	29,06	29,37
		2	29,26	28,96	29,28
		3	29,23	28,92	29,25
		∞	29,16	28,81	–
525	0,1	0	28,87	28,45	29,02
		1	25,92	25,20	25,74
		2	25,08	24,36	24,83
		3	24,62	23,91	24,35
		∞	24,40	23,63	–
525	0,5	0	26,06	25,02	26,43
		1	20,60	19,54	20,31
		2	19,42	18,45	19,05
		3	18,81	17,88	18,42
		∞	18,24	17,28	–

Краткий анализ полученных решений

Из таблиц 2, 4 и 6 видно, что взаимное влияние каналов, и, как следствие, различия между частотными конфигурациями минимальны в случае высокого затухания между ТД (модель ITU-R P.1238) и с точки зрения среднего SNR составляют менее 0,5 дБ. В то же время в случае слабого затухания сигнала между ТД (модель ITU-R P.525), и особенно в случае высоконагруженных БЛВС, различия в величине среднего SNR между решениями могут достигать 2–3 дБ, что существенно при проектировании.

В абсолютных же значениях межканальные помехи оказывают наибольшее влияние (до 15 дБ) на SNR при низких затуханиях между ТД.

К особенностям полученных наилучших решений для $D = 0$ можно отнести следующее:

- в рамках мотивной единицы нет смежных вершин, использующих соседние каналы;
- в рамках трансляций есть смежные вершины, использующие соседние каналы.

Последнее связано с тем, что данное решение было найдено без учета трансляций и является оптимальным без учета «замощения».

Отличием решений для $D = 3$ является отсутствие смежных вершин в рамках трансляций, использующих соседние каналы, так как с учетом «замощения» наилучшее решение учитывает связь между смежными мотивными единицами. В структуре «замощения» для $N = 4$ наблюдается S-образная форма вариационного ряда решений, в которой наилучшим является одно решение. Напротив, в обеих структурах «замощения» для $N = 6$ можно выделить группу оптимальных решений числом 384 шт. для структуры № 1 и 128 шт. для структуры № 2, хорошо заметных в вариационном ряду.

При всех прочих равных условиях значения SNR в решениях для структуры № 2 меньше на величины порядка 0,5 дБ по сравнению с аналогичными

решениями для структуры № 1 в «замощении» с координатным числом $N = 6$, что говорит о предпочтительности ее выбора.

Выводы и перспективы дальнейших исследований

В результате проведенной работы можно отметить, что:

- проанализированы три структуры «замощения» плоской зоны покрытия для частотных планов с восемью каналами, отвечающих задаче построения сети IEEE 802.11 в частотном диапазоне 5 ГГц (поддиапазоны UNII-1 и UNII-2);
- получены частотные конфигурации, отвечающие требованиям к наилучшим решениям задачи минимизации межканальных помех;
- разница между значениями среднего SNR для худших и лучших частотных конфигураций в зависимости от рассматриваемой регулярной струк-

туры различается в пределах 0,5–3 дБ, что существенно при работе БЛВС и должно быть учтено при выборе частотного плана на этапе проектирования;

- значения среднего SNR для структуры № 2 при прочих равных условиях говорят о предпочтительности ее выбора по сравнению со структурой № 1;
- результаты расчетов показывают, что как выбор модели затухания, так и нагрузка на БЛВС не влияют качественно на выбор наилучшей частотной конфигурации;
- решение, выбранное исходя из критерия максимального среднего SNR, обладает также лучшим минимальным SNR и с точностью до 0,01 дБ – максимальным третьим SNR в решении.

Отметим также, что полученные результаты расчетов открывают перспективу дальнейшего анализа частотных конфигураций с точки зрения исследования возможных алгоритмов их построения.

Список источников

1. Institute of Electrical and Electronics Engineers. 802.11-2020. IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems. Local and Metropolitan Area Networks. Specific Requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE, 2021. 4379 p. DOI:10.1109/IEEESTD.2021.9363693
2. Institute of Electrical and Electronics Engineers. 802.11ax-2021. IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks. Specific Requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN. IEEE, 2021. 767 p. DOI:10.1109/IEEESTD.2021.9442429
3. Wireless LAN Design Guide: For High Density Environments in Higher Education // Cisco Systems. 2017. URL: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/cisco_wlan_design_guide.pdf (дата обращения 10.11.2022)
4. High Density Wi-Fi Design Principles // Aerohive Networks. 2012. URL: <https://dokumen.tips/documents/aerohive-whitepaper-hi-density-principles.html> (дата обращения 10.11.2022)
5. High Density Wi-Fi Deployment Guide. Best Practices Design Guide. // Ruckus Wireless. 2018. URL: <https://support.ruckuswireless.com/documents/1345-best-practices-design-guide-high-density-wi-fi-ap-deployment> (дата обращения 10.11.2022)
6. Aruba High Density Wireless Networks for Auditoriums. VRD. // Aruba Networks. 2010. URL: <https://www.arubanetworks.com/vrd/HighDensityVRD/wwhelp/wwhimpl/js/html/wwhelp.htm#href=Chap1.html> (дата обращения 10.11.2022)
7. Best Practices for High Density Wireless Network Design in Education and SMB. White Paper // Netgear. 2013 URL: https://www.netgear.com/images/pdf/High_Density_Best_Practices.pdf (дата обращения 10.11.2022)
8. Беделл П. Сети. Беспроводные технологии. М.: НТ Пресс, 2008.
9. Рыжков А.Е., Сиверс М.А., Бабкин А.С., Пыленок А.М., Трофимов А.П. Сети стандарта LTE. Развитие технологий радиодоступа. СПб.: СПбГУТ, 2015. 254 с.
10. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005. 592 с.
11. Викулов А.С., Парамонов А.И. Постановка задачи замощения плоскости в применении к частотно-территориальному планированию сетей IEEE 802.11 // Радиотехнические и телекоммуникационные системы. 2021. № 1(41). С. 24–32.
12. Викулов А.С., Парамонов А.И. Построение типовых структур для замощения плоскости в задаче частотно-территориального планирования сетей IEEE 802.11 // Радиотехнические и телекоммуникационные системы. 2021. № 2(42). С. 17–28.
13. Бабков В.Ю., Стариков В.В. Выбор кластерной структуры сети начального приближения стандарта LTE // Информационные системы и технологии. 2017. № 5(103). С. 72–80.
14. Викулов А.С. Эффективное частотно-территориальное планирование сетей IEEE 802.11 как задача «замощения» плоской зоны покрытия регулярными структурами. Часть 1. Модель межканальных помех // Труды учебных заведений связи. 2022. № 2. С. 29–36. DOI:10.31854/1813-324X-2022-8-2-29-36
15. Викулов А.С. Эффективное частотно-территориальное планирование сетей IEEE 802.11 как задача «замощения» плоской зоны покрытия регулярными структурами. Часть 2. Метод выбора частотной конфигурации и решения для малого числа каналов // Труды учебных заведений связи. 2022. Т. 8. № 3. С. 27–36. DOI:10.31854/1813-324X-2022-8-3-27-36
16. Фёдоров Л.И. Генератор перестановок транспозицией соседних элементов в Mathcad // Вестник Московского государственного областного университета. Серия: Физика-математика. 2014. № 4. С. 129–136.

17. Рекомендация МСЭ-R P.1238-8 (2016) Данные о распространении радиоволн и методы прогнозирования для планирования систем радиосвязи внутри помещений и локальных зонных радиосетей в частотном диапазоне 300 МГц – 100 ГГц. Серия Р. Распространение радиоволн.
18. Рекомендация МСЭ-R P.525-2 (1994) Расчет ослабления в свободном пространстве. (1978-1982-1994).

References

1. Institute of Electrical and Electronics Engineers. 802.11-2020. *IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems. Local and Metropolitan Area Networks. Specific Requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE; 2021. DOI:10.1109/IEEESTD.2021.9363693
2. Institute of Electrical and Electronics Engineers. 802.11ax-2021. *IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks. Specific Requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN*. IEEE; 2021. DOI:10.1109/IEEESTD.2021.9442429
3. Cisco Systems. Wireless LAN Design Guide for High Density Environments in Higher Education. 2017. URL: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/cisco_wlan_design_guide.pdf [Accessed 10th November 2022]
4. Aerohive Networks. High Density Wi-Fi Design Principles. 2012. URL: <https://dokumen.tips/documents/aerohive-whitepaper-hi-density-principles.html> [Accessed 10th November 2022]
5. Ruckus Wireless. High Density Wi-Fi Deployment Guide. Best Practices Design Guide. 2018. URL: <https://support.ruckuswireless.com/documents/1345-best-practices-design-guide-high-density-wi-fi-ap-deployment> [Accessed 10th November 2022]
6. Aruba Networks. Aruba High Density Wireless networks for Auditoriums. VRD. 2012. URL: <https://www.arubanetworks.com/vrd/HighDensityVRD/wwhelp/wwhimpl/js/html/wwhelp.htm#href=Chap1.html> [Accessed 10th November 2022]
7. Netgear. Best Practices for High Density Wireless Network Design in Education and SMB. White Paper. 2013. URL: https://www.netgear.com/images/pdf/High_Density_Best_Practices.pdf [Accessed 10th November 2022]
8. Bedell P. *Wireless Crash Course*. McGraw-Hill Professional, 2001.
9. Ryzhkov A.E., Sivers M.A., Babkin A.S., Pilenok A.M., Trofimov A.P. *LTE Networks. Development of Radio Access Technologies*. St. Petersburg: The Bonch-Bruевич Saint Petersburg State University of Telecommunications Publ.; 2015. 254 p. (in Russ.)
10. Vishnevsky V.M., Lyakhov A.I., Portnoy S.L., Shakhnovich I.V. *Broadband Wireless Networks for Information Transmission*. Moscow: Tekhnosfera Publ.; 2005. 592 p. (in Russ.)
11. Vikulov A.S., Paramonov A.I. Problem Statement of Tiling the Plane for Frequency and Area Planning of IEEE 802.11 Networks. *Radio and Telecommunication Systems*. 2021;1(41):24–32. (in Russ.)
12. Vikulov A.S., Paramonov A.I. Arrangement of Standard Structures for Tiling the Plane for Frequency and Area Planning of IEEE 802.11 networks. *Radio and Telecommunication Systems*. 2021;2(41):17–28. (in Russ.)
13. Babkov V.Yu., Starikov V.V. Selection of Cluster Structure of Initial Approximation LTE Network. *Information Systems and Technologies*. 2017;5(103):72–80. (in Russ.)
14. Vikulov A. Effective Channel Planning of IEEE 802.11 Networks as a Plane Tessellation Problem. Part 1. Adjacent Channel Interference Model. *Proc. of Telecom. Universities*. 2022;8(2):29–36. DOI:10.31854/1813-324X-2022-8-2-29-36
15. Vikulov A. Effective Channel Planning for IEEE 802.11 Networks as a Plane Tessellation Problem. Part 2. Method of Best Channel Configuration Selection and Solutions for a Low Number of Channels. *Proc. of Telecom. Universities*. 2022;8(3):27–36. (in Russ.) DOI:10.31854/1813-324X-2022-8-3-27-36
16. Fedorov L. Generator of Permutations by Transposition of Neighboring Elements in Mathcad. *Bulletin of the Moscow State Regional University. Series: Physics-Mathematics*. 2014;4:129–136. (in Russ.)
17. Rec. ITU-R P.1238-8 *Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 100 GHz*. 2016.
18. Rec. ITU-R P.525-2 *Calculation of free-space attenuation*. 1994.

Статья поступила в редакцию 06.09.2022; одобрена после рецензирования 31.10.2022; принята к публикации 02.11.2022.

The article was submitted 06.09.2022; approved after reviewing 31.10.2022; accepted for publication 02.11.2022.

Информация об авторе:

**ВИКУЛОВ
Антон Сергеевич**

кандидат технических наук, доцент кафедры сетей связи и передачи данных
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича

 <https://orcid.org/0000-0002-6671-9267>

Научная статья

УДК 681.586.5

DOI:10.31854/1813-324X-2023-9-1-52-58



The Sensitivity Investigation of Fiber Optic Paths in the Framework of an Intruder Localization at a Protected Facility

Vadim Kartak¹, kvmail@mail.ruOlga Gubareva²✉, o.gubareva@psuti.ruMichael Dashkov², mvd.srttc@gmail.comVladimir Gureev², gureevvo.rabota@gmail.comAlexander Evtushenko², alex2194ru@yandex.com

¹Ufa State Aviation Technical University,
Ufa, 450008, Russian Federation

²Povolzhskiy State University of Telecommunications and Informatics,
Samara, 443010, Russian Federation

Abstract: The paper considers the possibility of using communication lines already existing at urban development sites based on such information transfer technologies as «fiber-to-the-office» and «fiber-to-the-desk» in relation to the tasks of physical protection of objects. The aspects of using distributed acoustic sensors based on a phase-sensitive optical time-domain reflectometer for localizing sources of acoustic impact in real-time, that is, for determining the location of an intruder on a protected object, are considered. The sensitivity of optical paths to acoustic influences corresponding to the speech signals of the alleged intruder was assessed. An optical path based on optical fiber in an optical module with a hydrophobic filling is considered. An analysis of the spectral sensitivity of the optical fiber samples under study has been carried out. An assessment of the influence of the conditions for the passage of the route of laying the optical cable and the interaction of the acoustic sensor with the surrounding objects was carried out. The analysis of the results obtained during the test events at the experimental site was carried out.

Keywords: optical fiber, distributed acoustic sensor, optical reflectometer, intruder, acousto-optics

Funding: The paper was made as part of a grant to graduate students, applicants and young scientists for research aimed at ensuring information security for the tasks of the digital economy Contract No. 40469-36/2021-D.

For citation: Kartak V., Gubareva O., Dashkov M., Gureev V., Evtushenko A. The Sensitivity Investigation of Fiber Optic Paths in the Framework of an Intruder Localization at a Protected Facility. *Proc. of Telecom. Universities*. 2023;9(1):52–58. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-52-58

Исследование чувствительности оптических волокон в контексте локализации злоумышленника в защищенном помещении

Вадим Михайлович Картак¹, kvmail@mail.ruОльга Юрьевна Губарева²✉, o.gubareva@psuti.ruМихаил Викторович Дашков², mvd.srttc@gmail.comВладимир Олегович Гуреев², gureevvo.rabota@gmail.comАлександр Сергеевич Евтушенко², alex2194ru@yandex.com

¹Уфимский государственный авиационный технический университет,
Уфа, 450008, Российская Федерация

²Поволжский государственный университет телекоммуникаций и информатики,
Самара, 443010, Российская Федерация

Аннотация: В статье рассмотрена возможность использования уже существующих на объектах городской застройки линий связи на основе таких технологий передачи информации, как «волокно в офис» и «волокно до рабочего места» применительно к задачам физической защиты объектов. Изучены аспекты использования распределенных акустических датчиков на основе фазочувствительного оптического рефлектометра для локализации источников акустического воздействия в режиме реального времени, то есть для определения местоположения нарушителя на охраняемом объекте. Оценивалась чувствительность оптических трактов к акустическим воздействиям, соответствующим речевым сигналам предполагаемого нарушителя. Рассмотрен оптический тракт на основе оптического волокна в оптическом модуле с гидрофобным наполнением. Проведен анализ спектральной чувствительности исследуемых образцов оптических волокон. Представлена оценка влияния условий прохождения трассы прокладки оптического кабеля и взаимодействия акустического датчика с окружающими предметами. Приведен анализ результатов, полученных в ходе тестовых мероприятий на испытательном полигоне.

Ключевые слова: оптическое волокно, распределенный акустический датчик, оптический рефлектометр, злоумышленник, акусто-оптика.

Источник финансирования: Работа выполнена в рамках гранта аспирантам, соискателям и молодым ученым на проведение исследований, направленных на обеспечение информационной безопасности для задач цифровой экономики, договор № 40469-36/2021-Д.

Ссылка для цитирования: Картак В.М., Губарева О.Ю., Дашков М.В., Гуреев В.О., Евтушенко А.С. Исследование чувствительности оптических волокон в контексте локализации злоумышленника в защищенном помещении // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 52–58. DOI:10.31854/1813-324X-2023-9-1-52-58

Introduction

The development of the digital economy, which is based on the development of information networks, served as an impetus for the creation of a system of optical fibers spaced apart in space, laid at almost every modern facility. These systems provide new opportunities in terms of information security. In particular, it becomes possible not only to pick up audio information but also to determine the location of the sound source with given accuracy and subsequent identification of the sound source. For example, an attacker, observing a 3D model of a system of spaced-out objects, can determine which employees work in which rooms, track their daily routine, etc. From the object security point of view, video surveillance systems can be supplemented with audio monitoring systems and create complete 3D models of space, which is why it is advisable to develop models of distributed fiber-optic acoustic sensors spaced in 3D space. Until recently, wireless sensor networks (WSNs) were the most widely used to solve problems of determining the exact location [1–7]. However, WSNs do not have sufficient accuracy in determining the location of the sensor itself, which in turn affects the error in localizing the sound source [6, 7].

To solve the problem of determining with a given accuracy the location of an intruder at a protected facility, it was proposed to use the fiber-optic communi-

cation lines available at the facility with distributed acoustic sensors (DAS) installed on them [8–12]. One of the implementation methods was proposed by Gubareva O.Yu. and Burdin V.A. in patent RU2702983 [13]. Time Difference of Arrival (TDOA) systems built on the basis of DAS have a span in the distance between sensors of less than 1 m and a sensitivity of up to 90 dB [14–16]. It is worth considering that in addition to the desired source of acoustic impact, many other factors affect the sensor. For example, sources of extraneous noise, fluctuations of the medium in which the optical fiber is located, micro- and macro-bends, as well as compression and stretching of the optical fiber itself [17]. Today, almost all buildings have a network of fiber optic communication lines. Free optical fibers can be successfully used as a DAS to determine the location of a sound source, including an intruder. Based on the data obtained, it is proposed to build a digital 3D map of the object with an overlay on the video surveillance system to form adequate threat models. In addition, we can include the means of identifying and classifying information security threats existing at the facility for objects of various types and classes, as well as supplement user identification technology on the object.

After choosing the Algorithm of Simple Triangulation as the main method [18], the possibility of using communication lines already existing at urban devel-

opment sites in relation to physical protection tasks was considered. For this, an experimental test site was prepared on the territory of the university.

Intruder Localization at a Protected Facility

The simple triangulation algorithm investigates the acoustic impact on a set of sensor points [19]. Separate elementary sections x_i, x_{i+1} etc. are determined. The section length is equal to the DAS gauge length. An optical fiber is represented as a set of such elementary sections. Fig. 1 shows the impact on the elementary sections of the optical fiber by the sound source. Here r_0 is the shortest distance from the sound source to the fiber. It is assumed that the sound wave is incident perpendicularly.

Fig. 1 shows, that α_i is the acoustic beam incidence angle on the i -th elementary section of the optical fiber. Then its value can be defined as:

$$\alpha_i = \arccos\left(\frac{\phi_{i+1} - \phi_i}{k \cdot \Delta x}\right), \quad (1)$$

here ϕ is the phase obtained by analyzing the fiber backscattering characteristics, k is the wavenumber, Δx is the gauge length.

Knowing how the wave number and the speed of sound in air are calculated, we determine the shortest distance to the sound source:

$$x_{0i} = \frac{x_i \cdot \operatorname{tg} \alpha_i - x_{i+1} \cdot \operatorname{tg} \alpha_{i+1}}{\operatorname{tg} \alpha_i - \operatorname{tg} \alpha_{i+1}}, \quad (2)$$

$$r_{0i} = x_{0i} \cdot \operatorname{tg} \alpha_i. \quad (3)$$

For 3D space, the shortest distance from the optical fiber to the sound source will be determined by the formula:

$$r_0 = \sqrt{z_0^2 + y_0^2 + x_0^2}, \quad (4)$$

where z_0, y_0, x_0 and x_0 is the shortest distances to the sound source in Z, Y and X planes, accordingly.

One of the options for the location of the optical cable in the room to localize the sound source is shown in Fig. 2.

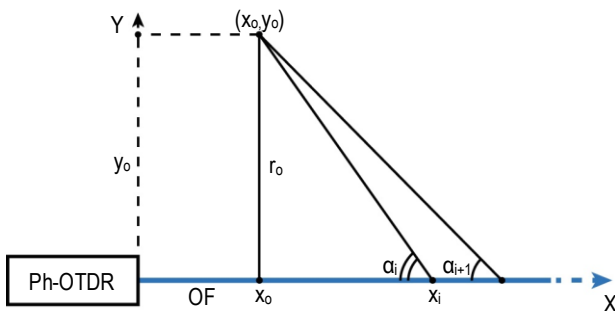


Fig. 1. Estimation of the Distance from the Optical Fiber to the Source of Acoustic Impact

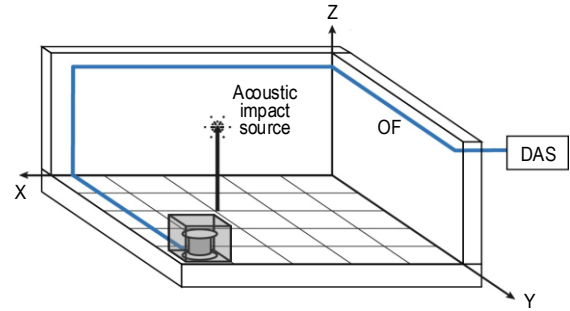


Fig. 2. Determining the Coordinates of the Sound Source

For each of the three axes of the optical fiber, we determine the corresponding values x_{01}, x_{02}, x_{03} . Then the sound source will be located on the plane as the intersection of three circles, the radii of which are equal to r_{01}, r_{02} , and r_{03} , accordingly. Next, we decompose the sound source into spectral characteristics and set the necessary conditions $\Delta\phi = \phi_{i+1} - \phi_i < 2\pi, k\Delta x < 2\pi$. All calculations are carried out only at low frequencies, cutting off parasitic noise and interference.

For typical DAS, the gauge length is in the range of 1.0–10 m [20, 21]. The response of the i -th segment of the DAS will be written as [22, 23]:

$$s_i(t) = \int_{x_{i,0}}^{x_{i,1}} \eta(x) \cdot \varepsilon(x, t) dx, \quad (5)$$

where $\varepsilon(x, t)$ is the optical fiber deformation equal to the ratio of fiber axial deformation Δl to fiber length l ; $\eta(x)$ is the response factor. It depends on the cable laying conditions, cable design, the position of the optical fiber in the cable, etc.

In general, the coefficient $\eta(x)$ varies along the fiber optic cable. However, in the first approximation, within the construction length of the optical cable, it can be assumed to be constant.

Consider the case of a plane wave. If we confine ourselves to the analysis for the far zone (assuming that the conditions for such an assumption are satisfied), then the acoustic field of a point source acting on the optical fiber of the cable is described as [23]:

$$P(t, x) = \frac{P_0}{r} \exp[j(\omega t - kr)], \quad (6)$$

$$r = \sqrt{(z - z_0)^2 + (y - y_0)^2 + (x - x_0)^2},$$

where x_0, y_0, z_0 are the coordinates of the source of acoustic signals, x, y, z are the coordinates of some point of the optical fiber, ω is the circular frequency, t is time, k is the wavenumber, P_0 is the amplitude of the acoustic signal at the output of the source.

Taking into account (5)–(6), the signal recorded by DAS from an optical fiber on an elementary section of the cable is described as:

$$P_C(t, x_i) = P_0 \times$$

$$\times \exp(j\omega t) \int_{x_{i,0}}^{x_{i,1}} \frac{\varepsilon(x, t) \eta(x)}{r} \exp(-jkr) dx. \quad (7)$$

It should be taken into account that for the effective application of such algorithms, information is needed on the sensitivity of optical fibers in an optical cable to external vibro-acoustic influences, as well as the spectral dependences of their responses.

Experimental Studies

A room close to real operating conditions was equipped for testing. The dimensions of the room were 5×5×2 m. There were areas with furniture along the optical fiber and areas without it. That way we can assess the influence of parasitic objects on the propagation of sound within the room and on the accuracy of determining the coordinates of the sound source. The acoustic effect was in the frequency sweep mode in the range from 100 to 1900 Hz for 180 seconds. Measurements were made with a polling frequency of 5 kHz and a measuring base of 5 meters. The obtained characteristics were processed using the Fourier window transform. The spectral characteristics and their dependence on the level of the influencing signal were analyzed. One optical cable was used, located in a configuration (Fig. 3), where it was possible to characterize the distribution of the amplitude of the sound signal acting on the optical cable in three planes with a shifted center of coordinates, and also to compare the response to the acoustic signal source of two parallel sections of the fiber.

As we can see in Fig. 3, the optical paths, parallel with X and Y axes have a common center of coordinates, while the optical path, parallel with Z axis is offset by 3 meters. One end of the optical fiber is connected to the DAS, the other end of the optical fiber is located in a buffer coil, fixed in space and isolated from various sound influences. Since the principle of DAS operation is based on comparing the characteristics of backscattering between fiber sensors at a distance equal to the gauge length, the isolated part of the fiber did not introduce additional errors when analyzing the behavior of the amplitude and phase of the acoustic signal. Fig. 4 shows the spectral characteristics of the acoustic signal obtained with DAS.



Fig. 3. Testing Site Structure. The Nearest Wall is Hidden for Better Visibility

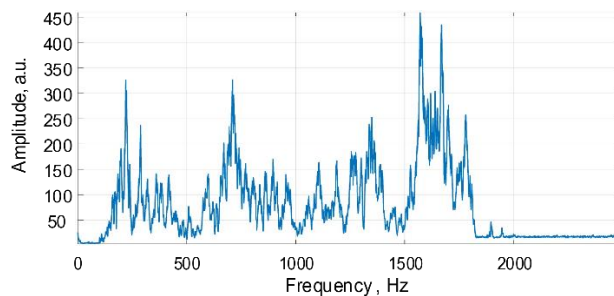


Fig. 4. Spectral Characteristics of the Acoustic Signal

As shown in Fig. 4, the maxima appear in the regions of 240, 650 and 1600 Hz. These ranges are typical for human speech and the sounds of object movement. The graph shown is the result of repeated testing under constant conditions. The constancy of the behavior of the maxima of the spectral components makes it possible to use them for statistical analysis.

Since in a real scenario the sound source (intruder) is not static in space, measurements were taken while moving the sound source. Fig. 5 shows the spectral characteristics of the acoustic signal. There is a homogeneity of the spectral characteristics obtained using DAS, which indicates the possibility of real-time acousto-optical analysis.

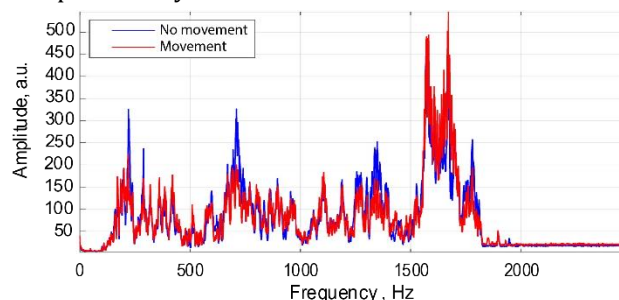


Fig. 5. Spectral Characteristics of the Acoustic Signal of a Source Moving in Space

It is also worth considering that measurements in real conditions can be carried out not from the point of the shortest distance from the fiber to the sound source, but from an array of fiber sensors in a particular room. Fig. 6 shows the results of the spectral analysis of the acoustic signal received from different points of the optical fiber on the test site. The characteristics of the amplitude distribution in three sections of the fiber were taken simultaneously, taking into account their mutual influence on each other.

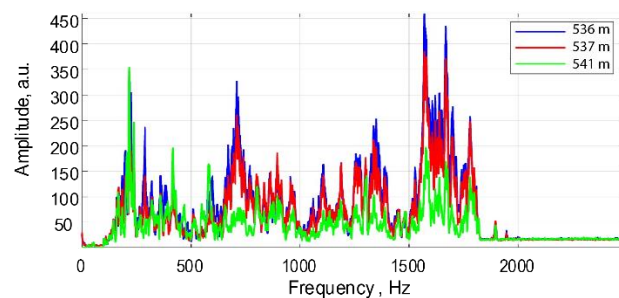


Fig. 6. Spectral Characteristics of the Acoustic Signal Obtained from Different Points of the DAS

The picture of the maxima is generally preserved, despite the presence of natural obstacles, the difference in distances from the sensor to the sound source, and the peculiarities of the location of the sensor itself.

In the course of the work, localization of the sound source was performed with the methods based on the amplitude and phase characteristics analysis of the acoustic signal spectral components. Fig. 7 shows the

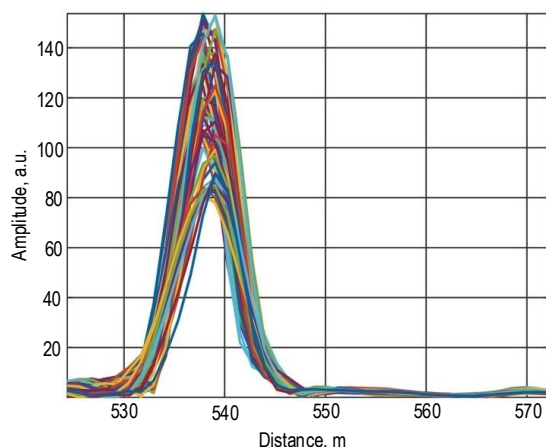


Fig. 7. Spectral Component Amplitude at a Frequency of 150 Hz, Time Variations with a Step of 1 Second

The amplitude indicators of the spectral characteristics make it possible to judge the coordinate of the sound source on the axis of the optical fiber. The results obtained make it possible to use the simple triangulation algorithm for localizing a sound source in three-dimensional space in real time using DAS on the basis of communication lines already existing in urban areas, based on such information transmission technologies as "fiber-to-the-office" and "fiber-to-the-workplace".

Of great interest for further research are configurations with higher acoustic frequencies. Although low-frequency signal has a greater effect on DAS, it has a tangible effect on all surrounding objects leading to an increased proportion of parasitic influences on sensor.

measurements of the ratio $P(t, x)/P_0$ amplitude distribution for the spectral component with a frequency of 240 Hz over time (with a step of 1 second) along the optical fiber. Fig. 8 shows a histogram of the values of the coordinate corresponding to the maximum of the spectral component. The approximation was made by the Gaussian function.

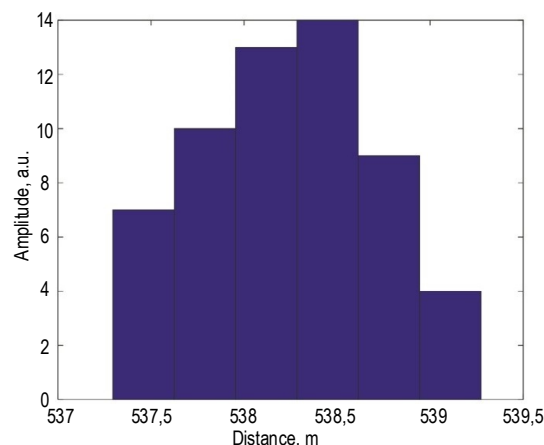


Fig. 8. Histogram of the Fiber Axis Coordinate Values Corresponding to the Spectral Component Maximum

Conclusion

During the experimental verification, the possibility of using DAS in the context of determining the location of the source of acoustic vibrations of different frequencies in space was established. The possibility of localizing the source of acoustic vibrations during its movement was proved. The possibility of source localization from different points of a DAS was shown. In addition, DAS can be used as an acoustic microphone. This will allow projecting onto the 3D map of the room not only the location of the source but also its sound-track. Additional tests will introduce the classification and identification of sound sources. This will expand the understanding of the actions of a potential attacker in a protected area.

References

1. Segura-Garcia J., Felici-Castell S., Perez-Solano J.J., Cobos M., Navarro J.M. Low-Cost Alternatives for Urban Noise Nuisance Monitoring Using Wireless Sensor Networks. *IEEE Sensors Journal*. 2015;15(2):836–844. DOI:10.1109/JSEN.2014.2356342
2. Bertrand A. Applications and trends in wireless acoustic sensor networks: A signal processing perspective. *Proceedings of the 18th IEEE Symposium on Communications and Vehicular Technology in the Benelux, SCVT, November 2011, Ghent, Belgium*. IEEE; 2011. p.1–6. DOI:10.1109/SCVT.2011.6101302
3. Cheng L., Wu C., Zhang Y., Wu H., Li M., Maple C. A Survey of Localization in Wireless Sensor Network. *International Journal of Distributed Sensor Networks*. 2012;8(12):962523. DOI:10.1155/2012/962523
4. Liu H., Darabi H., Banerjee P., Liu J. Survey of Wireless Indoor Positioning Techniques and Systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*. 2007;37(6):1067–1080. DOI:10.1109/TSMCC.2007.905750
5. Wang H. *Wireless sensor networks for acoustic monitoring*. Ph.D. Theses. Los Angeles: University of California, 2006.
6. Priyantha N.B., Chakraborty A., Balakrishnan H. The Cricket location-support system. *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, MobiCom '00, 6–11 August 2000, Boston, USA*. ACM; 2000. p.32–43. DOI:10.1145/345910.345917
7. Raykar V.C., Kozintsev I.V., Lienhart R. Position calibration of microphones and loudspeakers in distributed computing platforms. *IEEE Transactions on Speech and Audio Processing*. 2005;13(1):70–83. DOI:10.1109/TSA.2004.838540

8. Bucaro J.A., Dardy H.D., Carome E. F. Optical fiber acoustic sensor. *Applied Optics*. 1977;16(7):1761. DOI:10.1364/AO.16.001761
9. Kim B.Y., Blake J.N., Huang S.Y., Shaw H.J. Use of highly elliptical core fibers for two-mode fiber devices. *Optics Letters*. 1987;12(9):729. DOI:10.1364/OL.12.000729
10. Wang Y., Yuan H., Liu X., Bai Q., Zhang H., Gao Y., et al. A Comprehensive Study of Optical Fiber Acoustic Sensing. *IEEE Access*. 2019;7:85821–85837. DOI:10.1109/ACCESS.2019.2924736
11. Wild G., Hinckley S. Acousto-Ultrasonic Optical Fiber Sensors: Overview and State-of-the-Art. *IEEE Sensors Journal*. 2008;8(7):1184–1193. DOI:10.1109/JSEN.2008.926894
12. Gubareva O.Y. Potential capabilities of optical distributed acoustic sensors to determine the location of an intruder. Proceedings of the 18th International Scientific and Technical Conference on Optical Technologies for Telecommunications, 17–20 November 2020, Samara, Russian Federation. 2021: 33. DOI:10.1117/12.2593047
13. Burdin V.A., Gubareva O.Y. *Method of simplex data transmission over an optical fiber of a cable line*. Patent RF no. 2702983 C1, 14.10.2019. (in Russ.)
14. Treshchikov V.N. *Dunay software and hardware complex*. 2019. URL: <https://t8.ru/wp-content/uploads/2019/01/Dunay-2019-eng.pdf>.
15. Groznov D.I., Leonov A.V., Naniy O.E., Nesterov E.T., Treshchikov V.N. Dunay – a system for monitoring of activity in the buffer zone of the pipeline. *Oil Gas Expo*. 2014;4(36):51–53. (in Russ.)
16. Treshchikov V.N., Naniy O.E. *Distributed sensor of acoustic and vibration actions*. Patent RF no. 2532562 C1, 10.11.2014. (in Russ.)
17. Blake J.N., Engan H.E., Shaw H.J., Kim B.Y. Analysis of intermodal coupling in a two-mode fiber with periodic microbends. *Optics Letters*. 1987;12(4):281. DOI:10.1364/OL.12.000281
18. Gubareva O., Gureev V., Osipov O. Algorithms for Determining the Location of an Intruder Using DAS in Space. *Proceedings of the VIII International Conference on Information Technology and Nanotechnology, ITNT, 23–27 May 2022, Samara, Russian Federation*. IEEE; 2022. p.1–6. DOI:10.1109/ITNT55410.2022.9848680
19. Gubareva O.Y., Burdin V.A., Gureev V.O., Dashkov M.V., Gavryushin S.A., Masyuk S.S., et al. Localization method for all-dielectric fiber-optic cable. *Proceedings of the XIX International Scientific and Technical Conference on Optical Technologies for Telecommunications, 23–26 November 2021, Samara, Russian Federation*. 2022. p.27. DOI:10.1117/12.2631780
20. Pan Z., Liang K., Ye Q., Cai H., Qu R., Fang Z. Phase-sensitive OTDR system based on digital coherent detection. *Proceedings of the Conference and Exhibition on Optical Sensors and Biophotonics, 13–16 November 2011, Shanghai, China*. 2011. p.83110S. DOI:10.1364/ACP.2011.83110S
21. Wang S., Fan X., Liu Q., He Z. Distributed fiber-optic vibration sensing based on phase extraction from time-gated digital OFDR. *Optics Express*. 2015;23(26):33301. DOI:10.1364/OE.23.033301
22. Fenta M.C., Potter D.K., Szanyi J. Fibre Optic Methods of Prospecting: A Comprehensive and Modern Branch of Geophysics. *Surveys in Geophysics*. 2021;42(3):551–584. DOI:10.1007/s10712-021-09634-8
23. Huang Y., Benesty J. *Audio Signal Processing for Next-Generation Multimedia Communication Systems*. Boston: Kluwer Academic Publishers; 2004. URL: <http://link.springer.com/10.1007/b117685> [Accessed 29th May 2022]

Список источников

1. Segura-Garcia J., Felici-Castell S., Perez-Solano J.J., Cobos M., Navarro J.M. Low-Cost Alternatives for Urban Noise Nuisance Monitoring Using Wireless Sensor Networks // *IEEE Sensors Journal*. 2015. Vol. 15. Iss. 2. PP. 836–844. DOI:10.1109/JSEN.2014.2356342
2. Bertrand A. Applications and trends in wireless acoustic sensor networks: A signal processing perspective // *Proceedings of the 18th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT, Ghent, Belgium, November 2011)*. IEEE, 2011. PP. 1–6. DOI:10.1109/SCVT.2011.6101302
3. Cheng L., Wu C., Zhang Y., Wu H., Li M., Maple C. A Survey of Localization in Wireless Sensor Network // *International Journal of Distributed Sensor Networks*. 2012. Vol. 8. Iss. 12. P. 962523. DOI:10.1155/2012/962523
4. Liu H., Darabi H., Banerjee P., Liu J. Survey of Wireless Indoor Positioning Techniques and Systems // *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*. 2007. Vol. 37. Iss. 6. PP. 1067–1080. DOI:10.1109/TSMCC.2007.905750
5. Wang H. *Wireless sensor networks for acoustic monitoring*. Ph.D. Theses. Los Angeles: University of California, 2006.
6. Priyantha N.B., Chakraborty A., Balakrishnan H. The Cricket location-support system // *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00, Boston, USA, 6–11 August 2000)*. ACM, 2000. PP. 32–43. DOI:10.1145/345910.345917
7. Raykar V.C., Kozintsev I.V., Lienhart R. Position calibration of microphones and loudspeakers in distributed computing platforms // *IEEE Transactions on Speech and Audio Processing*. 2005. Vol. 13. Iss. 1. PP. 70–83. DOI:10.1109/TSA.2004.838540
8. Bucaro J.A., Dardy H.D., Carome E. F. Optical fiber acoustic sensor // *Applied Optics*. 1977. Vol. 16. Iss. 7. P. 1761. DOI:10.1364/AO.16.001761
9. Kim B.Y., Blake J.N., Huang S.Y., Shaw H.J. Use of highly elliptical core fibers for two-mode fiber devices // *Optics Letters*. 1987. Vol. 12. Iss. 9. P. 729. DOI:10.1364/OL.12.000729
10. Wang Y., Yuan H., Liu X., Bai Q., Zhang H., Gao Y., et al. A Comprehensive Study of Optical Fiber Acoustic Sensing // *IEEE Access*. 2019. Vol. 7. PP. 85821–85837. DOI:10.1109/ACCESS.2019.2924736
11. Wild G., Hinckley S. Acousto-Ultrasonic Optical Fiber Sensors: Overview and State-of-the-Art // *IEEE Sensors Journal*. 2008. Vol. 8. Iss. 7. PP. 1184–1193. DOI:10.1109/JSEN.2008.926894
12. Gubareva O.Y. Potential capabilities of optical distributed acoustic sensors to determine the location of an intruder // *Proceedings of the 18th International Scientific and Technical Conference on Optical Technologies for Telecommunications (Samara, Russian Federation, 17–20 November 2020)*. 2021. P. 33. DOI:10.1117/12.2593047

13. Бурдин В.А., Губарева О.Ю. Способ симплексной передачи данных по оптическому волокну кабельной линии. Патент на изобретение RUS 2702983 C1 от 30.05.2019. Оpubл. 14.10.2019.
14. Treshchikov V.N. Dunay software and hardware complex. 2019. URL: <https://t8.ru/wp-content/uploads/2019/01/Dunay-2019-eng.pdf>.
15. Грознов Д.И., Леонов А.В., Наний О.Е., Нестеров Е.Т., Трещиков В.Н. «Дунай» – система мониторинга активности в охранной зоне трубопровода // Экспозиция Нефть Газ. 2014. № 4(36). С. 51–53.
16. Трещиков В.Н., Наний О.Е. Распределенный датчик акустических и вибрационных воздействий. Патент на изобретение RUS 2532562 C1 от 17.07.2013. Оpubл. 10.11.2014.
17. Blake J.N., Engan H.E., Shaw H.J., Kim B.Y. Analysis of intermodal coupling in a two-mode fiber with periodic microbends // Optics Letters 1987. Vol. 12. Iss. 4. P. 281. DOI:10.1364/OL.12.000281
18. Gubareva O., Gureev V., Osipov O. Algorithms for Determining the Location of an Intruder Using DAS in Space // Proceedings of the VIII International Conference on Information Technology and Nanotechnology (ITNT, Samara, Russian Federation, 23–27 May 2022). IEEE, 2022. PP. 1–6. DOI:10.1109/ITNT55410.2022.9848680
19. Gubareva O.Y., Burdin V.A., Gureev V.O., Dashkov M.V., Gavryushin S.A., Masyuk S.S., et al. Localization method for all-dielectric fiber-optic cable // Proceedings of the XIX International Scientific and Technical Conference on Optical Technologies for Telecommunications (Samara, Russian Federation, 23–26 November 2021). 2022. P. 27. DOI:10.1117/12.2631780
20. Pan Z., Liang K., Ye Q., Cai H., Qu R., Fang Z. Phase-sensitive OTDR system based on digital coherent detection // Proceedings of the Conference and Exhibition on Optical Sensors and Biophotonics (Shanghai, China, 13–16 November 2011). 2011. P. 83110S. DOI:10.1364/ACP.2011.83110S
21. Wang S., Fan X., Liu Q., He Z. Distributed fiber-optic vibration sensing based on phase extraction from time-gated digital OFDR. Optics Express. 2015. Vol. 23. Iss. 26. P. 33301. DOI:10.1364/OE.23.033301
22. Fenta M.C., Potter D.K., Szanyi J. Fibre Optic Methods of Prospecting: A Comprehensive and Modern Branch of Geophysics // Surveys in Geophysics. 2021. Vol. 42(3). PP. 551–584. DOI:10.1007/s10712-021-09634-8
23. Huang Y., Benesty J. Audio Signal Processing for Next-Generation Multimedia Communication Systems. Boston: Kluwer Academic Publishers, 2004. URL: <http://link.springer.com/10.1007/b117685> (Accessed 29.05.2022)

Статья поступила в редакцию 28.11.2022; одобрена после рецензирования 27.02.2023; принята к публикации 28.02.2023.

The article was submitted 28.11.2022; approved after reviewing 27.02.2023; accepted for publication 28.02.2023.

Информация об авторах:

КАРТАК
Вадим Михайлович

доктор физико-математических наук, профессор, заведующий кафедрой вычислительной техники и защиты информации Уфимского государственного авиационного технического университета,
 <https://orcid.org/0000-0001-8167-8291>

ГУБАРЕВА
Ольга Юрьевна

кандидат технических наук, начальник управления научной и инновационной деятельности Поволжского государственного университета телекоммуникаций и информатики,
 <https://orcid.org/0000-0003-4177-0370>

ДАШКОВ
Михаил Викторович

кандидат технических наук, и. о. заведующего кафедрой линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики,
 <https://orcid.org/0000-0002-3919-4151>

ГУРЕЕВ
Владимир Олегович

аспирант кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики,
 <https://orcid.org/0000-0001-5148-6432>

ЕВТУШЕНКО
Александр Сергеевич

инженер кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики,
 <https://orcid.org/0000-0001-5677-7802>

Научная статья

УДК 004.055

DOI:10.31854/1813-324X-2023-9-1-59-73



Тестирование облачных систем видеоконференцсвязи на основе параметра Хёрста

Руслан Валентинович Киричек¹, kirichek@sut.ru
Александр Александрович Берёзкин¹✉, berezkin.aa@sut.ru
Дмитрий Сергеевич Кукунин¹, kukunin.ds@sut.ru
Андрей Вячеславович Колесников², andrei@iotas.ru

¹Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

²Ассоциация участников рынка интернета вещей
Москва, 101000, Российская Федерация

Аннотация: В статье рассматриваются вопросы тестирования популярных отечественных и зарубежных облачных систем видеоконференцсвязи (ВКС). Предложена методика тестирования и сравнения качественных параметров приложений ВКС на основе международного опыта. Оценка и сравнение услуг ВКС выполнены на основе вычисления параметра Хёрста потоков данных, формируемых исследуемыми облачными системами ВКС. Проведено тестирование различных приложений зарубежных и отечественных систем ВКС в различных режимах работы при разных параметрах качества канала связи.

Ключевые слова: качество восприятия, видеоконференцсвязь, параметр Хёрста, DION, Zoom, TrueConf, Webinar meetings, Cisco WebEx, Microsoft Teams, Discord

Ссылка для цитирования: Киричек Р.В., Берёзкин А.А., Кукунин Д.С., Колесников А.В. Тестирование облачных систем видеоконференцсвязи на основе параметра Хёрста // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 59–73. DOI:10.31854/1813-324X-2023-9-1-59-73

Analysis of Experience Quality Parameters of Cloud Video Conferencing Systems under Interference Conditions

Ruslan Kirichek¹, kirichek@sut.ru
Aleksandr Berezhkin¹✉, berezkin.aa@sut.ru
Dmitry Kukunin¹, kukunin.ds@sut.ru
Andrey Kolesnikov², andrei@iotas.ru

¹The Bonch-Bruевич Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

²Association of Internet of Things Market Participants
Moscow, 101000, Russian Federation

Abstract: The article deals with the testing of popular domestic and foreign cloud videoconferencing systems. A methodology for testing and comparing qualitative parameters of videoconferencing applications based on international experience is proposed. Assessment and comparison of videoconferencing services is based on the calculation of Hurst data flows, formed by the investigated cloud videoconferencing systems. Various applications of

foreign and domestic videoconferencing systems have been tested in different operation modes with different channel quality parameters.

Keywords: quality of experience, video conferencing, Hurst parameter, DION, Zoom, TrueConf, Webinar meetings, Cisco WebEx, Microsoft Teams, Discord

For citation: Kirichek R., Berezkin A., Kukunin D., Kolesnikov A. Analysis of Experience Quality Parameters of Cloud Video Conferencing Systems under Interference Conditions. *Proc. of Telecom. Universities*. 2023;9(1):59–73. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-59-73

Введение

Видеоконференции стали важным инструментом эффективного общения и сотрудничества для предприятий, школ и частных лиц. С появлением облачных систем видеоконференцсвязи (ВКС) крайне важно обеспечить, чтобы эти системы были должным образом протестированы перед развертыванием. Тестирование облачных систем ВКС помогает выявить и устранить любые потенциальные проблемы, которые могут повлиять на пользовательский опыт и качество восприятия. Например, система может быть протестирована, чтобы убедиться в ее способности обрабатывать большое количество пользователей, в соответствующем качестве звука и видео, а также в том, что она безопасна и защищена от киберугроз.

Кроме того, тестирование помогает оптимизировать производительность облачных систем ВКС. Его можно использовать для оценки пропускной способности сети, ресурсов сервера и других компонентов, которые имеют решающее значение для бесперебойной работы ВКС. Кроме того, это может помочь определить наиболее эффективные настройки приложений ВКС, такие как пропускная способность и сжатие, которые можно установить в соответствии с потребностями различных пользователей и вариантами использования.

Еще одним важным преимуществом тестирования облачных систем ВКС является то, что это может помочь улучшить общий пользовательский опыт. Хорошо спроектированная и должным образом протестированная система ВКС может обеспечить надежную и бесперебойную связь с минимальными техническими проблемами. Это может повысить удовлетворенность пользователей и стимулировать дальнейшее использование, что поспособствует более широкому внедрению и росту системы ВКС.

В настоящее время российским пользователям доступно множество облачных систем ВКС, причем некоторые из них, например, DION, Webinar meetings или TrueConf развиваются на основе отечественных разработок. Другая группа облачных ВКС представлена решениями западных IT-компаний – Cisco WebEx, Microsoft Teams, Zoom US и др.

Однако важно отметить, что в настоящее время не существует общего стандарта для тестирования

облачных систем ВКС. Это означает, что каждая компания или организация вынуждены разрабатывать свои собственные протоколы и процедуры тестирования.

В результате исследования рекомендаций ITU-T выявлено, что наиболее близкой к задаче тестирования облачных систем ВКС является Рекомендация ITU-T Q.3949 [1]: *Real-time multimedia service testing framework at the user-to-network interface of next generation networks*, где описываются процедуры, требования, физические конфигурации и стандартные комплекты документов для тестирования мультимедийных услуг в режиме реального времени на интерфейсе «пользователь – сеть» (UNI, аббр. от англ. User-to-Network Interface) сетей следующего поколения (NGN, аббр. от англ. Next Generation Networks), что может быть использовано как основа для тестирования облачных систем ВКС.

Облачные системы ВКС в терминологии NGN могут рассматриваться как «End-to-End»-услуги между терминалами абонентов, где тестируемые оконечные услуги (Test Subject) находятся по обе стороны канала связи. На рисунке 1 показана физическая конфигурация для тестирования услуги ВКС на основе [1], где Клиент 1 и Клиент 2 – оконечные устройства и ПО для проведения ВКС (Terminal-A, Terminal-B); сеть NGN – облачная система ВКС в сети интернет; UNI – интерфейс доступа оконечных устройств к сети интернет.

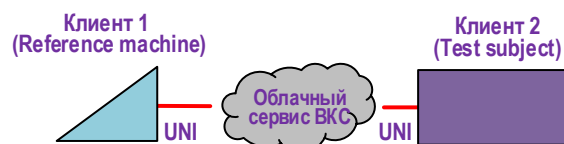


Рис. 1. Типовая физическая конфигурация для тестирования облачных систем ВКС в соответствии с Рекомендацией ITU-T Q.3949 [1]

Fig. 1. Typical Physical Configuration for Testing Video Conferencing Cloud Systems in Accordance with Recommendation ITU-T Q.3949 [1]

В [1] определены критерии тестирования протокола взаимодействия службы с услугами NGN, однако порядок тестирования сеанса аудио- и видеосвязи не определен. В предлагаемой методике тестирования выявляется порядок тестирования сценария 3 «сеанс аудио- и видеосвязи» Рекомендации Q.3949. Оценка качества услуги ВКС QoS (аббр. от англ. Quality of Service) определяется че-

рез оценку качества восприятия QoE (аббр. от англ. Quality of Experience)

Оценка качества восприятия

QoE – это мера удовольствия или раздражения клиента от использования услуги (например, системы ВКС), которая фокусируется на всем опыте обслуживания. QoE является новой междисциплинарной областью, основанной на социальной психологии, когнитивной науке, экономике и инженерных науках, ориентированной на понимание общих требований к качеству восприятия человеком. Качество восприятия зависит от нескольких факторов (рисунок 2) как субъективных, так и объективных [2]. В первом случае на оценку пользователя влияет его опыт работы с другими услугами.

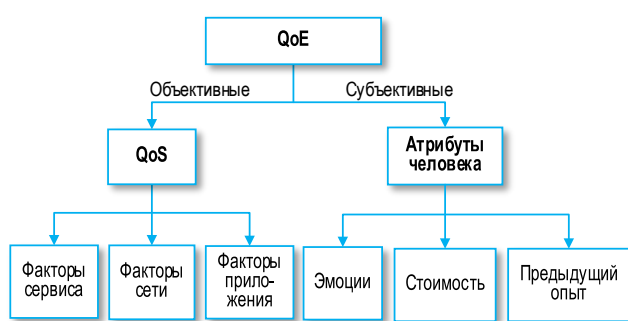


Рис. 2. Объективные и субъективные параметры оценки QoE

Fig. 2. Objective and Subjective Parameters of QoE Assessment

Главной метрикой объективных факторов QoE выступает QoS. В этом случае впечатления абонента формирует производительность и стабильность предоставляемой услуги, наличие/отсутствие артефактов при просмотре видео, задержки при взаимодействии с услугой, а также посторонние щелчки и шумы при передаче аудиоданных. Для тестирования систем ВКС необходимо определить измеримые показатели качества, которые позволяют связать QoE с QoS.

Применяемые на сегодняшний день методы оценки качества передачи видео, основанные на анализе характеристик сети, являются фактически теми же средствами, что используются для контроля качества передачи голосовой информации, т. е. они измеряют параметры транспортной сети [3–11]. В отличие от субъективных методов объективные не дают представления о том, что же на самом деле видит пользователь на экране, т. к. они не делают различия между пакетами, передающими видео, и пакетами, передающими другую информацию. Для того, чтобы измерить в количественном отношении качество услуг ВКС и сравнить их между собой, необходимо ввести определенную метрику. На сегодняшний день не разработано рекомендаций, определяющих введение какой-либо метрики, поэтому известен ряд методов, которые имеют существенные различия меж-

ду собой и базируются на разных подходах: Media Delivery Index (MDI), Video Quality Metric (VQM), Moving Pictures Quality Metric (MPQM), Noise Quality Measure (NQM) и т. д. Данные методы можно отнести к общим методам оценки работоспособности сети, в полной мере не учитывающих особенности приложения. Кроме того, предлагаемые подходы оценки QoE на основе E-модели [12] очень ресурсоемкие и имеют граничные условия использования.

Особенности передачи видео по IP-сетям требуют разработки новых показателей оценки QoE [13, 14]. Исследования показывают, что видеотрафик для большинства видов услуг является самоподобным [15–18]. Учет самоподобных свойств видеотрафика предоставляет возможность более точного оценивания видеопоследовательности, что, в свою очередь, позволяет улучшить методы оценки качества передачи видео и получить показатели QoE, близкие к реально наблюдаемым. Одним из показателей объективной оценки качества видео, так называемый V-фактор, по аналогии с R-фактором для речи, является параметр Хёрста [19–21], учитывающий степень самоподобия мультимедийного трафика, передаваемого в рамках функционирования облачных систем ВКС. Доказано, что видеотрафик обладает свойством самоподобия. Таким образом, отслеживая параметр Хёрста, можно наблюдать за наличием видеотрафика в сети, а по изменениям значений параметра прогнозировать изменения характеристик видеопотока, что может повлиять на оценку качества восприятия.

В предлагаемой методике тестирования оценка QoE и сравнение облачных систем ВКС проводится на основе вычисления параметра Хёрста потоков данных, формируемых исследуемыми системами.

Методика тестирования

В рамках исследования проводились испытания следующих приложений: Zoom, Cisco WebEx, DION, Discord, Microsoft Teams, TrueConf и Webinar meetings. Для проведения тестирования составлен чек-лист, включающий в себя возможные конфигурации системы приложения для конференций, а также значения параметров дополнительной искусственной задержки и потерь пакетов для осуществления тестирования надежности и отказоустойчивости системы. Дополнительная искусственная задержка и потери пакетов на приемной стороне тракта ВКС введены с целью реализации каналов связи различного качества. В рассматриваемых условиях данные параметры дополнительно применяются к естественным задержкам передачи данных в сети Интернет. Далее под параметрами «Задержка» и «Потери» понимается искусственные задержки и потери пакетов, добав-

ляющие дополнительные значения параметров к естественным задержкам в сети Интернет. При этом, значение параметра равно нулю означает отсутствие такого искусственного добавления.

Реализован дизайн тест-кейсов (ТК) с применением техник тестирования [22]. Параметры, различные значения которых необходимо протестировать, определены в таблице 1.

ТАБЛИЦА 1. Параметры тестирования

TABLE 1. Testing Parameters

№ п/п	Наименование показателя	Возможные значения
1	OS Terminal-A	[Windows, MacOS, Linux, IOS, Android]
2	OS Terminal-B	[Windows, MacOS, Linux, IOS, Android]
3	Тип приложения Terminal-A	[Desktop Windows, Desktop MacOS, IOS mobile App, Android mobile App, Web application]
4	Тип приложения Terminal-B	[Desktop Windows, Desktop MacOS, IOS mobile App, Android mobile App, Web application]
5	Задержка, мс	[0, 50, 100, 200, 300]
6	Потери, %	[0, 0,5, 1, 3, 5]

Для составления списка тест-кейсов на основе тестируемых параметров необходимо применить техники тест-дизайна. Параметр «Задержка» принимает значения от 0 до бесконечности. При тестировании облачных систем ВКС использовано значение 300 мс, как достаточно большое с учетом наличия дополнительных задержек в сети Интернет. Это в достаточной степени согласуется с известными нормами класса 1 QoS, к которому относятся услуги ВКС [23], допускающие задержку до 400 мс. Однако если задержка более 100 мс, то качество связи начинает падать. Следовательно, для параметра «Задержка» можно выделить 2 класса эквивалентности (таблица 2).

ТАБЛИЦА 2. Классы эквивалентности параметра «Задержка»

TABLE 2. Equivalence Classes of the "Delay" Parameter

Класс эквивалентности, мс	Среднее значение, мс	Качество связи	Граничные условия, мс
[0–100]	50	приемлемое	[0, 100, 300]
[100–300]	200	неприемлемое	

При использовании техники граничных значений также необходимо учитывать значения, отличающиеся от граничных на один пункт (+1, –1). Однако при тестировании систем ВКС смоделировать задержку 99 и 101 мс с помощью имеющихся технических средств невозможно. В связи с тем, что тестирование параметров задержки и потерь не является тестированием, например, полей ввода в интерфейсе пользователя, где условная единица существенно влияет на поведение системы, то нет необходимости в его проведении вблизи

граничных значений. С помощью техник «Классы эквивалентности» и «Граничные условия» [23] были определены следующие значения для тестирования параметра «Задержка»: 0, 50, 100, 200 и 300 мс.

Для параметра «Потери» также можно выделить 2 класса эквивалентности (таблица 3).

ТАБЛИЦА 3. Классы эквивалентности параметра «Потери»

TABLE 3. Equivalence Classes of the "Loss" Parameter

Класс эквивалентности, %	Среднее значение, %	Качество связи	Граничные условия, %
[0–1]	0,5	приемлемое	[0, 1, 5]
[1–5]	3	неприемлемое	

При тестировании систем ВКС смоделировать потери 0,9 и 1,1 % с помощью имеющихся технических средств оказалось невозможным. Поэтому для случая с параметром «Потери» также нет необходимости в проведении тестирования вблизи граничных значений. С помощью техник «Классы эквивалентности» и «Граничные условия» были определены следующие значения для тестирования параметра «Потери»: 0, 0,5, 1, 3 и 5 %.

Применение техник тест-дизайна позволяет прийти к оптимальному количеству тестов и покрыть наиболее распространенные конфигурации использования тестируемого программного обеспечения. Для создания тест-кейсов с наивысшим приоритетом необходимо, руководствуясь целью тестирования, определить параметры, тестирование значений которых наиболее приоритетно. Для создания остальных тест-кейсов целесообразно применить технику «Попарное тестирование».

С учетом наиболее часто используемых сценариев применения ПО ВКС определен приоритет тест-кейсов (таблицы 4–7). Приоритеты тест-кейсов обозначены как P0 (высокий), P1 (средний) и P2 (низкий).

В группе тест-кейсов P0 в таблице 5 приведены устанавливаемые числовые значения джиттера задержек и потерь пакетов, где джиттер вычисляется случайным образом в течение указанного периода времени. Например, значение «400 мс → 5000 мс» в столбце 4 устанавливает джиттер от 1 до 400 мс в течение 5000 мс. То же самое относится и к параметру потерь пакетов в столбце 5 таблицы 5. Порядковые номера таких параметров в таблице указывают на последовательность изменения параметров джиттера. При этом в тест-кейсе P0_8 значения джиттера не менялись. В последнем столбце таблицы 5 указаны параметры изменения содержимого пакетов данных. Например, значение «15 (1–10 шт.)» означает, что в 15 % случаев изменялось содержимое пакетов длиной от 1 до 10 штук. При этом длины пакетов выбираются случайным образом. Для рас-

чета параметра Хёрста необходимо произвести регистрацию количества пакетов, переданных по лучателю с течением времени $N(t)$ в процессе работы сеанса ВКС для каждого тест-кейса.

ТАБЛИЦА 4. Группа тест-кейсов высокого приоритета (P0)

TABLE 4. Group of High Priority Test Cases (P0)

Код ТК	Terminal-A	Terminal-B	Задержка, мс	Потери, %
P0_1	Windows web browser	Windows web browser	0	0
P0_2	Windows web browser	Windows web browser	50	0,5
P0_3	Windows web browser	Windows web browser	100	1
P0_4	Windows web browser	Windows web browser	200	3
P0_5	Windows web browser	Windows web browser	300	5

ТАБЛИЦА 5. Группа тест-кейсов P0 (экстремальные значения параметров)

TABLE 5. Group of Test Cases P0 (extreme values of parameters)

Код ТК	Terminal-A	Terminal-B	Задержка/джиттер, мс	Потери/джиттер, %	Изменение содержимого пакетов, %
P0_6	Windows web browser	Windows web browser	1)400 мс → 5000 мс 2)0 мс → 2000 мс 3)300 мс → 5000 мс 4)0 мс → 2000 мс 5)100 мс → 5000 мс 6)0 мс → 2000мс	1)0 % → 20000 мс 2)10 % → 10000 мс 3)20 % → 10000 мс 4)30 % → 10000 мс 5)20 % → 10000 мс 6)10 % → 10000 мс 7)5 % → 10000 мс	15 (1–10 шт.)
P0_7	IOS mobile	IOS mobile	1)400 мс → 5000 мс 2)0 мс → 2000 мс 3)300 мс → 5000 мс 4)0 мс → 2000 мс 5)100 мс → 5000 мс 6)0 мс → 2000 мс	1)0 % → 20000 мс 2)10 % → 10000 мс 3)20 % → 10000 мс 4)30 % → 10000 мс 5)20 % → 10000 мс 6)10 % → 10000 мс 7)5% → 10000 мс	15 (1–10 шт.)
P0_8	Windows desktop	Windows desktop	400	30	20 (1–50 шт.)

ТАБЛИЦА 6. Группа тест-кейсов среднего приоритета (P1)

TABLE 6. Group of Medium Priority Test Cases (P1)

Код ТК	Terminal-A	Terminal-B	Задержка, мс	Потери, %
P1_1	Windows web browser	Android mobile	200	3
P1_2	MacOS web browser	MacOS web browser	100	3
P1_3	MacOS web browser	IOS mobile	200	0
P1_4	MacOS web browser	Android mobile	0	0,5
P1_5	MacOS web browser	Windows web browser	50	1
P1_6	IOS mobile	IOS mobile	0	1
P1_7	IOS mobile	Android mobile	50	3
P1_8	IOS mobile	Windows web browser	100	0
P1_9	IOS mobile	MacOS web browser	200	0,5
P1_10	Android mobile	Android mobile	100	0,5
P1_11	Android mobile	Windows web browser	200	1
P1_12	Android mobile	MacOS web browser	0	3
P1_13	Android mobile	IOS mobile	50	0
P1_14	Windows web browser	Android mobile	200	3
P1_15	MacOS web browser	MacOS web browser	100	3

ТАБЛИЦА 7. Группа тест-кейсов низкого приоритета (P2)

TABLE 7. Group of Low Priority Test Cases (P2)

Код ТК	Terminal-A	Terminal-B	Тип канала связи	Задержка, мс	Потери, %
P2_1	Windows web browser	Windows web browser	WiFi	300	5
P2_2	Windows Desktop	Windows Desktop	WiFi	100	1
P2_3	MacOS Desktop	MacOS Desktop	WiFi	200	3
P2_4	Windows Desktop	Windows Desktop	WiFi	0	0
P2_5	MacOS Desktop	Windows Desktop	WiFi	50	0,5
P2_6	Windows Desktop	Windows Desktop	WiFi	300	5
P2_7	Android mobile	Android mobile	LTE	0	0
P2_8	Android mobile	IOS mobile	LTE	50	0,5
P2_9	Android mobile	Android mobile	LTE	100	1
P2_10	IOS mobile	Android mobile	LTE	200	3
P2_11	IOS mobile	IOS mobile	LTE	0	0

Сбор и обработка данных проводились при различных условиях состояния сети с варьированием искусственной задержки пакетов (0, 50, 100 и 200 мс) и вероятности потери пакетов (0, 0,5, 1 и 3 %). В качестве инструмента сбора статистических данных был использован анализатор сетевого трафика TamiSoft CommView версии 7.0. После установки связи между клиентами системы ВКС осуществлялся захват сетевого трафика. Длительность захвата трафика составляла $T = 300$ с. По завершению периода сбора данных захват трафика прекращался. Далее с помощью инструментов CommView выгружались статистические данные по принятым пакетам, которые модифицировались в массив данных, необходимый для расчета параметра Хёрста. Результаты вычисления параметра Хёрста для всех систем ВКС при тест-кейсах разных групп приоритета заносятся в таблицу 8, где H_{ij} – значение параметра Хёрста для i -й системы ВКС и j -го тест-кейса; N – количество тест-кейсов соответствующего приоритета $P0$, $P1$ и $P2$.

Заполнение таблицы 8, где i – порядковый номер ВКС; j – порядковый номер тест-кейса производятся в следующей последовательности:

- 1) для всех $i = 1 \dots 7$ и $j = 1 \dots N_{P0}$;
- 2) для всех $i = 1 \dots 7$ и $j = (N_{P0} + 1) \dots N_{P1}$;
- 3) для всех $i = 1 \dots 7$ и $j = (N_{P1} + 1) \dots N_{P2}$.

Оценка параметра Хёрста для каждой ВКС производится на основе аддитивной свертки. Каждо-

му тест-кейсу в зависимости от экспертного решения был назначен весовой коэффициент k_j , где j – порядковый номер тест-кейса. Значения весовых коэффициентов назначаются в соответствии с важностью тест-кейса и для каждой i -й ВКС в рамках своей группы важности ($P0$, $P1$ и $P2$) удовлетворяют условиям:

$$\sum_{j=1}^{N_{P0}} k_j^{P0} = 1, \quad \sum_{j=(N_{P0}+1)}^{N_{P1}} k_j^{P1} = 1, \quad \sum_{j=(N_{P1}+1)}^{N_{P2}} k_j^{P2} = 1 \quad (2)$$

Вычисление параметра Хёрста H^{P0} в первом диапазоне $P0$ позволит определить его базовое значение для самых важных тест-кейсов:

$$H_j^{P0} = \sum_{j=1}^{N_{P0}} k_j^{P0} H_{ij} = 1. \quad (3)$$

Вычисление параметра Хёрста H^{P1} во втором диапазоне $P1$ при наличии достаточного временного ресурса позволит произвести его определение для менее важных тест-кейсов:

$$H_j^{P1} = \sum_{j=(N_{P0}+1)}^{N_{P1}} k_j^{P1} H_{ij} = 1. \quad (4)$$

ТАБЛИЦА 8. Параметр Хёрста для группы тестов [$P0$, $P1$, $P2$]TABLE 8. Hurst Parameter for the Test Group [$P0$, $P1$, $P2$]

№ п/п	Тест-кейс	Cisco WebEx	Zoom	Microsoft Teams	Webinar meetings	DION	TrueConf	Discord
1	$P[0,1,2]_1$	H_{11}	H_{12}	H_{13}	H_{14}	H_{15}	H_{16}	H_{17}
2	$P[0,1,2]_2$	H_{21}	H_{22}	H_{23}	H_{24}	H_{25}	H_{26}	H_{27}
...								
N	$P[0,1,2]_3$	H_{N1}	H_{N2}	H_{N3}	H_{N4}	H_{N5}	H_{N6}	H_{N7}

Вычисление параметра Хёрста H^{P2} в третьем диапазоне $P2$ также при наличии достаточного временного ресурса позволит произвести его определение для оставшихся тест-кейсов, которые являются наименее важными, но вносят определенный вклад в точность вычисления данного параметра:

$$H_j^{P2} = \sum_{j=(N_{P1}+1)}^{N_{P2}} k_j^{P2} H_{ij} = 1. \quad (5)$$

Таким образом, вычисление базового значения параметра Хёрста для всех ВКС (2) являлось минимальной задачей. Наличие достаточного временного ресурса позволило повысить точность его вычисления за счет определения (4) и (5). При этом необходимо было снова задействовать принцип аддитивной свертки и назначить весовые коэффициенты K каждой группе важности, чтобы выполнялось условие:

$$K_{P0} + K_{P1} + K_{P2} = 1. \quad (6)$$

В таком случае более точное значение параметра Хёрста при всех N выполненных тест-кейсах для каждой i -й ВКС вычисляется по формуле:

$$H_i = K_{P0} H_i^{P0} + K_{P1} H_i^{P1} + K_{P2} H_i^{P2}. \quad (7)$$

Далее результаты (7) были упорядочены по убыванию H_i и проранжированы.

Итогом данного этапа исследования является выбор трех ВКС с наименьшим рангом R_i . Для них в дальнейшем могут проводиться дополнительные исследования для субъективной оценки качества. В данном тестировании субъективная оценка качества не проводилась.

Описание стенда

На рисунке 4 изображена структура стенда для тестирования облачных систем ВКС.

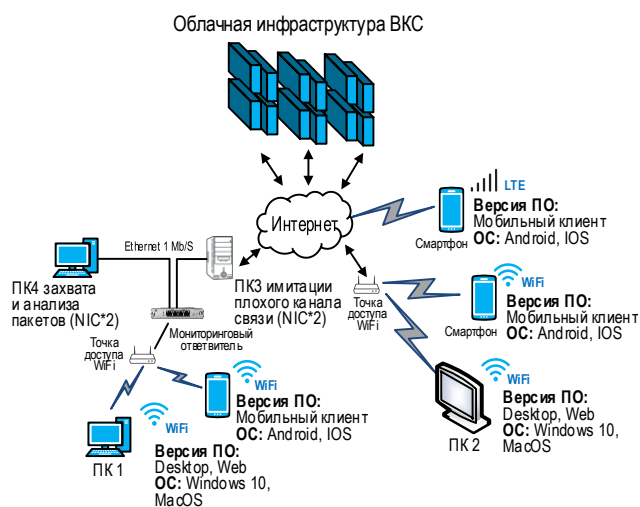


Рис. 4. Структура стенда

Fig. 4. Structure of the Stand

Архитектурно с помощью элемента имитации плохого канала связи система позволяет реализовать взаимодействие по различным типам каналов связи за счет управления дополнительной задержкой и потерями пакетов. Для более универсального типа подключения элементов использован канал подключения по WiFi.

Элементы стенда.

1) *Смартфон* – мобильный телефон Huawei Honor 7C под управлением ОС Android версия 12.4.2.1 и iPhone 12 под управлением ОС IOS версии 15.2 с установленными мобильными приложениями исследуемых систем ВКС.

2) *ПК1 и ПК2* – ноутбук под управлением Windows 10 версии 21H2 и MacOS версии 12.2.1 с установленными desktop приложениями систем ВКС.

3) *ПК3* – персональный компьютер под управлением ОС Windows 10 с установленным программным обеспечением имитации плохого канала связи NetDisturb (<https://www.zti-communications.com/netdisturb>) версии 7.0.15.

NetDisturb – это программное обеспечение эмулятора сети (IPv4 и IPv6), генерирующее определяемые пользователем искажения: задержку, джиттер, ограничение пропускной способности, потерю пакетов, дублирование пакетов, изменение содержимого пакета и многое другое.

4) *ПК4* – персональный компьютер под управлением ОС Windows 10 с установленным программным обеспечением для захвата и анализа пакетов TamiSoft CommView версии 7.0.

5) *Мониторинговый ответвитель* – устройство контроля трафика Net Optics Gig Zero Delay™ Tap. Ответвитель 10/100/1000BaseT с нулевой задержкой, обеспечивающий пассивный доступ без помех потоку данных на скоростях 10/100/1000 Мбит/с.

Результаты тестирования

В соответствии с методикой тестирования введены коэффициенты важности тест-кейсов в группах $P0$, $P1$ и $P2$ (таблица 9–11), а также самих групп (таблица 12). Тест-кейсы на плохих каналах связи имеют больший вес, чем на хороших (задержка не более 100 мс, потери менее 1 %). Это важно для смещения фокуса оценки систем с точки зрения их устойчивости к изменению параметров и типа канала связи.

ТАБЛИЦА 9. Коэффициенты важности тест-кейсов группы $P0$

TABLE 9. Coefficients of Importance of Test Cases of Group $P0$

код ТК	$P0_1$	$P0_2$	$P0_3$	$P0_4$	$P0_5$	$P0_6$	$P0_7$	$P0_8$
k^{P0}	0,1	0,1	0,1	0,1	0,1	0,14	0,14	0,22

ТАБЛИЦА 10. Коэффициенты важности тест-кейсов группы P1

TABLE 10. Importance Ratios of test Cases in Group P1

код ТК	P1_1	P1_2	P1_3	P1_4	P1_5	P1_6	P1_7	P1_8
k^{P0}	0,03	0,07	0,12	0,1	0,07	0,03	0,07	0,07
код ТК	P1_9	P1_10	P1_11	P1_12	P1_13	P1_14	P1_15	
k^{P0}	0,1	0,03	0,07	0,03	0,09	0,09	0,03	

ТАБЛИЦА 11. Коэффициенты важности тест-кейсов группы P2

TABLE 11. Importance Ratios of Test Cases in Group P2

код ТК	P2_1	P2_2	P2_3	P2_4	P2_5	P2_6	P2_7	P2_8	P2_9	P2_10	P2_11
k^{P0}	0,15	0,07	0,11	0,07	0,07	0,14	0,07	0,07	0,07	0,11	0,07

ТАБЛИЦА 12. Коэффициенты важности групп тест-кейсов

TABLE 12. Importance Ratios for Groups of Test Cases

группа тест-кейсов	P0	P1	P2
K	$K_{P0} = 0,5$	$K_{P1} = 0,3$	$K_{P2} = 0,2$

Вычисленные средние значения параметра Хёрста в соответствии с выражениями (3–7) для исследуемых систем в заданных диапазонах и весовых коэффициентов важности представлены в таблице 13. Результат ранжирования систем ВКС представлен в таблице 14.

ТАБЛИЦА 13. Средние значения параметра Хёрста

TABLE 13. Average Values of the Hurst Parameter

Система	Cisco WebEx	Zoom	MS Teams	Webinar meetings	DION	TrueConf	Discord
H^{P0}	0,9448	0,9439	0,9315	0,8476	0,9303	0,8981	0,9084
H^{P1}	0,9522	0,9716	0,9387	0,9474	0,9365	0,9284	0,9330
H^{P2}	0,9308	0,9504	0,94	0,94	0,9255	0,8962	0,9162
H	0,9442	0,9535	0,9354	0,8961	0,9312	0,9068	0,9174

ТАБЛИЦА 14. Ранжирование результатов

TABLE 14. Ranking of Results

	Zoom	Cisco WebEx	MS Teams	DION	Discord	TrueConf	Webinar meetings
H	0,95	0,94	0,94	0,93	0,92	0,91	0,90
N	1	2	3	4	5	6	7
R	1	2,5	2,5	4	5	6	7
Позиция	1 место	2 место		3 место	4 место	5 место	6 место

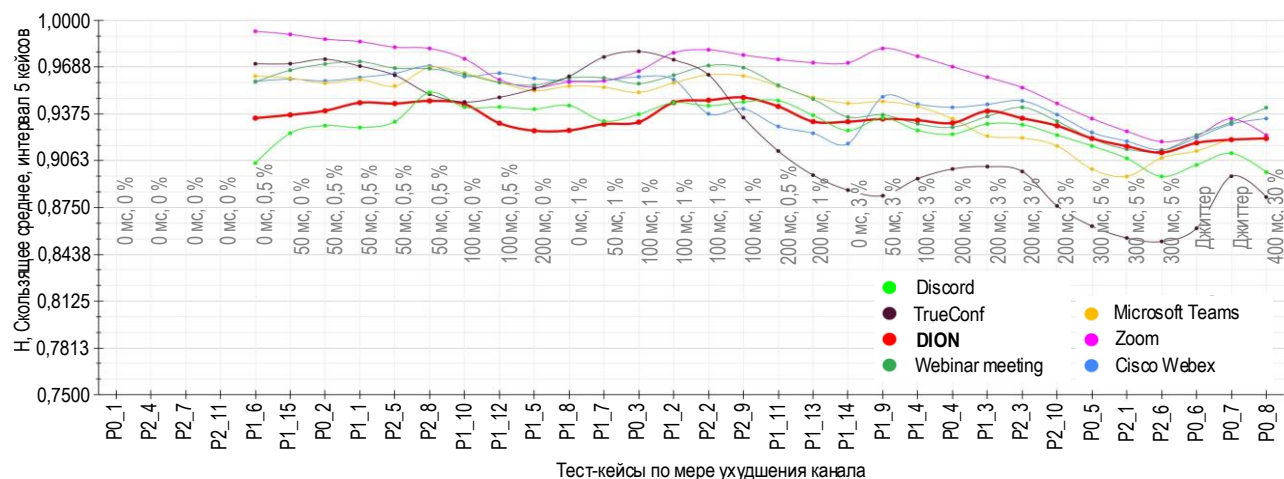


Рис. 5. Зависимость параметра Хёрста от качества канала связи

Fig. 5. The Dependence of the Hurst Parameter on the Quality of the Communication Channel

Анализ результатов показывает, что лучшей системой с точки зрения QoE является Zoom. Второе место поделили между собой Cisco WebEx и MS Teams. DION занял третье место.

Анализ результатов

В целях всесторонней оценки качества рассматриваемых систем ВКС необходимо изучить влияние различных показателей качества.

Для анализа были определены следующие показатели:

- параметр Хёрста (H);
- средняя длина пакетов данных (L);
- зависимость (в том числе взаимная корреляция) H от L ;
- типы используемых приложений.

На рисунке 5 представлена зависимость параметра Хёрста от качества канала связи, при этом тест-кейсы отсортированы по мере ухудшения качества канала. Для сглаживания краткосрочных колебаний с целью определения долгосрочного тренда данный график преобразован через скользящее среднее, где размер «окна» установлен в 5 значений.

Выводы

Во-первых, при ухудшении качества канала связи для всех систем наблюдается общее снижение параметра Хёрста. При этом, система DION при нулевых значениях задержек и потерь пакетов работает около нижней границы оценки параметра Хёрста. В то же время, при больших потерях в каналах связи система DION «проходит» близко к верхней границе. В плохих каналах связи значения параметра Хёрста всех рассматриваемых систем существенно снижаются и по своим значениям приближаются к значению DION.

Во-вторых, система TrueConf уже при небольшом значении потерь и задержек в канале связи имеет самый низкий параметр Хёрста. Это может означать, что данная система в большей степени предназначена для работы только в условиях хороших каналов.

В-третьих, система Zoom имеет наиболее стабильно высокое значение параметра Хёрста при любых каналах связи.

В-четвертых, система DION менее устойчива к переменным значениям качества канала связи (джиттер) (тест-кейсы P0_6 и P0_7), чем остальные системы (рисунок 6а). Особенно это заметно в тест-кейсе P0_7 при использовании мобильного приложения (IOS mobile – IOS mobile).

В-пятых, в тест-кейсе P0_8 (рисунок 6б) были установлены экстремальные значения с очень плохими параметрами канала связи: задержка 400 мс, потери 30 %, изменение содержимого пакетов 20 % со случайными пачками пакетов от 1 до 50 штук. В данном случае видно, что система DION имеет высокий показатель при экстремальных значениях.

Такой показатель достигается за счет получения большего количества пользовательских данных в единицу времени на приемной стороне за

счет использования пакетов небольшой длины. При этом, происходит потеря небольших объемов данных в отличие от других систем. Зависимость изменения средней длины пакета от качества канала связи представлена на рисунке 7.

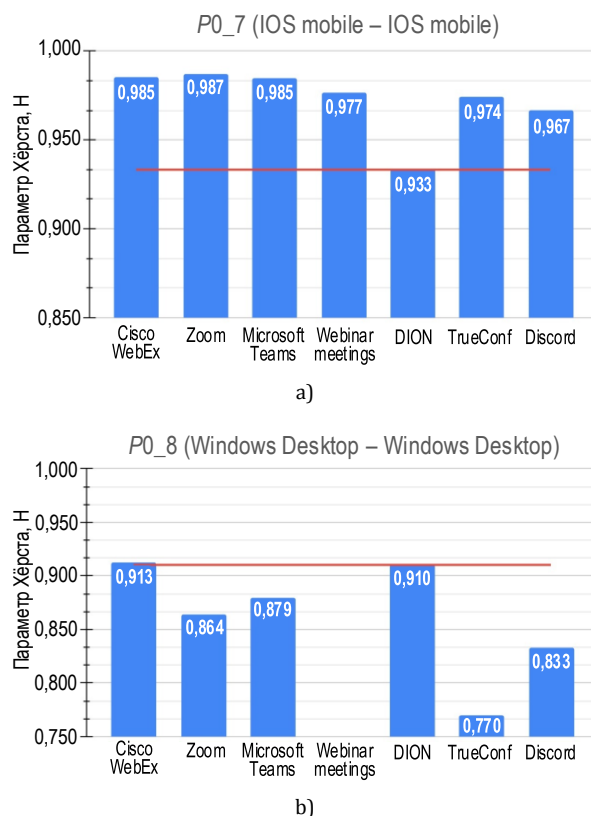


Рис. 6. Параметр Хёрста для ТК с экстремальными значениями качества в каналах: с джиттером (а) и с экстремальными значениями качества (б)

Fig. 6. Hurst Parameter for TC with Extreme Quality Values in Channels: with Jitter (a) and with Extreme Quality Values (b)

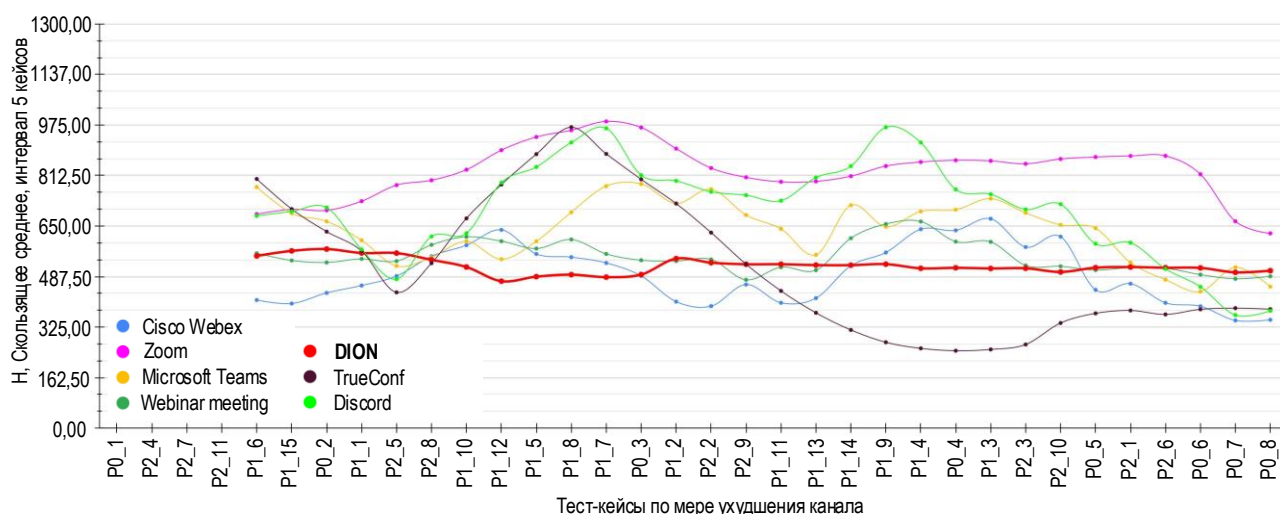


Рис. 7. Зависимость средней длины пакета от качества канала связи (скользящее среднее)

Fig. 7. Dependence of the Average Packet Length on the Quality of the Communication Channel (Moving Average)

Выводы

1) На рисунке 7 видно, что система Zoom во всех тест-кейсах имеет высокий показатель среднего значения длины пакетов, в то время как система TrueConf при плохих характеристиках канала имеет самые малые значения. Система DION на протяжении всего графика имеет равномерную длину пакетов, которая означает, что ухудшение канала не оказывает влияния на этот параметр.

2) При существенном уменьшении длины пакетов значение параметра Хёрста также уменьшается. Например, для системы DION в тест-кейсах P1_12 и P0_7. Также заметно, что на хороших каналах у остальных систем длины выше, что, вероятно, дает повышенный параметр Хёрста, однако, по мере ухудшения качества канала, длины падают и становятся сравнимы с длинами пакетов системы

DION. Вместе с этим, параметр Хёрста падает у других систем сильнее, чем у DION со стабильно небольшой длиной, что непосредственно является преимуществом системы DION на плохих каналах связи.

Для определения зависимости параметра Хёрста от средней длины пакетов использован метод оценки по критерию корреляции Пирсона и регрессионный анализ, а также проведена оценка выбросов в данных методом квартильного анализа. Вычисленные параметры межквартильного диапазона, его «внутренние» и «внешние» границы, а также «значительные выбросы» измерений для исследуемых систем ВКС представлены в таблице 15, где H – параметр Хёрста; L – средняя длина пакета данных; $Q1$ – нижняя квартиль; $Q3$ – верхняя квартиль; IQR – интерквартильный размах.

Таблица 15. Определение выбросов

TABLE 15. Determination of Emissions

Система ВКС	Параметр	Q1	Q3	IQR	внутренняя граница		внешняя граница	
					High	Low	High	Low
Cisco WebEx	H	0,9323	0,9691	0,0369	1,0244	0,8769	1,0798	0,8216
	L	330,5075	601,6	271,0925	1008,2388	-7,1312	1414,8775	-482,77
	Выбросы	незначительные: P1_4, P2_2 значительные: отсутствуют						
Zoom	H	0,9295	0,9872	0,0577	1,0738	0,8430	1,1603	0,7564
	L	717,2050	852,9075	135,7025	1056,4613	513,6513	1260,015	310,0975
	Выбросы	незначительные: P1_12 значительные: P0_7						
Microsoft Teams	H	0,9251	0,9712	0,0461	1,0404	0,856	1,1095	0,7868
2	L	448,14	797,43	349,29	1321,365	-75,795	1845,3	-599,73
	Выбросы	незначительные: P1_3 значительные: отсутствуют						
Webinar meetings	H	0,9344	0,9799	0,0455	1,0480	0,8662	1,1162	0,7981
	L	463,115	628,4375	165,3225	876,4213	215,1313	1124,405	-32,8525
	Выбросы	незначительные: P1_14 значительные: отсутствуют						
DION	H	0,9264	0,9475	0,0211	0,9792	0,8947	1,0109	0,863
	L	500,49	553,4775	52,9875	632,9588	421,0088	712,44	341,5275
	Выбросы	незначительные: P1_6, P1_13, P2_1, P0_7 значительные: P1_12						
TrueConf	H	0,8819	0,9748	0,0929	1,1141	0,7426	1,2534	0,6033
	L	335,2575	757,7275	422,47	1391,4325	-298,4475	2025,1375	-932,1525
	Выбросы	незначительные: отсутствуют значительные: отсутствуют						
Discord	H	0,9098	0,9494	0,0396	1,0089	0,8504	1,0683	0,7909
	L	259,7	1009,59	749,89	2134,425	-865,135	3259,26	-1989,97
	Выбросы	незначительные: P0_8 значительные: отсутствуют						

В целях анализа взаимосвязей и визуализации наличия значительных выбросов в данных необходимо построить диаграммы рассеяния, которые также позволяют определить потенциальную нелинейную взаимосвязь средней длины пакета и параметра Хёрста.

Для исследуемых систем ВКС диаграммы рассеяния представлены на рисунке 8, где красным вы-

делены значительные выбросы, которые необходимо учесть при исследовании корреляции.

Рассчитанные значения коэффициента корреляции Пирсона и оценки статистической значимости представлены в таблице 16 и на рисунке 9, где r_{xy} – коэффициент корреляции; $|t_r|$ – абсолютное значение t -критерия Стьюдента, $t_{\text{крит}}$ – критическое значение t -критерия Стьюдента при уровне значимости $p = 0,05$.

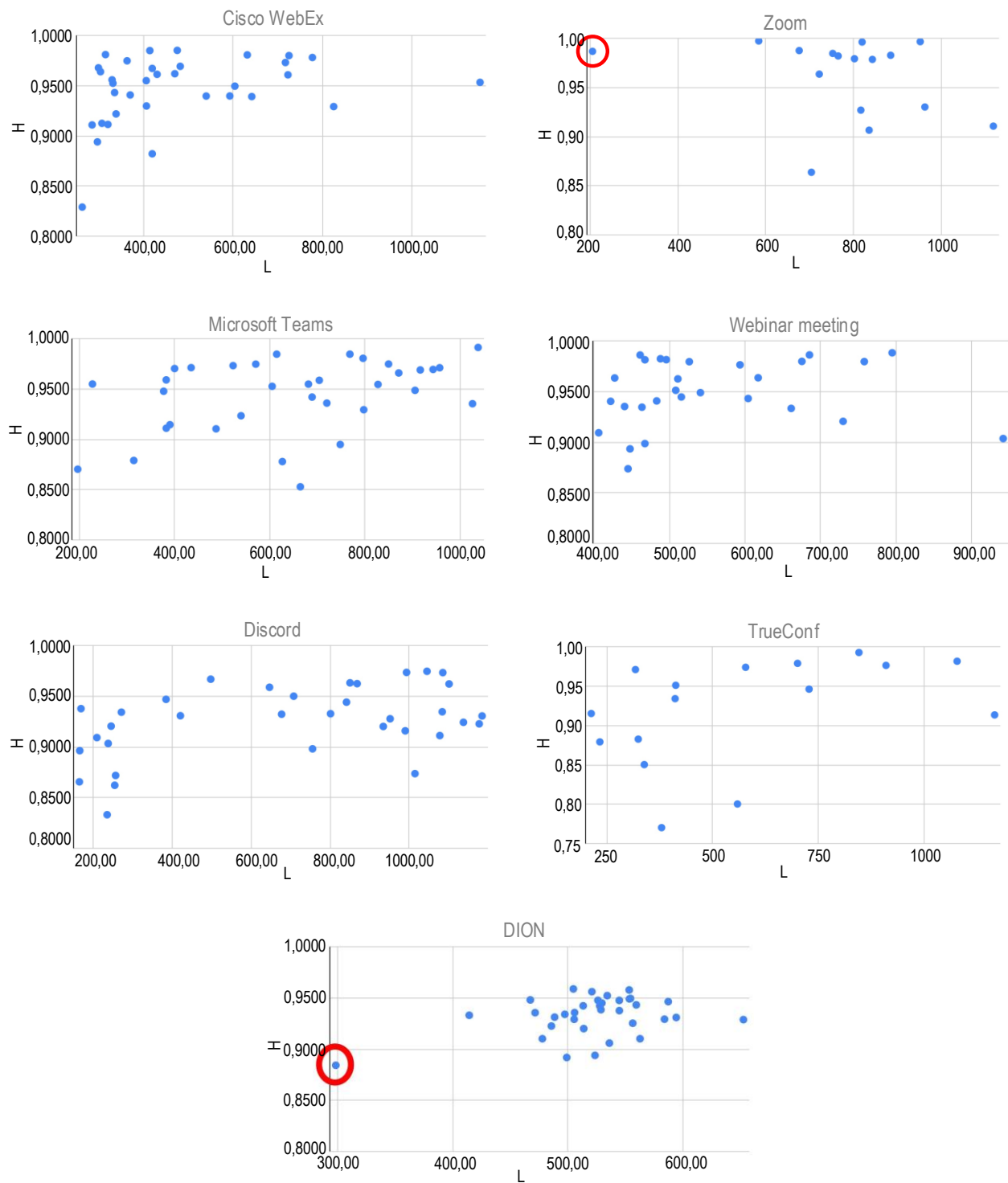


Рис. 8. Диаграммы рассеяния

Fig. 8. Scattering Diagrams

ТАБЛИЦА 16. Значения коэффициента Пирсона и оценки статистической значимости

TABLE 16. Values of the Pearson Coefficient and Estimates of Statistical Significance

Система	Cisco WebEx	Zoom	MS Teams	Webinar meetings	DION	TrueConf	Discord
r_{xy}	0,3104	-0,2423	0,3808	0,1478	0,0896	0,4277	0,4560
$ t_r $	2,653	1,322	3,345	1,0982	0,720	2,591	4,163
$t_{\text{крит}}$	1,997	2,048	1,997	1,163	1,998	2,042	1,997

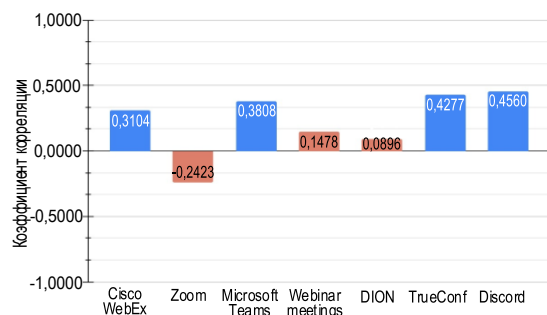


Рис. 9. Коэффициент корреляции Пирсона

Fig. 9. Pearson Correlation Coefficient

Выводы

Во-первых, анализ данных таблицы 16 показывает, что для всех систем, кроме Zoom, Webinar meetings и DION, наблюдаемая корреляционная связь статистически значима при $p < 0,05$, т. е. не случайно отличается от нуля. Для остальных – носит более случайный характер. Также это подтверждается низким значением коэффициента Пирсона. С другой стороны, количество полученных значений для системы Zoom в два раза меньше, чем для остальных. Увеличение числа измерений для Zoom, возможно, изменит эту ситуацию.

Во-вторых, для увеличения значения параметра Хёрста требуется увеличение длин пакетов, кроме системы Zoom, где требуется их уменьшение; это связано с алгоритмами работы систем. Например, для системы Microsoft Teams увеличение длины пакетов оказывает почти такое же влияние на параметр, как и в случае с TrueConf и Cisco WebEx. В то время, как достижение заданного значения параметра потоков данных, формируемых алгоритмами работы DION, никак не зависит от длины пакетов, либо эта зависимость носит случайный характер. Для систем TrueConf и Discord длина пакетов является определяющим фактором при изменении параметра Хёрста.

Для выявления факта наличия корреляционной зависимости параметра Хёрста (H) от средней длины пакета (L), а также ее вида, направления и силы были построены линии регрессии (рисунок 10).

Анализ линий регрессии показывает, что:

1) корреляционная зависимость между параметром Хёрста и средней длиной пакета наблюдается для всех систем, кроме DION, где размеры пакетов колеблются в очень узком диапазоне; это связано с использованием протокола взаимодействия STUN;

2) вид корреляционных зависимостей носит линейный характер;

3) для систем Cisco WebEx, Discord, Microsoft Teams, TrueConf и Webinar meetings наблюдается положительная корреляция между параметром Хёрста и средней длиной пакета (более высоким значениям параметра соответствуют более высокие значения средней длины пакета); для системы Zoom наблюдается отрицательная корреляция;

4) значения тангенса угла между линией регрессии и осью абсцисс характеризует силу корреляционной связи, что также подтверждается коэффициентом корреляции Пирсона (см. рисунок 9).

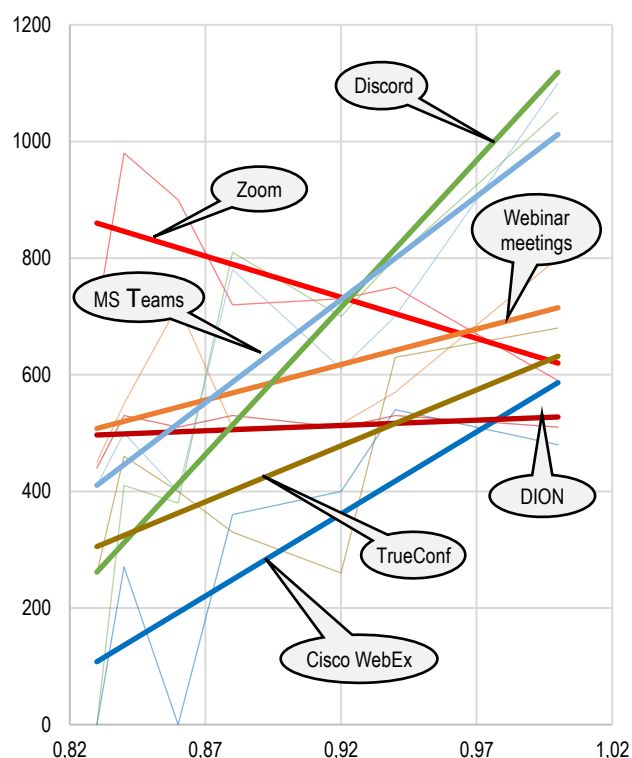


Рис. 10. Линии регрессии (бесплатные подписки)

Fig. 10. Regression Lines (Free Subscriptions)

На рисунке 11 показана зависимость параметра Хёрста от типа приложений. При этом, значение параметра Хёрста усреднено по всем тест-кейсам данной группы приложений.

Выводы

Во-первых, наиболее высокий показатель параметра Хёрста для всех систем наблюдается при использовании мобильных устройств, а именно (IOS mobile – IOS mobile), (IOS mobile – Android mobile), (Android mobile – IOS mobile), (Android mobile – Android mobile). При этом, значение DION находится на своем среднем уровне. Даже при высоких значениях потерь и задержки параметр Хёрста значительно больше именно в тест-кейсах с мобильными приложениями.

Во-вторых, по показателю параметра Хёрста вторым является связь между двумя веб-версиями приложений вне зависимости от ОС.

В-третьих, система DION наиболее стабильна к использованию различных типов приложений. Скорее всего, это достигается за счет использования одинаковых алгоритмов обработки для всех типов приложений; в то время как остальные системы делают упор на использование мобильных приложений.

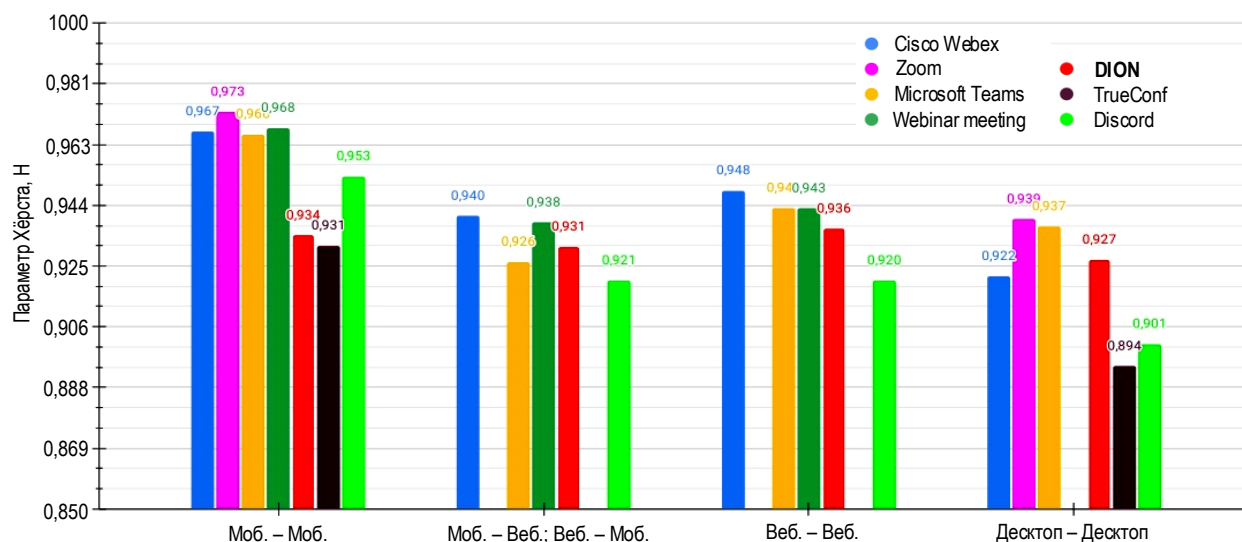


Рис. 11. Зависимость параметра Хёрста от типа приложений

Fig. 11. The Dependence of the Hurst Parameter on the Type of Applications

Заключение

Результаты исследований показали, что приложение DION занимает первое место среди тестируемых отечественных средств ВКС: DION, TrueConf и Webinar meetings, а также третье место среди всех тестируемых приложений. Второе место делят между собой Cisco WebEx и Microsoft Teams. Условно бесплатное приложение Discord занимает четвертое место.

Лидером настоящего исследования можно считать систему Zoom. Вероятная причина ее достаточно стабильной работы заключается в наличии уникальных исследований, защищенных множеством патентов [24], которые направлены на

улучшение сеансов ВКС, пользовательского опыта и самих клиентских приложений. В качестве аудиокодека система Zoom использует кодек SILK с двумя резервными пакетами с частичным резервированием и формат LBRR (аббр. от Low Bit-Rate Redundancy). Фактически это повторение содержимого предыдущих пакетов в последующих по принципу вложенности. Для улучшения пользовательских характеристик систем ВКС необходимы исследования и реализация нестандартных уникальных технических решений в области передачи данных, разработки кодеков (возможно на базе нейронных сетей), а также развитие облачных услуг в части предсказания трафика.

Список источников

1. Rec. ITU-T Q.3949 (08/2012). Real-time multimedia service testing framework at the user-to-network interface of next generation networks.
2. Грачева М.А., Божкова В.П., Казакова А.А., Рожкова Г.И. Субъективная оценка качества статических и видеоизображений: методологический обзор // Сенсорные системы. 2019. Т. 33. № 4. С. 287–304.
3. Ahmed M.S. Achieving QoS in media streaming for peer to peer networks // International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT, Chennai, India, 2016). 2016. PP. 3694–3698. DOI:10.1109/ICEEOT.2016.7755399
4. Bao Y., Lei W., Zhang W., Song J. HD streaming media QoE quantitative evaluation model for multipath transmission // 11th International Conference on Computer Science & Education (ICCSE, Nagoya, Japan, 2016). 2016. PP. 658–665. DOI:10.1109/ICCSE.2016.7581658
5. Fowdur T.P., Narrainen L. Enhanced video streaming using dynamic quality control with bandwidth prediction // International Conference on Computer as a Tool (EUROCON, Salamanca, Spain, 2015). 2015. PP. 1–6. DOI:10.1109/EUROCON.2015.7313675
6. Taraghi B., Nguyen M., Amirpour H., Timmerer C. Intense: In-Depth Studies on Stall Events and Quality Switches and Their Impact on the Quality of Experience in HTTP Adaptive Streaming. IEEE, 2021. Vol. 9. PP. 118087–118098. DOI:10.1109/ACCESS.2021.3107619
7. Yeganeh H., Qassemi F., Rabiee H.R. Joint effect of stalling and presentation quality on the quality-of-experience of streaming videos // IEEE International Conference on Image Processing (ICIP, Beijing, China, 2017). 2017. PP. 310–314. DOI:10.1109/ICIP.2017.8296293
8. Seufert A., Wamser F., Yarish D., Macdonald H., Hoßfeld T. QoE Models in the Wild: Comparing Video QoE Models Using a Crowdsourced Data Set // 13th International Conference on Quality of Multimedia Experience (QoMEX, Montreal, QC, Canada, 2021). 2021. PP. 55–60. DOI:10.1109/QoMEX51781.2021.9465422

9. Hoßfeld T., Heegaard P.E., Skorin-Kapov L., Varela M. No silver bullet: QoE metrics, QoE fairness, and user diversity in the context of QoE management // Ninth International Conference on Quality of Multimedia Experience (QoMEX, Erfurt, Germany, 2017). 2017. PP. 1–6. DOI:10.1109/QoMEX.2017.7965671
10. Mardian R. D., Suryanegara M., Ramli K. Measuring Quality of Service (QoS) and Quality of Experience (QoE) on 5G Technology: A Review // IEEE International Conference on Innovative Research and Development (ICIRD, Jakarta, Indonesia, 2019). 2019. PP. 1–6, DOI:10.1109/ICIRD47319.2019.9074681
11. Hewage C. T. E. R., Ahmad A., Mallikarachchi T., Barman N., Martini M. G. Measuring, Modeling and Integrating Time-Varying Video Quality in End-to-End Multimedia Service Delivery: A Review and Open Challenges. IEEE. 2022. Vol. 10. PP. 60267–60293. DOI:10.1109/ACCESS.2022.3180491
12. Рекомендация МСЭ-Т G.107 (06.2015). Е-модель – вычислительная модель, используемая при планировании передачи.
13. Кучерявый, А.Е., Парамонов А.И., Кучерявый Е.А. Сети связи общего пользования. Тенденции развития и методы расчета. М.: ФГУП ЦНИИС, 2008. 296 с.
14. Rec. ITU-T G.1011 (07/2016). Reference guide to quality of experience assessment methodologies.
15. Шелухин О.И., Осин А.В., Смольский С.М. Самоподобие и фракталы. Телекоммуникационные приложения. М.: Физматлит, 2008.
16. Janevski T., Vanevski Z. Statistical Analysis of Multicast versus Instant Channel Changing Unicast IPTV Provisioning // Proceedings of the 16th Telecommunications Forum (TELFOR, Belgrade, Serbia, 25–27 November 2008). 2008. PP. 96–99.
17. Paramonov P., Tarasov D., Koucheryavy A. The Video Streaming Monitoring in the Next Generation Network // Proceedings of the 9th International Conference on Next Generation Wired/Wireless Networking (NEW2AN 2009) and Second Conference on Internet of Things and Smart Spaces (ruSMART 2009), St. Petersburg, Russia, 15–18 September 2009. Lecture Notes in Computer Science. Vol. 5764. Berlin, Heidelberg: Springer, 2009. PP. 191–205. DOI:10.1007/978-3-642-04190-7_18
18. Rezaul K.M., Pakstas A., Gilchrist R., Chen T.M. HEAF: A Novel Estimator for Long-Range Dependent Self-similar Network Traffic // Proceedings of the 6th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN 2006), St. Petersburg, Russia, 29 May–2 June 2006. Lecture Notes in Computer Science. Vol. 4003. Berlin, Heidelberg: Springer, 2006. PP. 34–45. DOI:10.1007/11759355_6
19. Маколкина М.А. Взаимосвязь субъективных оценок качества восприятия видео и значений параметра Хёрста // Системы управления и информационные технологии. 2014. 1-1(55). С. 169–172.
20. Маколкина М.А. Учет параметра Хёрста при формировании субъективных оценок качества восприятия видео и значений // Информационные технологии моделирования и управления. 2016. Т. 99. № 3. С. 197–204.
21. Маколкина М.А. Анализ модели объективной оценки качества передачи видео в IP-сетях // Электросвязь. 2011. № 12. С. 20а–23.
22. Куликов С. Тестирование программного обеспечения. Базовый курс. EPAM systems, 2015–2022. URL: https://svyatoslav.biz/software_testing_book_download (дата обращения 09.02.2023)
23. Rec. ITU-T Y.1541 (12/2013). Network performance objectives for IP-based services. Amendment 1: New Appendix XII – Considerations for low speed access networks.
24. Zoom Patents // Zoom. URL: <https://explore.zoom.us/en/trust/patents> (дата обращения 09.02.2023)

References

1. Rec. ITU-T Q.3949. Real-time multimedia service testing framework at the user-to-network interface of next generation networks. December 2012.
2. Gracheva M.A., Bozhkovaa V.P., Kazakovaa A.A. Rozhkovaa G.I. Subjective image and video quality assessment: methodology review. *Sensornye seti*. 2019;33(4):287–304. (in Russ.)
3. Ahmed M.S. Achieving QoS in media streaming for peer to peer networks. *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. Chennai, India; 2016. pp. 3694–3698. DOI:10.1109/ICEEOT.2016.7755399
4. Bao Y., Lei W., Zhang W., Song J. HD streaming media QoE quantitative evaluation model for multipath transmission. *2016 11th International Conference on Computer Science & Education, ICCSE, Nagoya, Japan*. 2016. p.658–665. DOI:10.1109/ICCSE.2016.7581658
5. Fowdur T.P., Narrainen L. Enhanced video streaming using dynamic quality control with bandwidth prediction *IEEE EUROCON 2015 – International Conference on Computer as a Tool, EUROCON, Salamanca, Spain*. 2015. p.1–6. DOI:10.1109/EUROCON.2015.7313675
6. Taraghi B., Nguyen M., Amirpour H., Timmerer C. Intense: In-Depth Studies on Stall Events and Quality Switches and Their Impact on the Quality of Experience in HTTP Adaptive Streaming. *IEEE*; 2021. vol.9. p.118087–118098. DOI:10.1109/ACCESS.2021.3107619
7. Yeganeh H., Qassemi F., Rabiee H.R. Joint effect of stalling and presentation quality on the quality-of-experience of streaming videos. *2017 IEEE International Conference on Image Processing, ICIP, Beijing, China*. 2017. p.310–314. DOI:10.1109/ICIP.2017.8296293
8. Seufert A., Wamser F., Yarish D., Macdonald H., Hoßfeld T. QoE Models in the Wild: Comparing Video QoE Models Using a Crowdsourced Data Set. *2021 13th International Conference on Quality of Multimedia Experience, QoMEX, Montreal, Canada*. 2021. p.55–60. DOI:10.1109/QoMEX51781.2021.9465422
9. Hoßfeld T., Heegaard P.E., Skorin-Kapov L., Varela M. No silver bullet: QoE metrics, QoE fairness, and user diversity in the context of QoE management. *2017 Ninth International Conference on Quality of Multimedia Experience, QoMEX, Erfurt, Germany*. 2017. p.1–6. DOI:10.1109/QoMEX.2017.7965671

10. Mardian R.D., Suryanegara M., Ramli K. Measuring Quality of Service (QoS) and Quality of Experience (QoE) on 5G Technology: A Review. *2019 IEEE International Conference on Innovative Research and Development, ICIRD, Jakarta, Indonesia*. 2019. p.1–6. DOI:10.1109/ICIRD47319.2019.9074681
11. Hewage C.T.E.R., Ahmad A., Mallikarachchi T., Barman N., Martini M.G. Measuring, Modeling and Integrating Time-Varying Video Quality in End-to-End Multimedia Service Delivery: A Review and Open Challenges. *IEEE*. 2022. vol. 10. pp. 60267–60293. DOI:10.1109/ACCESS.2022.3180491
12. Rec. ITU-T G.107. *International Telephone Connections and Circuits – Transmission Planning and the E-Model*. June 2015.
13. Koucheryavy A., Paramonov A., Koucheryavy E. Public Communication Networks. Development Trends and Calculation Methods. Moscow: Central Research Institute of Communication Publ.; 2008. (in Russ.)
14. Rec. ITU-T G.1011. *Reference guide to quality of experience assessment methodologies*. June 2016.
15. Shelukhin O.I., Osin A.V., Smolsky S.M. *Self-Similarity and Fractals. Telecommunication Applications*. Moscow: Fizmatlit Publ.; 2008. (in Russ.)
16. Janevski T., Vanevski Z. Statistical Analysis of Multicast versus Instant Channel Changing Unicast IPTV Provisioning. *Proceedings of the 16th Telecommunications Forum, TELFOR, 25–27 November 2008, Belgrade, Serbia*. 2008. p.96–99.
17. Paramonov P., Tarasov D., Koucheryavy A. The Video Streaming Monitoring in the Next Generation Network. *Proceedings of the 9th International Conference on Next Generation Wired/Wireless Networking, NEW2AN 2009, and Second Conference on Internet of Things and Smart Spaces, ruSMART 2009, 15–18 September 2009, St. Petersburg, Russia. Lecture Notes in Computer Science, vol.5764*. Berlin, Heidelberg: Springer; 2009. p.191–205. DOI:10.1007/978-3-642-04190-7_18
18. Rezaul K.M., Pakstas A., Gilchrist R., Chen T.M. HEAF: A Novel Estimator for Long-Range Dependent Self-similar Network Traffic. *Proceedings of the 6th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking, NEW2AN 2006, 29 May–2 June 2006, St. Petersburg, Russia. Lecture Notes in Computer Science, vol.4003*. Berlin, Heidelberg: Springer; 2006. p.34–45. DOI:10.1007/11759355_6
19. Makolkina M.A. The Relationship between Subjective Assessments of the Quality of Video Perception and the Values of the Hurst Parameter. *Sistemy upravleniia i informatsionnye tekhnologii*. 2014;1-1(55):169–172. (in Russ.)
20. Makolkina M. Parameter Values Hurst in Subjective Evaluations of the Quality of the Relationship of Perception and Video. *Informatsionnye tekhnologii modelirovaniia i upravleniia*. 2016;99(3):197–204. (in Russ.)
21. Makolkina M.A. Analysis of the Model for an Objective Assessment of the Quality of Video Transmission in IP Networks. *Electrosvyaz*. 2011;12:20–23. (in Russ.)
22. Kulikov S. *Software Testing. Basic Course*. EPAM systems; 2015–2022. (in Russ.) URL: https://svyatoslav.biz/software_testing_book_download [Accessed 9th February 2023]
23. Rec. ITU-T Y.1541. *Network performance objectives for IP-based services. Amendment 1: New Appendix XII – Considerations for low speed access networks*. December 2013.
24. Zoom. Zoom Patents. URL: <https://explore.zoom.us/en/trust/patents> [Accessed 9th February 2023]

Статья поступила в редакцию 13.02.2023; одобрена после рецензирования 27.02.2023; принята к публикации 28.02.2023.

The article was submitted 13.02.2023; approved after reviewing 27.02.2023; accepted for publication 28.02.2023.

Информация об авторах:

КИРИЧЕК
Руслан Валентинович

доктор технических наук, доцент, ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
 <https://orcid.org/0000-0002-8781-6840>

БЕРЁЗКИН
Александр Александрович

кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
 <https://orcid.org/0000-0002-1748-8642>

КУКУНИН
Дмитрий Сергеевич

кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
 <https://orcid.org/0000-0002-2674-5217>

КОЛЕСНИКОВ
Андрей Вячеславович

директор Ассоциации участников рынка интернета вещей,
 <https://orcid.org/0009-0000-8401-8723>

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

**2.3.1 – Системный анализ,
управление и обработка
информации**

**2.3.6 – Методы и системы защиты
информации, информационная
безопасность**

Научная статья

УДК 004.42

DOI:10.31854/1813-324X-2023-9-1-75-93



Моделирование программы с уязвимостями с позиции эволюции ее представлений. Часть 1. Схема жизненного цикла

Константин Евгеньевич Израилов, konstantin.izrailov@mail.ru

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук,
Санкт-Петербург, 199178, Российская Федерация

Аннотация: Изложены результаты исследования процесса создания программ и возникающих при этом уязвимостей. В первой части цикла статей предлагается графическая схема жизненного цикла представлений (а именно следующих: Идея, Концептуальная модель, Архитектура, Двухмерная структурная схема, Функциональная диаграмма, Блок-схема, Структурограмма, Псевдокод, Классический, Метакод генерации, Сценарный код, Ассемблерный код, Дерево абстрактного синтаксиса, Машинный код, Байт-код), через которые проходит любая типовая программа. Указываются основные свойства таких представлений – назначение, форма и содержание, способы получения и восстановления представлений, а также возможные уязвимости и способы их обнаружения. Вводится вложенная классификация уязвимостей, состоящая из их деления по структурному уровню в программе, изменению содержания функционала и воздействию на обрабатываемую информацию.

Ключевые слова: программная инженерия, информационная безопасность, уязвимости, представления программы, жизненный цикл, моделирование

Благодарность: Автор выражает благодарность своему научному консультанту – доктору технических наук, профессору М.В. Буйневичу за существенный вклад в текущее исследование.

Ссылка для цитирования: Израилов К.Е. Моделирование программы с уязвимостями с позиции эволюции ее представлений. Часть 1. Схема жизненного цикла // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 75–93. DOI:10.31854/1813-324X-2023-9-1-75-93

Modeling a Program with Vulnerabilities in the Terms of Its Representations Evolution. Part 1. Life Cycle Scheme

Konstantin Izrailov, konstantin.izrailov@mail.ru

Saint-Petersburg Federal Research Center of the Russian Academy of Sciences,
St. Petersburg, 199178, Russian Federation

Abstract: The investigation results of the creating programs process and the resulting vulnerabilities are presented. The first part of the articles series offers a life cycle graphical scheme of the representations (namely, the following: Idea, Conceptual model, Architecture, 2D block diagram, Function diagram, Flowchart, Structogram, Pseudo-code, Classical code, Generation metacode, Script code, Assembly code, Abstract Syntax Tree, Machine Code, Bytecode) through which any sample program passes. The main properties of such representations are indicated - the purpose, form and content, obtaining and restoring representations methods, as well as possible vulnerabilities and ways to

detect them. A vulnerabilities nested classification is introduced, consisting of their division according to the structural level in the program, the change in the content of the functionality and the impact on the information being processed.

Keywords: software engineering, information security, vulnerabilities, program representations, life cycle, modeling

Acknowledgment: The author expresses his gratitude to his scientific adviser - Doctor of Technical Sciences, Professor M.V. Buinevich for significant contributions to the current research.

For citation: Izrailov K. Modeling a Program with Vulnerabilities in the Terms of Its Representations Evolution. Part 1. Life Cycle Scheme. *Proc. of Telecom. Universities*. 2023;9(1):75–93. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-75-93

1. ВВЕДЕНИЕ

Одной из актуальнейших проблем в сфере информационной безопасности (далее – ИБ) является недостаточное количество удовлетворительных способов поиска в программном обеспечении (далее – ПО) уязвимостей, наличие которых может приводить к нарушениям конфиденциальности, целостности и доступности критически важной информации. Существующие же способы можно считать подходящими лишь для отдельных типов уязвимостей или условий применения. Например, отслеживание программных исключений путем «фаззинга» данных в памяти тестируемой программы [1]. Для разрешения данной проблемы необходимо, в первую очередь, исследовать сам породивший ее объект – уязвимость: при этом не только статические, но и динамические свойства, определяющие ее жизненный цикл (далее – ЖЦ) в процессе создания программ). Анализ динамических свойств позволит более широко охватить все возможные способы поиска, поскольку они напрямую зависят от того, какой вид имеет уязвимость, что непосредственно влияет на ее обнаруживаемость. В свою очередь, статические свойства дают лишь удобные классификации уязвимостей и частично формируют дополнительные знания о них. В такой постановке проблемного вопроса актуальным является моделирование ЖЦ программы с уязвимостями, для чего используется авторская нотация. Предметная область исследования будет задана, как рассмотрение эволюции программы в процессе ее создания и появляющихся при этом уязвимостей.

2. ОСНОВНЫЕ ПОНЯТИЯ ПРЕДМЕТНОЙ ОБЛАСТИ В НОТАЦИИ ПРЕДСТАВЛЕНИЙ

Для проведения любого исследования требуется однозначный понятийный аппарат. В этом аспекте базовые термины настоящей предметной области используются современными исследователями в крайне неоднозначной трактовке, приводя их к трудно сопоставимым результатам и противоречивым выводам.

Так, только на международном уровне¹ декларировано 16 критериев классификации программных средств, что свидетельствует о большом разнообразии «софта» и не могло не сказаться на его определении, как IT-термина. В результате имеется множество, в том числе стандартизованных² в РФ определений ПО с акцентом на вторую составляющую – *обеспечение* компьютера (компьютерной системы), как средства решения задачи. Причиной последнего, скорее всего, является направленность IT-мысли лишь на субъект исполнения, а не на объект приложения ПО, а именно – на информацию.

Еще более дискуссионным, но весьма характерным для программы, является понятие (ее) уязвимости. Попытки использования устоявшихся и общепринятых³, не всегда тождественных (но по смыслу сводящихся к некому эксплуатируемому источником угрозы дефекту или «слабости» ПО), определений в немалой степени затрудняет систематизацию и формализацию предметной области; за редким положительным исключением [2].

С учетом вышеизложенного предлагается введение следующих, более конкретных и «ортогональных» определений используемых далее понятий, что позволит повысить однозначность результатов проводимого исследования.

Будем понимать под компьютерной программой некую автоматическую процедуру (конкретную или обобщенную) решения вполне определенной задачи, связанной с обработкой информации – т. н. информационной задачи. Ввиду технологичности процесс создания программы состоит из типовых стадий; в рамках каждой стадии определенные

¹ ISO/IEC TR 12182:2015. Systems and software engineering. Framework for categorization of IT systems and software, and guide for applying it.

² ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. М.: Стандартинформ, 2010; ГОСТ 34.003-90 Информационная технология. Автоматизированные системы. Термины и определения. М.: Стандартинформ, 2009.

³ ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. М.: Стандартинформ, 2018.

процессы (или их объединения) производят соответствующие преобразования. Тем самым программа находится в своих различных представлениях (состояниях, точках развития), каждое из которых создается на основании предыдущего; также оно является входным для одних стадий или процессов и выходным для других.

Каждое такое представление (далее – Представление) является отдельным этапом эволюции решения задачи, не изменяя основополагающего содержания ее решения (в смысле его сути), постепенно конкретизируясь путем перехода от человеко-понятной к машинно-ориентированной форме. Т. е. содержание решения сохраняется на протяжении всего процессе создания программы, постепенно обретая конечную реальную форму из начального заданного идеала; используемая переменчивая форма для неизменного содержания соответствует применяемым стадиям-процессам. При этом, как и любая естественная эволюция, развитие решения задачи может иметь разветвления на параллельные Представления вследствие применения процессов их формирования различного рода (например, алгоритмы могут быть описаны графически или текстуально, а в качестве выполняемой сборки может быть получен машинный или байт-код).

Каждое Представление имеет назначение (или цель своего существования), определяющее основное его отличие от остальных и, как следствие, уникальную форму, наиболее подходящую для хранения содержания.

Для уменьшения неоднозначности в делении программы на Представления будем последние определять на основании их реального существования в виде законченной совокупности формы и содержания, а также учитывая распространенные практики применения. Так, например, Представление в виде блок-схем алгоритмов имеет право на существование, поскольку несмотря на то, что при реальном создании программ блок-схемы применяются редко, они используются для документирования и стандартизованы⁴. Впрочем, такая практика *неиспользования* отдельных Представлений исходит исключительно из экономических соображений, завышенных амбиций и умения разработчиков кода держать в голове и его алгоритмы, что в конечном итоге негативно сказывается на качестве создаваемого ПО. Следуя такой же логике, внутреннее представление байт-кода в виртуальной машине (имеющее, возможно, форму машинных инструкций для режима Just-In-Time – осуществляющего такое преобразование в процес-

се выполнения) не будет считаться отдельным Представлением, поскольку оно относится к стадии выполнения, а создание программы в этом случае заканчивается на Представлении выполняемого байт-кода.

Полный цикл процесса создания программы осуществляется ее переходом из Представления изначальной идеи в код, готовый для выполнения. Для работы последнего необходима соответствующая среда, воспринимающая только определенную форму Представления, через которую и передается содержание программы для непосредственного выполнения. Отсюда органично вытекает определение жизненного цикла программы как череды Представлений от изначального (придуманной идеи человеком) до одного из финальных (реализующего идею кода для автомата).

Наиболее известным и широко используемым Представлением можно считать исходный код, представляющий собой некие текстовые читаемые сообщения на специальном языке или нотации, предназначенные для строгого описания процедуры решения. Такой код может как выполняться напрямую (сценарный), так и преобразовываться в управляемый и выполняемый виртуальной машиной (байт-код) или платформенно-зависимый (машинный). Последний случай считается классически используемым при создании встроенного ПО, например, для телекоммуникационных, мобильных или киберустройств.

В рамках введенных понятий сразу отметим, что ни здесь, ни далее не рассматривается особый вид программ, предназначенный не столько для решения задач, сколько для их спецификации и ожидаемого результата – соответствующий декларативной парадигме программирования (примерами исходного кода таких программ служат языки запросов SQL и разметки HTML). Такое исключение как раз и призвано избавиться от смешения используемых понятий и парадигм.

Введем авторское – основанное на уже частично сформированной понятийной базе – определение уязвимости. Уязвимостью будем называть отличия между начальным (идеальным, исходно задуманным) и текущим (промежуточным или реально выполняемым) содержанием Представлений; отличия в их форме, очевидно, являются вполне законными, поскольку они как раз и служат способом «транспортировки» содержания от ориентированного на человека до понятного машине (т. е. выполняющему программу автомату). Поскольку все же уязвимости в большинстве случаев связаны именно с вопросами ИБ, то уточним указанные отличия теми, которые приводят к изменениям в состояниях конфиденциальности, целостности и доступности информации при ее обработке программой в этих Представлениях. Так, если начальное

⁴ ГОСТ 19.701-90 Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения. М.: Стандартинформ, 2010.

Представление имеет функционал, обеспечивающий одно состояние ИБ – например, полная конфиденциальность информации, а конечное имеет функционал, обеспечивающий другое – например, потерю конфиденциальности, то в процессе преобразования Представлений, очевидно, появляется уязвимость, приводящая к утечке информации. Отсюда следует несколько парадоксальное утверждение, что если изначальное Представление (по содержанию) никак не уточняет состояние задачи в части ИБ (например, не стремится обеспечить конфиденциальность), то утечка информации в конечном Представлении вполне допустима и не будет ассоциироваться с уязвимостью.

Это утверждение верно с оговоркой на недекларированные условия использования, которые следует понимать как аналогию недекларированных возможностей (НДВ) в том смысле, что программу начинают использовать не в соответствии с первоначальным замыслом, не по назначению, т. е. не в задуманных условиях.

Здесь можно привести достаточно яркий «анти-пример» того, что сегодня называется уязвимостями протоколов стека TCP/IP. 2 ноября 1988 г. сеть ARPANET была атакована программой, впоследствии получившей название «червь Морриса» – временно из строя было выведено 6 800 компьютеров. Для этого использовалось несколько особенностей функционирования сетевых сервисов, а также некоторые «слабые» места компьютерных систем, впоследствии названные уязвимостями. С учетом того, что ARPANET, явившаяся прототипом сети Интернет, была создана в далеком 1969 г. (за 20 лет до «легендарной» DoS-атаки), то эти «уязвимости» были закономерно обусловлены недостаточным вниманием к вопросам ИБ в то время.

Искусственное расширение назначения и изменение среды функционирования хотя и относится к условиям применения, однако, по сложившейся терминологической практике, приписывается к слабостям и/или дефектам программ – то есть, к его уязвимостям в широком смысле слова; хотя проблемы возникали не в самом ПО, а в его использовании. С учетом этих соображений уточним введенное выше в узком (контекстном, ассоциированным с Представлениями) смысле понятие уязвимости как «отличия между начальным и конечным Представлениями»: уязвимость – злоумышленно или случайно внесенный дефект (программная закладка) или НДВ, которые в любом случае проявляются искажением содержания относительно предыдущих Представлений. А так как у замысла нет предыдущего Представления, поэтому он может считаться «неуязвимым».

Несмотря на отмеченную парадоксальность, все же можно предполагать, что введенные понятия более четко и глубоко очерчивают границы пред-

метной области исследования по сравнению с привычными [3], в том числе стандартизованными⁵.

Следствием этого является более ясное понимание как причин, точек и последствий появления уязвимостей, так и способов их обнаружения. Исходя из особенностей введенной системы Представлений (а именно: в начальном Представлении уязвимости отсутствуют, Представления сами по себе не изменяются, каждое новое Представление получается из старого путем специального процесса создания программы), можно сделать следующие принципиальные выводы.

Во-первых, каждое новое (текущее, очередное) Представление содержит все уязвимости старого (предыдущего) за двумя исключениями (о которых речь пойдет ниже), а также дополнительные, внесенные в текущем процессе его создания. Как результат, конечное Представление хранит уязвимости, накопленные в процессе создания промежуточных Представлений.

Во-вторых, исчезновение уязвимостей в процессе создания программы возможно в двух случаях: неявно при создании нового Представления и целенаправленно специальными действиями. Первый случай соответствует случайному событию, когда отличие в Представлениях А и Б зеркально противоположно отличию в Представлениях Б и В, что приводит к отсутствию каких-либо отличий в Представлениях А и В (эффект «двойной ошибки»); такая ситуация может проявляться в результате антропоморфического взаимодействия как отдельных уязвимостей [4, 5], так и целых информационных подсистем [6–9]. Второй случай означает применение на стадиях создания программы дополнительных процессов обнаружения и нейтрализации уязвимостей.

В-третьих, поскольку создание программ идет по пути уменьшения уровня абстракции в Представлениях, то очевидно, что любая возникающая уязвимость, построенная на таких же сущностях, должна иметь подобный уровень, что и является ее статическим свойством. Динамическое же свойство уязвимости в виде ЖЦ может быть определено на базе Представлений, как путь от ее возникновения до обнаружения.

Согласно последнему сделанному выводу относительно уровней абстракций Представлений можно утверждать, что способ классификации уязвимостей может строиться (в том числе) на структурном уровне их «зарождения» нахождения в программе. Также в классификации целесообразно учесть такую ее сущность, как отличие со-

⁵ ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. М.: Стандартинформ, 2018.

держаний, и скоррелировать с классической триадой нарушений конфиденциальности, целостности и доступности информации. Конкретная же таксономия уязвимостей будет дана далее.

В реальной практике многие Представления для разных программных разработок могут субъективно опускаться, объединяются с другими или выносятся в среду выполнения. Так, небольшая программа вполне может быть создана путем написания исходного кода и его компиляции в машинный, выполняться напрямую на центральном процессоре. Однако, если такое упрощение и оправдано для создания простейших программ, то для крупных проектов подобная практика негативно скажется на обеспечении ИБ обрабатываемых данных, поскольку не позволит обеспечить эффективный поиск уязвимостей. Естественно, в ходе общей эволюции программной инженерии могут появляться и новые Представления, качественно отличные от текущих.

3. КРАТКИЙ ОБЗОР СОВРЕМЕННЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ МОДЕЛИРОВАНИЯ ЖИЗНЕННОГО ЦИКЛА

Для оценки степени проработанности предметной области проведем краткий обзор научных работ, посвященных моделированию ЖЦ с уязвимостями, указывая при этом выводы в аспекте решения текущей задачи. Работа [10] посвящена модели цикла разработки программ, используемых в обучении. Исходя из такого предназначения, подтверждаемого жизненной практикой автора, предлагается коэволюция учителей и разработчиков. Указывается, что для включения некоторого ПО в процесс обучения может потребоваться его адаптация: параметрическая (настройкой параметров), модульная (выбором элементов из существующих) и конструктивная (разработкой недостающих элементов). Также, отмечается важность коммуникации участников процесса создания ПО. **Выводы:** должны присутствовать научные стадии (со стороны учителя), которые лишь потом переходят в более технические (со стороны разработчика); возможно объединения некоторых Представлений (например, предназначенных для разработчиков и программистов); необходимость в коммуникации логично ведет и к появлению промежуточных Представлений на базе различных терминологических аппаратов, способствующих участникам разработки (оперирующих с различными формами) передавать идею программы (т. е. ее содержание).

В статье [11] исследуется ЖЦ программных продуктов. Приводятся стадии создания автоматизированных систем в соответствии с ГОСТ 34.601 – 90 «Информационная технология. Комплекс стандартов на автоматизированные системы. автоматизированные системы. Стадии создания». Помимо это-

го, авторы статьи выделяют собственные стадии ЖЦ продукта: планирование, анализ и формирование требований, проектирование, разработка, тестирование, отладка, внедрение, эксплуатация и сопровождение. Также указываются классические модели ЖЦ (каскадная, V-образная, спиральная и др.). В работе обосновывается, что применение компьютерных методов обучения (и в особенности, ситуационных) позволяет более эффективно получать профессиональных пользователей программного продукта, упрощая тем самым стадию его внедрения. **Выводы:** помимо чисто технических стадий по созданию продуктов, могут иметь место и более высокоуровневые – концептуальные и архитектурные; процесс формирования требований является достаточно крупным и может занимать существенное место в ЖЦ; обучение пользователей является достаточно сложной и неотъемлемой частью внедрения программного продукта, поскольку, скорее всего, даже при четко сформулированной идее программы и безошибочной ее реализации различия в понятийных аппаратах не позволят пользователям работать с продуктом также «логично и безошибочно», как создателю.

Статья [12], являясь одной из множества от молодых авторов и, по совместительству, разработчиков программных продуктов, описывает подробный процесс создания программы с достаточно распространенным функционалом (в данном случае это «личный блокнот для записей мыслей»). Вначале автор провел опрос и собрал мнения о будущем продукте – сформирована его некоторая идея, затем были визуализированы действия с продуктом в виде диаграммы прецедентов с выделением основных функций – создан некий аналог концептуальной модели и базовой архитектуры, далее была получена диаграмма активности, детализирующая операции и прецеденты – алгоритмы записаны в блок-схемной форме (параллельно описан интерфейс продукта), после этого была проведена непосредственная реализация кода алгоритмов на Python и компиляция в выполняемый код – путем получения машинного кода с помощью утилиты Pyinstaller. Также автор провел тестирование продукта, что можно не относить к циклу разработки программ. **Выводы:** даже процесс создания простейшего программного продукта может быть разложен в виде создания его характеризующих представлений – идеи, концептуальной модели, архитектуры, алгоритмов, исходного и машинного кода.

Работа [13] посвящена базовым основам *программной инженерии* – т. е. проектированию, кодированию, распространению и поддержке ПО. В рамках методологии инженерии авторы указывают основные этапы ЖЦ программы: спецификация требований, проектирование, кодирование, тестирование, документирование и сопровождение.

Приведены такие стандарты программной инженерии, как ISO/IEC 12207 – Information Technology – Software Life Cycle Processes, SEI CMM – Capability Maturity Model (for Software), PMBOK – Project Management Body of Knowledge, SWBOK – Software Engineering Body of Knowledge и ACM/IEEE CC2001 – Computing Curricula 2001. Авторы подчеркивают, что ЖЦ ПО считается период его жизни от принятия решения о создании до полного изъятия из эксплуатации; такой цикл разбивается на последовательность процессов, имеющих собственные цели. **Выводы:** существует достаточное количество стандартов программной инженерии; классически под ЖЦ понимается не только период создания программ, но и их дальнейшее сопровождение (*прим. от автора* – в данной статье момент после создания выполняемой версии программы не рассматривается); программа проходит через несколько обособленных и довольно четко разграниченных стадий.

Цель работы [14] – ответ на 4, фундаментальных для ИБ программ, вопроса, касательно уязвимостей: 1) как они вносятся; 2) по каким причинам; 3) насколько долговечны; 4) как нейтрализуются. Данное исследование имеет непосредственное отношение к текущему, как раз и посвященному ЖЦ программ с уязвимостями. Источником информации в исследовании послужило описание уязвимостей из открытого источника – NVD (аббр. от англ. National Vulnerability Database – Национальная База Уязвимостей). Частичные ответы на указанные вопросы следующие: 1) обнаруженная уязвимость, как правило, появляется не из-за одной ошибки разработчика, а является следствием накопления «слабых» (с позиции безопасности элементов); 2) большинство уязвимостей появляется уже после 1 года начала проекта и сохраняются вплоть до 30-дневного срока до релиза, что объясняется высокой нагрузкой разработчиков в этот период; 3) средняя живучесть уязвимостей чуть менее 2-х лет, а вероятность нейтрализации уязвимостей начинает увеличиваться после 1 года с последнего внесенного исправления; 4) исправления, как правило, включают один файл, число добавленных строк в котором превышает в 2 раза число удаленных, а наиболее частым подходом устранения уязвимости является проверка входных данных. Также, в статье делаются следующие основные заключения: уязвимости возникают вскоре после создания новых файлов и добавляются туда при их сохранении; основной вклад уязвимостей вносят разработчики с высокой нагрузкой; живучесть уязвимостей оценивается, как высокая. Выводы: уязвимости появляются уже на первых стадиях разработки программ (т. е. до исходного кода, например, в архитектуре); их нейтрализация существенно затруднена на более поздних стадиях разработки (например, в исходном коде); возможность исправления уязви-

стей со временем растет, вероятно, по причине перехода на Представления программы, более раннее, чем исходный код (т. е. на те, в которых уязвимость была внесена); затрудненность вносить исправления в текущем Представлении может быть следствием того, что недостатки в программе (которые пока еще не переросли в уязвимости) появились в предыдущих Представлениях, а понятийные аппараты этих Представлений (а значит и недостатков) качественно отличаются.

Избегая лишней скромности, необходимо упомянуть и собственные авторские работы, непосредственно посвященные ЖЦ программ, поскольку они легли в основу текущего исследования. Так, в [15] описан цикл, состоящий из Представлений, упоминаемых в выводах к [12]; при этом, для Представлений указаны 3 типа уязвимостей по глубине их нахождения в абстракции кода – высоко-, средне- и низкоуровневые. В [16] делается такая же «разбивка» ЖЦ на Представления; однако, основная часть работы посвящена более глубокому изучению переходов между Представлениями с позиции формы и содержания программы.

4. СХЕМА ЖИЗНЕННОГО ЦИКЛА ПРЕДСТАВЛЕНИЙ ПРОГРАММЫ С УЯЗВИМОСТЯМИ

Всесторонний и кропотливый анализ элементов предметной области (включая выводы, сделанные по обзорам статей) – стадий и процессов создания программ, возможных Представлений, дерева их эволюции, различных парадигм программирования, способов Представления алгоритмов, языков программирования, сред исполнения, типизации уязвимостей и их точек возникновения и обнаружения – с последующей систематизацией и частичной группировкой позволил создать достаточно обобщающую схему ЖЦ Представлений программы (далее – Схема).

Граф эволюции Представлений программы (с делением на стадии и процессы создания) с потенциально возникающими уязвимостями, который и составляет обозначенную Схему, представлен на рисунке 1. На Схеме узлы графа являются существующими Представлениями (имеют вид прямоугольников с синим фоном), а ребра (стрелками отмечено направление) – пути их создания из предыдущих. Так, граф начинается с Представления Идеи программы (№ 1 на схеме), и заканчивается 3-мя Представлениями: Машинным (№ 14 на схеме), Сценарным (№ 11) и Байт-кодом (№ 15), каждое из которых готово для непосредственного выполнения с помощью специальных программно-аппаратных механизмов (имеют вид прямоугольников с боковыми линиями и желтым фоном, к которым ведут указатели прямоугольного вида; механизм прямоугольника с более тусклым фоном включает остальные механизмы).

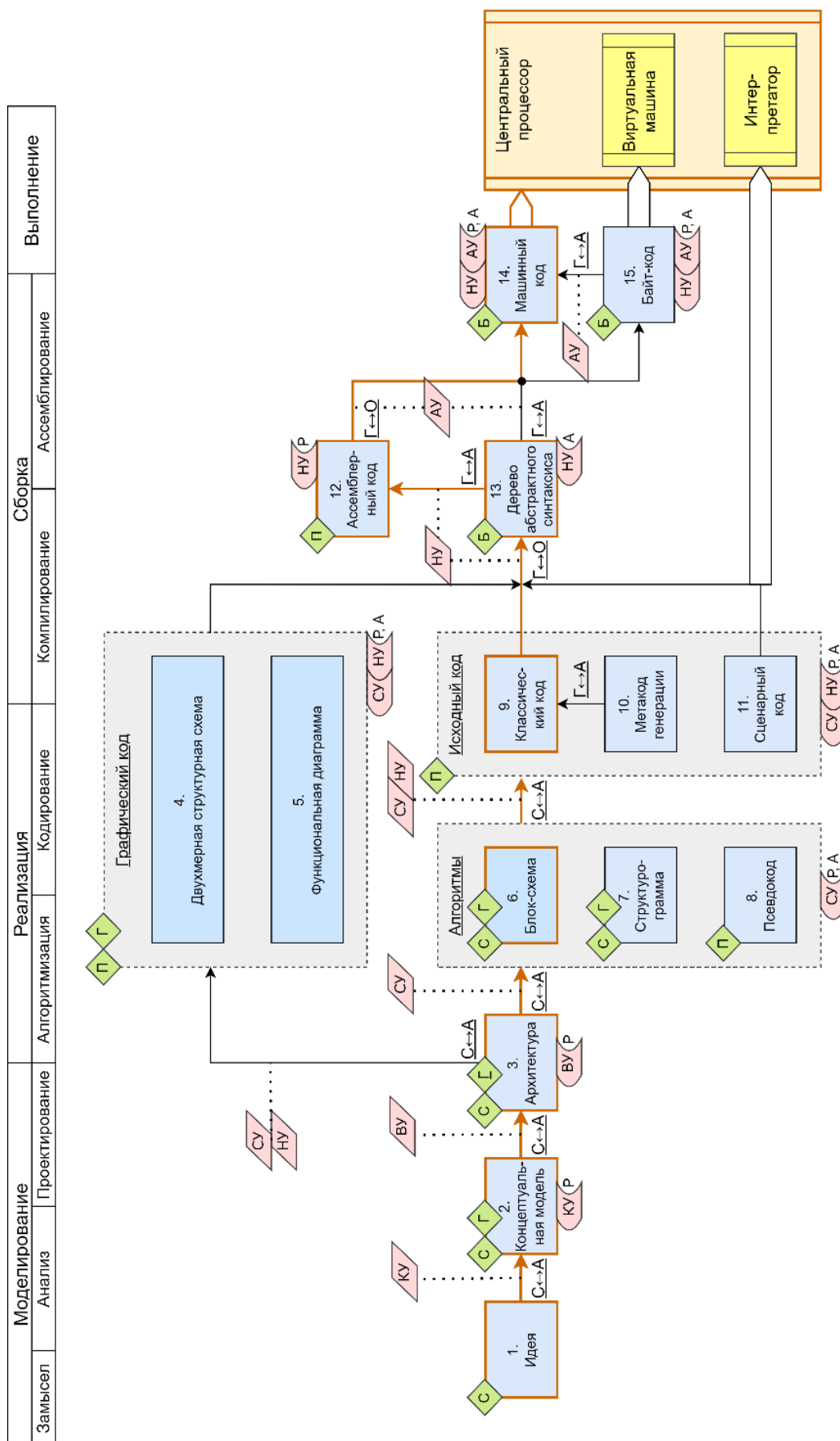


Рис. 1. Схема жизненного цикла Представлений программы с уязвимостями
Fig. 1. Life Cycle Scheme of Program Representation with Vulnerabilities

Согласно схеме, Представление № 14 исполняется на Центральном процессоре, для работы Представления № 15 необходима специализированная Виртуальная машина (имеющая, как правило, вид программного продукта и представляющая собой аналог реальной аппаратной платформы), а для выполнения Представления № 11 достаточно наличие Интерпретатора (часто, построчно выполняющего код). Некоторые Представления объединены в группы (имеют вид блоков с пунктирными границами и серым фоном) – входящее в группу и выходящее из нее ребро продлевается по умолчанию соответствующим образом на каждый элемент группы (за исключением Метакода генерации, из которого, как правило, может продуцироваться только Классический код).

Исходя из Схемы и ряда предыдущих умозаключений, предложим следующую 3-х компонентную классификацию уязвимостей.

Подкласс уязвимости – «структурный уровень»

Схема отражает уязвимости различных классов согласно их структурным уровням (что было обосновано ранее), а именно, следующие.

Во-первых, это концептуальные уязвимости (далее – КУ), заложенные в программу практически на первых стадиях ее создания; например, отсутствие учета понятий, связанных с аутентификацией пользователя (очевидно, если изначально не была указана столь базовая сущность, то и в архитектуре вряд ли она может появиться).

Во-вторых, это высокоуровневые уязвимости (далее – ВУ), такие, как ошибки в архитектуре программы: нарушение общих принципов ее функционирования, низкий уровень механизмов обеспечения ИБ и т. п.

В-третьих, это среднеуровневые уязвимости (далее – СУ), такие, как неверная реализация алгоритмов подпрограмм, передачи входных параметров, возврата из нее и т. п.

В-четвертых, это низкоуровневые уязвимости (далее – НУ), такие как ошибки в вычислениях, структурах данных, доступе к ним и т. п.

И, в-пятых, это атомарные уязвимости (далее – АУ), такие как ошибки в действиях для текущей среды выполнения программы, с помощью которых реализуются «низкоуровневые» вычисления и хранение данных; например, неверный выбор инструкций процессора или его регистров при «развертывании» операции сложения переменных для Центрального процессора.

Такое деление уязвимостей является более чем логичным, поскольку каждый новый класс присущ своей стадии разработки. Пожалуй, единственным исключением являются Представления группы Исходного кода, поскольку в них могут возникать одновременно СУ и НУ, которые также присущи

предыдущему и последующему Представлениям. Впрочем, это объясняется тем, что работа с Исходным кодом занимает основное время разработки любой программы, и оно, так или иначе, поглощает в себя окружающие Представления. Особое место в Схеме занимают Представления Графического кода, поскольку они объединяют в себе как Алгоритмы, так и сам Исходный код; соответственно, это ведет и к появлению в них одновременно СУ и НУ.

Подкласс уязвимости – «изменение содержания»

В связи с тем, что понятие уязвимости было введено, как отличие между Представлениями (в общем смысле – между начальным и конечным, а в частном – последовательность отличий между промежуточными Представлениями), то появление уязвимости в некотором Представлении можно понимать, как факт отличия содержания текущего Представления от Предыдущего. Саму же суть понятия «отличие» можно трактовать через результат сравнения множеств из элементов этих Представлений; что позволит расширить таксономию уязвимостью следующими подклассами:

1) во втором Представлении отсутствует элемент содержания, который был в первом – уязвимость подкласса «потеря функционала»;

2) во втором Представлении присутствует новый элемент содержания, который отсутствовал в первом – уязвимость подкласса «внесение функционала»;

3) элемент содержания второго Представления отличается от аналогичного элемента первого – уязвимость подкласса «модификация функционала».

Наглядная графическая интерпретация такой типизации подклассов уязвимостей представлена на рисунке 2.

Соответственно, совпадение множеств означает, что уязвимость не возникла (по крайней мере, при преобразовании этих двух Представлений); следовательно, ее подкласс отсутствует, поскольку функционал программы не изменился.

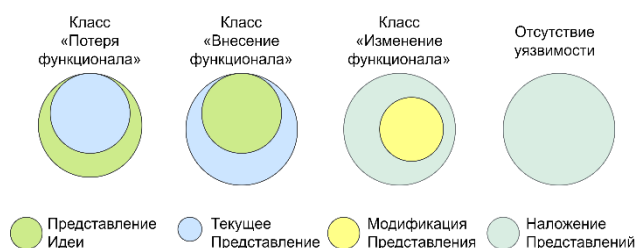


Рис. 2. Графическая интерпретация классификации уязвимостей по изменению содержания

Fig. 2. Graphical Interpretation of the Vulnerabilities Classification by Content Change

Необходимо отметить, что уязвимость 3-го подкласса в некотором смысле тождественна уязвимостям первых двух подклассов, поскольку удале-

ние одного элемента множества и добавление другого может быть истолковано как его изменение; данную коллизии разрешим соображением минимизации количества уязвимостей путем приоритета выбора для них одного 3-го подкласса вместо первых двух.

Подкласс уязвимости – «воздействие на информационные потоки»

Поскольку суть действия любой программы заключается в некотором изменении информации (что верно не только для императивных парадигм программирования – строго описывающих алгоритм работы, но даже и для декларативных – описывающих желаемый результат без составления шагов его достижения), то внесение изменений в содержание программы должно иметь некоторый эффект и на итоговую обработку информации. Так, например, удаление из программы проверок входных параметров приведет к появлению новых иноформенных потоков, не обрабатываемых ранее, и нарушению ее работы. С другой стороны, неверная реализация комплексной логики проверки параметров (например, ее реализация на основе логического И вместо логического ИЛИ) приведет к тому, что при корректных входных данных программа будет выдавать ошибку. Возможна и третья ситуация, отчасти близкая к комбинированию первых двух, когда вместо проверки параметра на один набор значений используется другой – т. е. информационный поток с верными входными данными исчез, а поток с неверными данными появился (например, ошибочная проверка установленного старшего бита числа вместо младшего). Вышесказанные размышления обосновывают введение еще одного способа классификации, наиболее субъективного из всех (хотя и продолжающего иметь достаточный уровень формализации), а именно – воздействие на информационные потоки вследствие внедрения уязвимости. Важно заметить, что эти классы достаточно хорошо коррелируют с классической триадой нарушений конфиденциальности, доступности и целостности (хотя и действуют на более «тонком» уровне – вместо глобального влияния всей программы на данные учитывается локальное влияние условно незначительных изменений ее содержания на внутренние информационные потоки), и, поэтому, будут введены подобным образом:

- аналог нарушения конфиденциальности информации, поскольку данные попадают к несанкционированным для этого обработчикам – уязвимость подкласса «появление информационного потока»;

- аналог нарушения доступности, поскольку существующие данные не доходят до санкционированных для этого обработчиков) – уязвимость подкласса «потеря информационного потока»;

- аналог нарушения целостности, поскольку данные доходят до санкционированных обработчиков, но в измененном виде – уязвимость подкласса «изменение информационного потока».

Объединение трех способов классификации уязвимостей (структурный уровень, изменение в содержании и воздействие на информационные потоки) как раз и определяет общую их таксономию, полностью построенную на базе предложенной Схемы, что говорит о целостности вводимого методологического аппарата. Классификации могут применяться независимо, что позволяет их считать вложенными. Так, класс любой уязвимости определяется совокупностью введенных подклассов.

Возникновение уязвимостей (имеющих вид параллелограммов с красным фоном) в процессе создания Представлений отражено в Схеме связывающими их пунктирными линиями (см. рисунок 1). Уязвимости, которые могут быть найдены в каждом из Представлений, отражены примыкающими к каждому Представлению сверху или снизу (имеют вид прямоугольника с гнутыми боками и красным фоном). Способ обнаружения уязвимостей в каждом Представлении может иметь как *ручной* тип – субъективно человеком, так и *автоматический* – специализированными программными средствами; естественно, возможно их объединение. На Схеме тип(ы) поиска уязвимостей указан(ы) справа от обозначения уязвимости (в вогнутой части прямоугольника).

Исходя из исторически сложившейся практики программирования, а также авторского опыта участия в создании крупных программных проектов, можно выделить следующие стадии создания программ и составляющие их процессы, расположенные как условная временная ось в верхней части Схемы.

Стадия *моделирования* – состоит из замысла (Идеи), разработки Концептуальной модели решения и проектирования Архитектуры программы.

Стадия *реализации* – состоит из алгоритмизации (т. е. создания Алгоритмов решения) и кодирования Исходного кода; также возможно их объединение, создавая тем самым Графический код (совмещающий алгоритмы и их высокоуровневую реализацию).

Стадия *сборки* – состоит из компиляции Исходного кода в Ассемблерный (через внутренние структуры утилит – Дерево абстрактного синтаксиса), и их ассемблирования в Машинный; современная практика создания программ также позволяет компилировать Исходный код напрямую в машинный.

Стадия *выполнения* – не входит по определению в процесс создания программ, но может использоваться для его отладки и тестирования в специ-

альной среде, которая приведена на Схеме для указания на факт и средства выполнения конечных Представлений. Так, Центральный процессор предназначен для непосредственной интерпретации инструкций Машинного кода, Виртуальная машина производит выполнение Байт-кода, а Интерпретатор предназначен для выполнения Сценарного кода. Важно отметить, что фактически Виртуальная машина и Интерпретатор являются лишь комплексами программ, также исполняемыми Центральным процессором (что отмечено на Схеме вложенностью графических форм); тем не менее, в рамках моделирования программы они являются отдельными независимыми сущностями.

Термины, использованные выше для обозначения стадий и процессов, не всегда совпадают со стандартизованными⁶ (некоторым из них около полувека), однако, по авторскому мнению, наилучшим образом (по аналогии с понятийным аппаратом) отражают суть и содержание исследуемого процесса.

Каждое из Представлений может принимать следующие формы или их комбинацию (имеют вид ромбов с зеленым фоном в левом верхнем Представления): *словесная* – с помощью естественного языка; *графическая* – в виде блок-схем, диаграмм, изображений графов; *программно-языковая* – с помощью формально-знакового текста на языках программирования; *бинарная* – в виде набора байтов (реже битов).

Получение последующих Представлений из текущих осуществляется с помощью превращений следующих типов: *синтез* – результат интеллектуальной деятельности человека, как правило, слабо формализуемый (например, получение из Блок-схем алгоритмов программы ее Исходного кода требует выполнение существенной исследовательской деятельности по выбору подходящих шаблонов и способов реализации логики); *генерация* – результат работы специализированных программных средств, как правило, основанный на заранее заложенных строгих правилах преобразования (например, получение Ассемблерного кода из Исходного в упрощенном виде представляет собой перевод конструкций языка программирования через их внутреннее представление в текстовую запись соответствующих инструкций процессора).

Исходя из вышесказанного, логично ввести и обратные типы превращений (если существующий не практически, то хотя бы теоретически), а именно следующие: *анализ* – по аналогии с синтезом, также результат деятельности человека, но

направленный на восстановление Представления (например, исходя из совокупного понимания Исходного кода подпрограммы можно восстановить и ее Алгоритмы в виде Блок-схем); *обратная генерация* – также, результат работы программных средств по формальным правилам, но в виде «реверс-инжиниринга» (например, восстановление Исходного кода из Машинного, называемое термином «декомпиляция», было описано автором в диссертационном исследовании [17, 18]). На Схеме получение каждого Представления из предыдущего указано в следующем формате: « $X \leftrightarrow Y$ », где X – первая буква типа прямого преобразования (т. е. «А» или «С»), а Y – первая буква типа обратного преобразования (т. е. «Г» или «О»). Можно предположить, что тип превращений напрямую зависит от степени формализации Представлений, поскольку генерация (прямая и обратная) может производиться лишь при строгом соблюдении правил описания программы; в отличие от синтеза и анализа, где отсутствие формализованных правил преобразования нивелируется творческой составляющей эксперта.

Важно отметить, что, согласно предыдущему авторскому исследованию [19], в части учета когнитивного аспекта восприятия кода, содержание может быть декомпозировано на две компоненты: *логику* и *словарь (или базис)*. В этом случае содержание решения определяется некоторой логикой, построенной на базе словаря (например, Архитектура в виде логических модулей или Исходный код в виде конструкций языка). Форма в данном случае является связкой между словарем и способом взаимодействия с содержанием. При описании каждого Представления далее примеры компонент содержания будут пояснены на интуитивно понятных примерах.

5. ПРЕДСТАВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ VS УЯЗВИМОСТИ

Приведем все существующие Представления с последовательным указанием следующих их характеристик: общее назначение, форма и содержание, связь с другими Представлениями, появление уязвимостей и их обнаружение, примеры Представлений и способы их выполнения (в случае наличия возможности). Это позволит создать законченную эволюционную картину возможных ветвей ЖЦ всех Представлений и уязвимостей, включая особенности их появления и исчезновения.

1. Идея (№ 1 на Схеме)

Назначением Идеи программы является отражение некоторого замысла программы и ее функционала с выделенными характеристиками и свойствами.

Форма Представления является словесной, поскольку отсутствует какая-либо возможность

⁶ ГОСТ Р ИСО/МЭК 12207-2010 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. М.: Стандартинформ, 2011; ГОСТ 19.102-77 Единая система программной документации. Стадии разработки. М.: Стандартинформ, 2010.

формализации. Содержание задается совокупностью осмысленных предложений в базисе используемого разговорного языка.

Представление считается началом любой программы и создается как результат творческого процесса решения крупной задачи, его вектор. Оно может быть восстановлено из Концептуальной модели путем анализа, поскольку данное и последующее Представления практически не формализуемы.

Представление не может иметь уязвимостей (об этом выше), поскольку оно используется как будущий прообраз желаемого результата, т. е. является «идеальным», несмотря на все свои недостатки и просчеты. Как результат, поиск уязвимостей тут также не имеет смысла.

Описание Представления возможно любыми способами (преимущественно когнитивными), поскольку никакого конкретного вида на данном шаге решение пока не имеет. Типичным примером Представления может быть записанные (систематизированные) результаты «мозгового штурма».

II. Концептуальная модель (№ 2 на Схеме)

Концептуальная модель программы является его Представлением, определяющим основные понятия, их структуру, взаимосвязи и особенности с указанием направления решения и используемых подходов. Здесь необходимо выделение базовой смысловой структуры и соответствующего терминологического аппарата.

Форма Представления является словесно-схемной (или словесно-графической), как наиболее подходящей для описания обобщенных моделей с привязанным текстовым пояснением. Содержание задается совокупностью утверждений, логически связанных с помощью графической схемы (или схем).

Представление создается в результате синтеза возможностей по воплощению Идеи разрабатываемой программы путем первоначальной условной формализации в направлении выбранного решения. По причине все также слабой формализации текущего и последующего (Архитектуры) Представлений, данное может быть восстановлено только путем применения анализа.

В данном Представлении могут появляться КУ вследствие неверного концепта основной идеи. Их поиск на сегодня возможен только ручным способом по причине крайне высокого уровня абстракции и уникальности Представления, оперирующего понятиями.

По этим же причинам какие-либо стандартные виды Представления отсутствуют. Примером Представления могут быть любые модели достаточного уровня абстрактности и носящий определяющий для создаваемой программы характер, имеющие текущее назначение и наиболее подходящий вид.

III. Архитектура (№ 3 на Схеме)

Архитектура программы является его наиболее полным высокоуровневым Представлением в виде схемы, близкой к Исходному коду, описываемой с использованием специфических особенностей (технологий, языков программирования, шаблонов/парадигм, средств реализации, форматов и т. п.). Архитектура определяет общую структуру программы, его физические и логические модули, их взаимодействие. С этой позиции Архитектура задает зоны ответственности сущностей (а также их взаимосвязи) каждого понятия, введенного Концептуальной моделью.

Форма Представления является графической (со словесными комментариями). Содержание задается аналогичным с Концептуальной моделью образом, но с раскрытием ее базовых элементов в сторону непосредственной реализации.

Представление создается на основании Концептуальной модели в результате синтеза требований и возможностей с применением опыта эксперта-архитектора. Хотя последующие возможные Представления (Алгоритмы или Графический код) и обладают определенной степенью формализации, тем не менее, какие-либо удовлетворительные средства обратной генерации из них Архитектуры отсутствуют, поэтому последняя восстанавливается с помощью ручного анализа.

В данном Представлении могут появляться ВУ вследствие ошибок в проектировании. Исходя из крайне сложной формализации и субъективности оценки, в большинстве случаев такие уязвимости могут быть найдены только ручным способом. Примером Представления может быть описание Архитектуры с помощью языков специального назначения ADLs (аббр. от англ. Architecture Description Languages – языки описания архитектуры) или их потенциального преемника в виде UML.

Различные пути эволюции алгоритмов до стадии выполнения позволяют объединить в группы их некоторые Представления, которые имеют по умолчанию общие входы и/или выходы, а также, как правило, одинаковые формы и способы поиска уязвимостей.

Группа графического кода (№№ 4–5 на Схеме) содержит в себе Представления, совмещающие алгоритмы программы и ее исходный код, расширяя область программирования из простого текстового в более наглядное – визуальное. Данная группа состоит из Двухмерной структурной схемы и Функциональной диаграммы, отличающейся от первой спецификой целевого применения.

Группа алгоритмов (№№ 6–8 на Схеме) позволяет разделить различные варианты Представления Алгоритмов программы: Блок-схема (в виде графа последовательности шагов решения зада-

чи), Структурограмма (в виде структуры блоков решения задачи) и Псевдокод (в виде текстового описания на специальном языке, еще не готовом для компиляции).

Группа Исходного кода (№№ 9–11 на Схеме) содержит различные варианты текстового решения задачи человеком на специальном языке программирования. Наиболее общепринятым и полноценным Представлением является код на классических языках (C/C++/C#/Java/Pascal и пр.), часть которого может быть создана из Метакода генерации с помощью автоматических средств. Сценарный код является упрощением Классического кода путем большего функционала внешних библиотек, минимизации синтаксиса и его лучшей наглядности.

IV. Двухмерная структурная схема (№ 4 на Схеме)

Представление используется в процессе двухмерного структурного программирования, совмещающая в себе две важнейшие, и при этом принципиально разные функции: графическая визуализация алгоритмов выполнения и текстовая программная реализация его элементов. Таким образом, Представление считается симбиозом двух других – из групп Алгоритмов и Исходного кода. Представления могут совместно использоваться при создании ПО как *инженерами* (не являющимися программистами), описывающими более абстрактную логику решения задачи, так и *программистами*, задающими ее менее абстрактную и детальную реализации: таким образом, Представление применимо в качестве языка общения и взаимодействия специалистов этих двух типов.

Формой Представления является совокупность графической и программно-языковой форм – *программно-графическая*. Содержание задается совокупностью следующих слоев: логикой работы блоков программы в базисе стандартных графических элементов, и текстового наполнения этих элементов деталями реализации их функционала в базисе некоторого языка программирования.

Представление создается в результате синтеза алгоритмов из Архитектуры программы с последующей их конкретизацией на языке программирования. Видоизменения Представления могут производиться одновременно как на графической составляющей, так и на текстовой, поскольку они представляются жестко-связанными сущностями. Двухмерная структурная схема может быть восстановлена из Древа абстрактного синтаксиса путем обратной генерацией, поскольку Древо частично содержит необходимую для этого информацию (деление на подпрограммы, именованные переменные, структуры циклов и ветвлений и т.п.).

В данном Представлении могут появляться как СУ, так и НУ. Первые связаны с неверными алго-

ритмическими решениями задач, определенных архитектурой (т. е. с инженерами), вторые же – с их реализацией или интерпретацией (т. е. с программистами). Применимы и ручные, и автоматические способы поиска уязвимостей. Первые более захватывают область СУ, вторые же – НУ. Примером Представления могут быть схемы языка ДРАКОН [20, 21] или используемые в Р-программировании, а также некоторые диаграммы активности языка UML [22].

V. Функциональная диаграмма (№ 5 на Схеме)

Представление является аналогом Двухмерного структурного в части симбиоза, но имеет собственное применение, что вносит определенные существенные отличия и в итоговый функционал программы. Относится к разряду графических языков, предназначенных в основном для программирования логических контроллеров, применяемых для автоматизации промышленного производства и ориентированных на работу посредством сигналов ввода/вывода. В отличие от Двухмерного структурного, Представление может быть полноценно использовано специалистами одного типа – *инженерами* логических контроллеров.

Впрочем, качественных отличий в принципах формирования формы и содержания от Двухмерной структурной схемы нет – используется графическая форма записи логики работы блоков программы с программно-языковой формой реализацией их функционала.

Согласно декларации о группировке Представлений, Функциональные диаграммы получаются из Архитектуры в результате синтеза и могут быть восстановлены из Древа абстрактного синтаксиса путем обратной генерации. Аналогичным образом, диаграммы могут иметь как СУ, так и НУ, для поиска которых применимы как ручные, так и автоматические способы. Примером Представления могут быть языки программирования FBD (*аббр. от англ. Function Block Diagram* – функциональные диаграммы блоков) [23], SFC (*аббр. от англ. Sequential Function Chart* – последовательные функциональные схемы) [24] и LD (*аббр. от англ. Ladder Diagram* – релейная логика) [25].

VI. Блок-схема (№ 6 на Схеме)

Одной из канонических форм Представления Алгоритмов является графическая в виде Блок-схем со словесным содержанием ее элементов (совместно, в базисах разговорного и программно-го языков). По сути, Представление переназначено для частично формализованного описания алгоритмов (или процессов) в «гостированном» для Российской Федерации виде.

Представление создается в результате синтеза алгоритмов из Архитектуры, явно следуя назначению ее модулей или подсистем. Поскольку каждый

алгоритм решает определенную задачу, зачастую являющуюся уникальной и/или имеющую особые требования, то процесс создания представляется полностью творческим. Восстановление Блок-схемы, как правило, осуществляется экспертом в результате анализа [26] (например, в рамках изучения Исходного кода на предмет СУ).

В данном Представлении могут появляться СУ вследствие неверного решения алгоритмами подзадач, определенных модулями. По данному Представлению возможен поиск СУ, поскольку оно не определяет Архитектуру (имеющую ВУ) и не содержит конкретной реализации алгоритмов (имеющих НУ), а находится между этими уровнями абстракций. Способ поиска уязвимостей является исключительно ручным. Примером Представления являются блок-схемы алгоритмов в соответствии с ГОСТ 19.701-90 (см. сноску 4).

VII. Структурограмма (№ 7 на Схеме)

Структурограмма является своеобразным аналогом Блок-схемы и предназначена для описания алгоритмов, составленных в соответствии со структурной парадигмой программирования. Последнее означает, что в данном Представлении должны отсутствовать безусловные переходы, на которых с формальной точки зрения построены Блок-схемы (в них безусловный переход является основным способом связывания элементов).

В остальном используемые форма и содержания Представлений под №№ 6 и 7 совпадают.

Согласно декларации о группировке Представлений, способы получения и восстановления Структурограмм такие же, как и для Блок-схем. В ней также могут возникать СУ, хотя для ручного поиска используются несколько иные подходы, делая его более эффективным. Примером Представления могут быть диаграммы Насси – Шнейдермана [27].

VIII. Псевдокод (№ 8 на Схеме)

Псевдокод, хотя и отнесен к группе Алгоритмов, тем не менее имеет существенные отличия от остальных Представлений группы.

Форма Представления является программно-языковой, что позволяет дополнительно применять автоматические средства поиска уязвимостей. Содержание задается совокупностью описания логики выполнения блоков программы в базе некоторого алгоритмического языка (например, С-подобного, но без использования типов переменных и с заменой тела некоторых подпрограмм на соответствующие человеко-ориентированные комментарии).

В остальном способы получения и восстановления Представления, а также уязвимости и их поиск, аналогичны другим элементам группы Алгоритмов. Примером Представления может быть учебный

алгоритмический язык и, с некоторыми поправками, семейство языков Algol (сокр. от англ. Algorithmic Language – алгоритмический язык) [28]. В современном понимании любой императивный язык программирования является алгоритмическим, однако такая трактовка здесь лишь приведет к подчеркнутому смешению терминологии и понятийной базы.

IX. Классический (исходный) код (№ 9 на Схеме)

Классический исходный код является основным «рабочим» Представлением, используемым программистами, и последним, подверженным влиянию человека. Использование термина «классический» призвано отделить данное Представление от других – Метакода генерации и Сценарного кода, имеющим иное предназначение и существенно более сложные парадигмы программирования. Назначением Представления является реализация алгоритмов на выбранном языке программирования с последующей отладкой, поддержкой, документированием и т. п.

Форма Представления является программно-языковой и достаточно точно отражает содержание Алгоритмов, поскольку определяет их пошаговую конкретную реализацию. Содержание задается детальным описанием реализации программы в базе выбранного языка программирования.

Следуя классической схеме программной инженерии, Исходный код получается из Алгоритмов (чаще – стандартизованных Блок-схем и Структурограмм, реже – из Псевдокода) в процессе рутинной деятельности типового программиста. Более частным случаем является получение Представления из Метакода путем применения специальных генераторов (некоторые детали этого будут описаны далее). Восстановить же Представление можно аналогичным с Графическим кодом образом – из Дерева абстрактного синтаксиса; впрочем, в случае Исходного кода данное восстановление является более распространенным. Так, например, различного рода декомпиляторы часто вначале по Машинному коду строят внутреннее Дерево абстрактного синтаксиса (с дополнительно навешанными на него связанными структурами), производят на нем оптимизирующие и гармонизирующие (для лучшего восприятия результата человеком) действия, а затем генерируют Классический исходный код или его аналоги [29].

Поскольку Представление является соединительным звеном между собственно алгоритмами и их итоговой низкоуровневой реализацией, то в нем могут появляться как НУ, так и СУ вследствие ошибок в реализации алгоритмов или их неверной интерпретации программистом. Такие же классы уязвимостей могут появляться и при ошибках в реализации утилит, генерирующих новый код по Метакоду. Способы поиска уязвимостей примени-

мы как ручные, так и автоматические. Первые более захватывают область СУ, вторые же – НУ. Примером Представления может быть любой большого множества средне- и высокоуровневых императивных языков программирования (поскольку единого универсального языка еще пока не создано [30]), наиболее яркими представителями которого являются Pascal, Java и C/C++/C#-подобные.

Несмотря на то, что изначально Классический исходный код не создавался для непосредственного выполнения, однако существуют проекты, которые с некоторыми ограничениями позволяют это делать для некоторых языков программирования. Так, проект Picoc (<https://github.com/jpoirier/picoc>) представляет собой достаточно миниатюрный интерпретатор языка C (естественно, без полноценной поддержки работы с указателями и других платформенно-зависимых особенностей программ).

X. Метакод генерации (№ 10 на Схеме)

Представление является промежуточным, предназначенным для генерации Исходного кода (в преобладающем большинстве – Классического).

Оно имеет программно-языковую форму и часто соответствует декларативной парадигме программирования (что является допустимым исключением из рамок введенных ранее понятий). Содержание задается аналогичным для Классического кода способом. Представление косвенно создается по Алгоритмам программы и, как правило, содержит правила для генерации отдельных частей реализации шагов решения задачи.

В остальном Представление и его уязвимости аналогично Классическому исходному коду. Исключением является теоретическая возможность восстановления Метакода из созданного по нему Классического кода, что, впрочем, крайне трудоемко и имеющий малую практическую значимость.

Примером Представления могут быть формальные грамматики, заданные с помощью синтаксиса для генераторов лексического анализатора Lex (Flex для GNU) и синтаксического анализатора Yacc (Bison для GNU) [31].

XI. Сценарный код (№ 11 на Схеме)

Представление Сценарного кода достаточно близко к Исходному (и имеет такие же форму и содержание), хотя и оперирует более крупными программными компонентами и функционалом; такое отличие в конечном итоге находит отражение, как в синтаксисе кода, так и в его дальнейших превращениях и заключительном выполнении.

Согласно декларации о группировке Представлений, Сценарный код может быть получен из Алгоритмов в результате синтеза и восстановлен из Древа абстрактного синтаксиса путем обратной генерации; он может иметь как СУ, так и НУ, для

поиска которых применимы как ручные, так и автоматические способы [32]. Примером Представления могут быть скриптовый язык JavaScript, интерпретируемый язык Perl, сценарий командной строки Shell Script [33].

Код данного представления готов для непосредственного выполнения соответствующим интерпретатором.

XII. Ассемблерный код (№ 12 на Схеме)

Представление задает конечные регистры и инструкции для выполнения процессором; оно также содержит пользовательские имена, сегменты с данными, а также ряд другой более специфичной информации.

Форма Представления является программно-языковой, которая уже в меньшей степени ориентирована на человека, но пока еще не подходит для выполнения машиной. Содержание задается описанием логики работы аппаратной части в базисе синтаксиса инструкций процессора.

Представление генерируется из Древа абстрактного синтаксиса (которое будет описано далее) и зачастую не используется, поскольку конкретные машинные инструкции, готовые для выполнения, могут быть созданы без промежуточного Ассемблерного кода. Восстановить Ассемблерный код можно из Машинного в процессе дизассемблирования, что в общем случае является тривиальной и хорошо отлаженной программной процедурой.

В данном Представлении могут появляться НУ вследствие неверной работы модуля генерации (по предыдущему представлению) или низкоуровневой оптимизации Машинного кода; впрочем, вероятность этого крайне мала. По данному Представлению возможен поиск НУ трудоемким ручным способом; в ряде случаев применяется автоматизации. Однако вследствие того, что Ассемблерный код считается промежуточным, их поиск откладывается на последующие Представления. Примером Представления может быть любой машинно-ориентированный язык низкого уровня для заданного процессора, например: MASM и TASM [34] для семейства x86, vasm для семейств PowerPC и ARM.

Хотя, как было сказано, код данного Представления классически не считается выполняемым; тем не менее существуют проекты, которые позволяют это делать, даже непосредственно через Интернет-ресурсы (например, <https://www.tutorialspoint.com/compile-assembly-online.php> или <https://www.jdoodle.com/compile-assembler-nasm-online/>).

XIII. Древо абстрактного синтаксиса (№ 13 на Схеме)

Представление является промежуточным между Исходным кодом, ориентированным на челове-

ка, и автоматомоориентированным Ассемблерным, а в последствие и Машинным, кодом. Оно, как правило, используется для преобразования кода в процессе работы соответствующих программных средств – *компиляторов*, при этом, частично отбрасывая ненужную для работы программы метайнформацию (например, комментарии к исходному коду, типы переменных и т. п.).

Форма Представления достаточно сильно зависит от конкретной реализации компилятора, но, как правило, она имеет бинарный вид; хотя в ряде случаев Дерево абстрактного синтаксиса может храниться во внешних файлах XML- или JSON-формата. Соответственно, способы задания содержания чаще всего имеют вид связей между разнотипными узлами (т. е. представляют множество классических графов и/или таблиц).

Исходя из назначения Дерева абстрактного синтаксиса, оно получается из Исходного кода (в процессе компиляции). Восстановить Представление можно из последующих Представлений – Ассемблера, Машинного кода и Байт-кода. Способ восстановления, как правило, является ручным (т. е. требует применения экспортного анализа), хотя и существует некоторый пул программных средств, проводящих такую процедуру – *декомпиляцию* (следуя названию – процесс, обратный компиляции). Тем не менее, отсутствие теоретических и практических возможностей полноценной реализации декомпиляторов (с учетом ограниченности поддерживаемых входных нотаций Машинного, Ассемблерного или Байт-кода, и получаемых синтаксисов Исходного кода) при крайней потребности в подобных средствах реверс-инжиниринга, переводят данную задачу в разряд проблемы, остро стоящей для области ИБ в части поиска уязвимостей в программах. В подтверждение этого приведем здесь ссылку на страницу авторского сайта с указанием некоторых наиболее известных на данный момент декомпиляторов: <http://demono.ru/links/decompilers>.

Особенность Представления заключается в хранении древовидной структуры кода (с более сложными связями между узлами), что позволяет решать определенные задачи более эффективно – например, производить различные типы оптимизации. Также Представление позволяет осуществлять более глубокий анализ программ непосредственно перед и во время выполнения. Уязвимости и их поиск совпадают с аналогичными у Ассемблерного кода, хотя сами способы будут более эффективным. Так, для Байт-кода языка Python существует инструмент Bandit [35], который использует плагины для обработки Дерева абстрактного синтаксиса на предмет поиска проблем в безопасности.

Примерами Представления, в общем случае, могут служить любые описания Исходного кода с

помощью Дерева абстрактного синтаксиса в подходящем для этого формате. Как правило, внутренняя структура такого Дерева в каждом программном средстве обработки Исходного кода собственная.

XIV. Машинный код (№ 14 на Схеме)

Представление является наиболее «дальним» от Идеи и представляет собой нечитательные данные, строго задающие выполнение инструкций процессора.

Форма Представления является бинарной. Содержание Представления, аналогично Ассемблерному коду, задается описанием логики работы аппаратной части, но уже в базисе кодирования инструкций процессора.

Представление генерируется по Ассемблерному коду с применением специальных программных средств – *ассемблеров*, полностью опуская всю метайнформацию, ненужную для выполнения процессором (например, имена переменных). Распространенной практикой является генерация Представления напрямую по Исходному или Графическому коду путем компиляции. Также для ускорения работы Представление может быть получено из Байт-кода (в том числе, в процессе работы виртуальной машины – с помощью т. н. механизма Just-In-Time [36]). Способ восстановления Машинного кода отсутствует, поскольку оно является конечным в Схеме.

В данном Представлении могут появляться АУ вследствие неверной работы ассемблеров кода или Just-In-Time-утилит; однако вероятность этого крайне мала. Из-за своей полной формализации Представление подходит для автоматического анализа на предмет НУ и АУ; впрочем, по частой причине отсутствия Исходный кодов программ, а также технических сложностей преобразования Представления в предыдущие, Машинный код также вынужденно анализируется и вручную. Примером Представления может быть любая любой бинарный образ для встроеного устройства или UEFI-прошивка [37].

Код данного Представления готов для непосредственного выполнения на Центральном процессоре.

XV. Байт-код (№ 15 на Схеме)

Байт-код является Представлением, аналогичным Машинному, но предназначенному для выполнения на виртуальной машине. Байт-код считается прошедшим синтаксический и семантический анализ и готовым для непосредственного выполнения. Его особенностью является независимость от конечного аппаратного обеспечения, на котором он должен работать, поскольку код не имеет платформенно-зависимых особенностей;

они полностью перенесены на сторону реализации виртуальной машины.

Представление имеет бинарную форму и содержание, аналогичные Ассемблерному и Машинному коду, но с учетом базиса инструкций виртуальной машине.

Отличительной чертой Байт-кода является минимизация в нем уязвимостей из-за особенностей (с позиции ИБ) языков программирования, для которых он генерируется; в частности, в них отсутствует работа с памятью, ограничен доступ к файловой системе, применяется встроенная верификация и автоматическая «сборка мусора» (т. н. *Garbage Collection*) и т. д. В данном Представлении могут появляться АУ, а поиск их осуществляется автоматическими и трудоемкими ручными способами (по аналогичным с Машинным кодом причинам). Примером Представления может быть высокоуровневый Ассемблерный код для виртуальных машин: CIL (аббр. от англ. *Common Intermediate Language* – общий промежуточный язык) для .Net [38] и JBC (аббр. от англ. *Java Byte Code*) для Java [39].

Код данного Представления готов для непосредственного выполнения на виртуальной машине.

Исходя из Схемы (см. рисунок 1), можно сделать важнейший вывод – за исключением Машинного и Байт-кода, уязвимости обнаруживаются исключительно в тех Представлениях, в которых они были внесены. Так, например, КУ, внесенная при создании Концептуальной модели, обнаруживаемая именно там (ручным способом), а более «дальние» Представления, такие, как Исходный, для этого не подходят. В случае же Машинного и Байт-кода, хотя при создании могут вноситься только АУ, однако по ним также возможен поиск НУ – что обосновывается близостью этих классов уязвимостей и тем, что для генерации Представлений из Древа абстрактного синтаксиса применяются достаточные «прямолинейные» правила.

7. ЗАКЛЮЧЕНИЕ

Проведенное в работе схематическое моделирование программы с уязвимостями с позиции эволюции ее Представлений, основанное на богатой авторской практике и подкрепленное реальными примерами, позволяет более глубоко взглянуть на динамику процесса создания программ, учитывая появление и обнаружение уязвимостей, что приводит к ряду следующих умозаключений.

Во-первых, проведенный обзор современных исследований в области моделирования ЖЦ показал, что достаточно абстрактные (но без потери сущности процессов) и системные модели предметной области отсутствуют, что свидетельствует о новизне представленного авторского подхода. Ближайшие аналоги «грешат» фрагментарностью, отсутствием причинно-следственных

связей и конструктивности выводов. Автором впервые введено четкое и не противоречащее практике описание механизма создания программ с делением на стадии и процессы, в которых непрерывно «зарождаются» и «живут» стратифицированные уязвимости.

Во-вторых, было установлено, что после каждой стадии и процесса создания программы, типы возникающих и обнаруживаемых уязвимостей в большинстве случаев совпадают, что позволяет сделать вывод о необходимости использования для каждого Представления собственных методов поиска, оперирующих соответствующими элементами абстракции. Также возможным решением может быть трансформация Представлений из более поздних в более ранние – т. е. их восстановление, поскольку связанное с этим повышение уровня абстракции также и поднимет структурный уровень обнаруживаемых уязвимостей. Часть из Представлений автоматически преобразуемы в предыдущие (например, Машинный код в Ассемблерный, Байт-код в Исходный), часть – с применением ручного анализа (например, Алгоритмы в Архитектуру), а часть – с применением специализированных программных средств (например, Машинный код в Алгоритмы [40]).

И, в-третьих, очевидная стадийность при создании программ и возможность прямого выполнения ее некоторых конечных Представлений (от бинарного Машинного кода до Сценарного текстового) позволяют предположить следующий вариант описания процесса программного инжиниринга, объединяя и полностью структурируя все существующие Представления. Так, полный путь создания программы для решения поставленной задачи может представлять собой пирамидообразный и конкретизирующий пошаговый процесс преобразования ее Представлений, каждое из которых является в некотором смысле завершенным и может быть выполнено реально или ментально. Например, если упрощенный путь создания программы для вычисления операций над входными значениями (простейший калькулятор) будет проходить через Представления Архитектуры, Алгоритмов и Машинного кода, то каждое из них гипотетически выполнимо в собственной среде с получением собственных (иногда обобщенных) результатов, построенных на собственном базисе, характерном для содержания Представления: для Архитектуры это будет взаимосвязь значений, для Алгоритмов – множество вычисляемых значений, а для Машинного кода – конкретные значения для заданных входных. Такой подход к описанию создания программ позволит на каждом шаге как локализовать появление в нем уязвимостей, так и применять специализированные и максимально эффективные способы их поиска.

Продолжение следует...

Список источников

1. Благодаренко А.В., Разработка метода, алгоритмов и программ для автоматического поиска уязвимостей программного обеспечения в условиях отсутствия исходного кода. Дис. ... канд. техн. наук. Таганрог: Южный федеральный университет, 2011. 140 с.
2. Марков А.С., Фадин А.А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. № 3(51). С. 56–61.
3. Баев Р.В., Скворцов Л.В., Кудряшов Е.А., Бучацкий Р.А., Жуйков Р.А. Предотвращение уязвимостей, возникающих в результате оптимизации кода с неопределенным поведением // Труды Института системного программирования РАН. 2021. Т. 33. № 4. С. 195–210.
4. Буйневич М.В., Израйлов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 1. Типы взаимодействий // Защита информации. Инсайд. 2019. № 5(89). С. 78–85.
5. Буйневич М.В., Израйлов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 2. Метрика уязвимостей // Защита информации. Инсайд. 2019. № 6(90). С. 61–65.
6. Максимова Е.А. Методы выявления и идентификации источников деструктивных воздействий инфраструктурного генеза // Электронный сетевой политематический журнал "Научные труды КубГТУ". 2022. № 2. С. 86–99.
7. Максимова Е.А. Аксиоматика инфраструктурного деструктивизма субъекта критической информационной инфраструктуры // Информатизация и связь. 2022. № 1. С. 68–74. DOI:10.34219/2078-8320-2022-13-1-68-74
8. Максимова Е.А., Буйневич М.В. Метод оценки инфраструктурной устойчивости субъектов критической информационной инфраструктуры // Вестник УрФО. Безопасность в информационной сфере. 2022. № 1(43). С. 50–63. DOI:10.14529/secur220107
9. Максимова Е.А. Инфраструктурный деструктивизм субъектов критической информационной инфраструктуры. Москва – Волгоград: Волгоградский государственный университет, 2021. 181 с.
10. Вихрев В.В. О механизме реализации коэволюционной модели жизненного цикла разработки компьютерных программ для обучения // Системы и средства информатики. 2014. Т. 24. № 4. С. 168–185. DOI:10.14357/08696527140411
11. Галимянов А.Ф., Аль-Саффар Н.М.Ф. Жизненный цикл программного продукта с большим количеством пользователей: на примере обучающих программ // VI Международные Махмутовские чтения. Проблемное обучение в современном мире (Казань, Елабуга, 12–14 апреля 2016): сборник статей. Елабуга: Казанский (Приволжский) федеральный университет, Елабужский филиал: 2016. С. 129–133.
12. Слепов В.А. Проектирование и разработка программного продукта "личный блокнот для записи мыслей" // Научное обозрение. Технические науки. 2020. № 4. С. 58–63.
13. Гишлагаев С.У., Минаев О.М. Базовые основы и процессы программной инженерии // XXVII Всероссийская научно-практическая конференция. Цифровизация образования: теоретические и прикладные исследования современной науки (Ростов-на-Дону, Россия, 25.01.2021). Ростов-на-Дону: Южный университет (ИУБиП), ООО "Издательство ВВМ", 2021. Ч. 1. С. 18–22.
14. Iannone E., Guadagni R., Ferrucci F., De Lucia A., Palomba F. The Secret Life of Software Vulnerabilities: A Large-Scale Empirical Study // IEEE Transactions on Software Engineering. 2023, Vol. 49. Iss. 1. PP. 44–63. DOI:10.1109/TSE.2022.3140868
15. Buinevich M., Izrailov K., Vladiko A. The life cycle of vulnerabilities in the representations of software for telecommunication devices // The Proceedings of 18th International Conference on Advanced Communication Technology (ICACT, Pyeongchang, South Korea, 31 January–3 February 2016). IEEE, 2016. PP. 430–435. DOI:10.1109/ICACT.2016.7423420
16. Buinevich M., Izrailov K., Vladiko A. Metric of vulnerability at the base of the life cycle of software representations // The Proceedings of 20th International Conference on Advanced Communication Technology (ICACT, Pyeongchang, South Korea, 11–14 February 2018). IEEE, 2018. PP. 1–8. DOI:10.1109/ICACT.2018.8323940
17. Израйлов К.Е. Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах. Автореф. дис. ... канд. техн. наук. СПб.: СПбГУТ, 2017. 22 с.
18. Израйлов К.Е. Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах. Дис. ... канд. техн. наук. СПб.: СПбГУТ, 2017. 261 с.
19. Буйневич М.В., Израйлов К.Е. Аналитическое моделирование работы программного кода с уязвимостями // Вопросы кибербезопасности. 2020. № 3(37). С. 2–12. DOI:10.21681/2311-3456-2020-03-02-12
20. Монастырская В.С., Фролов В.В. Визуальный язык дракон и его применение // Актуальные проблемы авиации и космонавтики. 2016. Т. 2. № 12. С. 78–79.
21. Паронджанов В.Д. Алгоритмические языки и программирование: ДРАКОН: учебное пособие для среднего профессионального образования. Москва: Издательство Юрайт, 2023. 436 с.
22. Лапшова А.А. Разработка графического описания программного обеспечения с помощью языка UML // Теория и практика современной науки. 2018. № 6(36). С. 894–896.
23. Долидзе А.Н. Обзор специфических функций языка FBD на примере программируемых реле Logo! // Инженерный вестник Дона. 2022. № 11(95). С. 1–10.
24. Pardo M.X.C., Ferreira G.R. SFC++: A Tool for Developing Distributed Real-Time Control Software // Microprocessors and Microsystems. 1999. Vol. 23. Iss. 2. PP. 75–84. DOI:10.1016/S0141-9331(99)00015-0
25. Ахмерова А.Н. Языки программирования контроллеров. особенности применения языков FBD, LD // Научный аспект. 2019. Т. 3. № 3. С. 340–345.
26. Туренко Д.Л., Кирьянов К.Г. Исследование подходов к идентификации и восстановлению алгоритмов программ // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Радиофизика. 2004. № 1. С. 37–46.
27. Nassi I., Shneiderman B. Flowchart techniques for structured programming // SIGPLAN Notices. Vol. 8. Iss. 8. PP. 12–26. DOI:10.1145/953349.953350

28. Басов А.С. Классификация языков программирования и их особенности // Вестник науки. 2020. Т. 2. № 8(29). С. 95–101.
29. Буйневич М.В., Израйлов К.Е., Покусов В.В., Тайлаков В.А., Федulina И.Н. Интеллектуальный метод алгоритмизации машинного кода в интересах поиска в нем уязвимостей // Защита информации. Инсайд. 2020. № 5(95). С. 57–63.
30. Кизянов А.О., Глаголев В.А. Концепция универсального языка программирования // Постулат. 2022. № 1(75).
31. Морозов Д.П., Слепнев А.В. Разработка анализатора кода C, C++ на языке Python с использованием Lex, Yacc // 74-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых. Студенческая весна – 2020 (Санкт-Петербург, Россия, 26–27 мая 2020). СПб.: СПбГУТ, 2020. С. 28–32.
32. Буйневич М.В., Израйлов К.Е. Основы кибербезопасности: способы анализа программ: учебное пособие. СПб.: Санкт-Петербургский университет ГПС МЧС России, 2022. 92 с.
33. Lee W.I., Lee G. From natural language to Shell Script: A case-based reasoning system for automatic UNIX programming // Expert Systems with Applications. 1995. Vol. 9. Iss. 1. PP. 71–79. DOI:10.1016/0957-4174(94)00050-6
34. Пирогов В. Ассемблер для Windows. Санкт-Петербург: БХВ-Петербург, 2012. 896 с.
35. Капустин Д.А., Швыров В.В., Шулика Т.И. Статический анализ корпуса исходных кодов Python-приложений // Программная инженерия. 2022. Т. 13. № 8. С. 394–403. DOI:10.17587/prin.13.394-403
36. Suganuma T., Ogasawara T., Kawachiya K., Takeuchi M., Ishizaki K., Koseki A., et al. Evolution of a Java just-in-time compiler for IA-32 platforms // IBM Journal of Research and Development. 2004. Vol. 48. Iss. 5.6. PP. 767–795. DOI:10.1147/rd.485.0767
37. Кричанов М.Ю., Чепцов В.Ю. Защищенная UEFI-прошивка для виртуальных машин // Системный администратор. 2021. № 11(228). С. 75–81.
38. Макаров А.В., Скоробогатов С.Ю., Чеповский А.М. Common Intermediate Language и системное программирование в Microsoft.NET: учебное пособие. Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. 397 с.
39. Красов А.В., Шариков П.И. Методика защиты байт-кода Java-программы от декомпиляции и хищения исходного кода злоумышленником // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2017. № 1. С. 47–0.
40. Buinevich M.V., Izrailov K.E. Method and Utility for Recovering Code Algorithms of Telecommunication Devices for Vulnerability Search // Proceedings of the 16th International Conference on Advanced Communications Technology (ICACT, Pyeongchang, South Korea, 16–19 February 2014). IEEE, 2014. PP. 172–176. DOI:10.1109/ICACT.2014.6778943

References

1. Blagodarenko A.V. *Development of a Method, Algorithms and Programs for Automatic Search for Software Vulnerabilities in the Absence of Source Code*. PhD Thesis. Taganrog: Southern Federal University Publ.; 2011. 140 p. (in Russ.)
2. Markov A.S., Fadin A.A. System of vulnerabilities and security defects of software resources. *Zashita informacii. Inside*. 2013;3(51):56–61. (in Russ.)
3. Baev R.V., Skvortsov L.V., Kudriashov E.A., Buchatskii R.A., Zhuikov R.A. Prevention of vulnerabilities arising from optimization of code with undefined behavior. *Trudy ISP RAN/Proc. ISP RAS*. 2021;4(33):195–210 (in Russ.)
4. Buinevich M.V., Izrailov K.E. Anthropomorphic approach to describing the interaction of vulnerabilities in program code. Part 1. Types of interactions. *Zashita informacii. Inside*. 2019;5(89):78–85. (in Russ.)
5. Buinevich M.V., Izrailov K.E. Anthropomorphic approach to describing the interaction of vulnerabilities in program code. Part 2. Vulnerability metric. *Zashita informacii. Inside*. 2019;6(90):61–65. (in Russ.)
6. Maksimova E.A. Methods for identifying and identifying sources of destructive impacts of infrastructural genesis. *Electronic network polythematic journal "Nauchnye trudy KubGTU"*. 2022;2:86–99. (in Russ.)
7. Maksimova E.A. Axiomatics of infrastructure destruction of the subject of critical information infrastructure. *Information and Communication*. 2022;1:68–74. (in Russ.) DOI:10.34219/2078-8320-2022-13-1-68-74
8. Maksimova E.A., Buinevich M.B. The method of assessing the infrastructural stability of the subjects of critical information infrastructure. *Vestnik UrFO. Security in the Information Sphere*. 2022;1(43):50–63. (in Russ.) DOI:10.14529/secur220107
9. Maksimova E.A. *Infrastructural Destructivism of Critical Information Infrastructure Subjects*. Moscow – Volgograd: Volgograd State University Publ.; 2021. 181 p. (in Russ.)
10. Vikhrev V.V. On the mechanism for implementing the co-evolutionary model of the life cycle of developing computer programs for learning. *Systems and Means of Informatics*. 2014;24(4):168–185. (in Russ.). DOI:10.14357/08696527140411
11. Galimianov A.F., Al-Saffar N.M.F. The Software Product's Life Cycle with Large Numbers of Users: The Case of Training Programs. *Vlth International Makhmutov Readings on Problem-Based Learning in the Modern World, 12–14 April 2016, Kazan, Yelabuga, Russia*. Yelabuga: Kazan (Volga region) Federal University Publ.; 2016. p.129–133. (in Russ.)
12. Slepov V.A. Design and development of a software product "personal notepad for writing thoughts". *Scientific Review. Technical science*. 2020;4:58–63. (in Russ.)
13. Gishlakaev S.U., Minaev O.M. Basic foundations and processes of software engineering. *Proceedings of the XXVII All-Russian Scientific and Practical Conference on Digitalization of Education: Theoretical and Applied Research of Modern Science, 25th January 2021, Rostov-on-Don, Russia*. Rostov-on-Don: Southern University Publ.; VVM Publ.; 2021. Part 1. p.18–22. (in Russ.)
14. Iannone E., Guadagni R., Ferrucci F., De Lucia A., Palomba F. The Secret Life of Software Vulnerabilities: A Large-Scale Empirical Study. *IEEE Transactions on Software Engineering*. 2023;49(1):44–63. DOI:10.1109/TSE.2022.3140868
15. Buinevich M., Izrailov K., Vladyko A. The life cycle of vulnerabilities in the representations of software for telecommunication devices. *The Proceedings of 18th International Conference on Advanced Communication Technology, ICACT, 31 January–3 February 2016, Pyeongchang, South Korea*. IEEE; 2016. p.430–435. DOI:10.1109/ICACT.2016.7423420

16. Buinevich M., Izrailov K., Vladyko A. Metric of vulnerability at the base of the life cycle of software representations. *The Proceedings of 20th International Conference on Advanced Communication Technology, ICACT, 11–14 February 2018, Pyeongchang, South Korea*. IEEE; 2018. p.1–8. DOI:10.1109/ICACT.2018.8323940
17. Izrailov K.E. *Machine Code algorithmization method for searching for vulnerabilities in telecommunication devices*. PhD Thesis. St. Petersburg: The Bonch-Bruевич Saint Petersburg State University of Telecommunications Publ.; 2017. 22 p. (in Russ.)
18. Izrailov K.E. *Machine Code algorithmization method for searching for vulnerabilities in telecommunication devices*. PhD Thesis. St. Petersburg: The Bonch-Bruевич Saint Petersburg State University of Telecommunications Publ.; 2017. 22 p. (in Russ.)
19. Buinevich M., Izrailov K. Analytical modeling of the vulnerable program code execution. *Voprosy kiberbezopasnosti*. 2020;3(37):2–12. (in Russ.) DOI:10.21681/2311-3456-2020-03-02-12.
20. Monastyrnaya V.S., Frolov V.V. Visual language dragon and its application. *Aktual'nye problemy aviatsii i kosmonavтики*. 2016;2(12):78–79. (in Russ.)
21. Parondzhanov V.D. *Algorithmic Languages and Programming: DRAGON*. Moscow: Yurajt Publ.; 2023. 436 p. (in Russ.)
22. Lapshova A.A. Development of a graphic description of software using the UML language. *Teoriya i praktika sovremennoj nauki*. 2018;6(36):894–896. (in Russ.)
23. Dolidze A.N. Overview of specific functions of the FBD language using the example of Logo! *Engineering journal of Don*. 2022;11(95):1–10. (in Russ.)
24. Pardo M.X.C., Ferreira G.R. SFC++: A Tool for Developing Distributed Real-Time Control Software. *Microprocessors and Microsystems*. 1999;23(2):75–84. DOI:10.1016/S0141-9331(99)00015-0
25. Akhmerova A.N. Controller programming languages. Features of the application of the languages. *Nauchnyj aspekt*. 2019;3(3):340–345. (in Russ.)
26. Turenko D.L., Kirianov K.G. Research of approaches to identification and recovery of program algorithms. *Vestnik of Lobachevsky University of Nizhni Novgorod*. 2004;(1):37–46. (in Russ.)
27. Nassi I., Shneiderman B. Flowchart techniques for structured programming. *SIGPLAN Notices*. 8(8):12–26. DOI:10.1145/953349.953350
28. Basov A.S. Classification of programming languages and their features. *Vestnik nauki*. 2020;2(8):95–101. (in Russ.)
29. Buinevich M.V., Izrailov K.E., Pokusov V.V., Tailakov V.A., Fedulina I.N. An intelligent method of machine code algorithmization in the interests of finding vulnerabilities in it. *Zashita informacii. Inside*. 2020;5(95):57–63. (in Russ.)
30. Kizianov A.O., Glagolev V.A. Concept of a universal programming language. *Postulat*. 2022;1(75). (in Russ.)
31. Morozov D.P., Slepnev A.V. Development of C, C++ code analyzer in Python using Lex, Yacc. *Proceedings of the 74th Regional Scientific and Technical Conference of Students, Graduate Students and Young Scientists "Student Spring – 2020", 26–27 May 2020, St. Petersburg, Russia*. St. Petersburg: The Bonch-Bruевич Saint Petersburg State University of Telecommunications Publ.; 2020. p.28–32. (in Russ.)
32. Buinevich M.V., Izrailov K.E. *Cybersecurity Fundamentals: Ways to Analyze Programs*. St. Petersburg: St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia Publ.; 2022. 92 p. (in Russ.)
33. Lee W.I., Lee G. From natural language to Shell Script: A case-based reasoning system for automatic UNIX programming. *Expert Systems with Applications*. 1995;9(1):71–79. DOI:10.1016/0957-4174(94)00050-6
34. Pirogov V. *Assembler for Windows*. BHV-Petersburg Publ.; 2012. 896 p. (in Russ.)
35. Kapustin D.A., Shvyrov V.V., Shulika T.I. Static analysis of the source code of python applications. *Software Engineering*. 2022;13(8):394–403. (in Russ.) DOI:10.17587/prin.13.394-403
36. Suganuma T., Ogasawara T., Kawachiya K., Takeuchi M., Ishizaki K., Koseki A., et al. Evolution of a Java just-in-time compiler for IA-32 platforms. *IBM Journal of Research and Development*. 2004;48(5.6):767–795. DOI:10.1147/rd.485.0767
37. Krichanov M.Y., Cheptsov V.Y. Secure UEFI firmware for virtual machines. *Sistemnyj administrator*. 2021;11(228):75–81. (in Russ.)
38. Makarov A.V., Skorobogatov S.Y., Chepovskii A.M. Common Intermediate Language and system programming in Microsoft.NET. Moscow, Saratov: Internet University of Information Technologies Publ.; Ai Pi Ar Media Publ.; 2020. 397 p. (in Russ.)
39. Krasov A.V., Sharikov P.I. Methods of protection byte code java-programs from decompilation and theft of source code by an attacker. *Vestnik of St. Petersburg State University of Technology and Design. Series 1: Natural and technical Sciences*. 2017;(1):47–50. (in Russ.)
40. Buinevich M.V., Izrailov K.E. Method and Utility for Recovering Code Algorithms of Telecommunication Devices for Vulnerability Search. *Proceedings of the 16th International Conference on Advanced Communications Technology, ICACT, 16–19 February 2014, Pyeongchang, South Korea*. IEEE; 2014. p.172–176. DOI:10.1109/ICACT.2014.6778943

Статья поступила в редакцию 20.02.2023; одобрена после рецензирования 27.02.2023; принята к публикации 28.02.2023.

The article was submitted 20.02.2023; approved after reviewing 27.02.2023; accepted for publication 28.02.2023..

Информация об авторе:

ИЗРАИЛОВ
Константин Евгеньевич

кандидат технических наук, старший научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук,
 <https://orcid.org/0000-0002-9412-5693>

Научная статья

УДК 004:519.854

DOI:10.31854/1813-324X-2023-9-1-94-104



Метрики вредоносных социальных ботов

✉ **Максим Вадимович Коломеец**¹, kolomeec@comsec.spb.ru

✉ **Андрей Алексеевич Чечулин**^{1, 2}, chechulin.aa@sut.ru

¹Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, 199178, Российская Федерация

²Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация: В работе представлена параметризация вредоносных ботов с помощью метрик, которые могут быть основой для построения моделей распознавания параметров ботов и качественного анализа характеристик атак в социальных сетях. Предложен ряд метрик для описания характеристик ботов социальной сети ВКонтакте, а именно: доверие, выживаемость, цена, тип продавца, скорость и экспертное качество. Для извлечения данных метрик разработан подход, который основан на методиках контрольной закупки и теста Тьюринга. Основное преимущество данного подхода состоит в том, что он предлагает извлекать признаки из данных, полученных экспериментальным способом, и тем самым получить более обоснованную оценку в сравнении с экспертным подходом. Также работа содержит описание эксперимента по извлечению метрик вредоносных ботов социальной сети ВКонтакте с использованием предложенного подхода, и результаты анализа зависимости метрик. Эксперимент подтверждает возможность извлечения и анализа метрик. В целом, предложенные метрики и подход к их извлечению могут стать основой для перехода от бинарного обнаружения атаки в социальных сетях к качественному описанию атакующего и его возможностей, а также анализу эволюции ботов.

Ключевые слова: безопасность социальных сетей, социальные боты, социальная инженерия, метрики, дезинформация, фейковые аккаунты, анализ рисков

Источник финансирования: Исследование выполнено за счет гранта Российского научного фонда № 18-71-10094.

Ссылка для цитирования: Коломеец М.В., Чечулин А.А. Метрики вредоносных социальных ботов // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 94–104. DOI:10.31854/1813-324X-2023-9-1-94-104

Properties of Malicious Social Bots

✉ **Maxim Kolomeets**¹, kolomeec@comsec.spb.ru

✉ **Andrey Chechulin**^{1, 2}, chechulin.aa@sut.ru

¹Saint-Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, 199178, Russian Federation

²The Bonch-Bruевич Saint-Petersburg State University of Telecommunications, St. Petersburg, 193232, Russian Federation

Abstract: The paper considers the ability to describe malicious bots using their characteristics, which can be the basis for building models for recognising bot parameters and qualitatively analysing attack characteristics in social networks. The following metrics are proposed using the characteristics of VKontakte social network bots as an example: trust, survivability, price, seller type, speed, and expert quality. To extract these metrics, an approach is

proposed that is based on the methods of test purchases and the Turing test. The main advantage of this approach is that it proposes to extract features from the data obtained experimentally, thereby obtaining a more reasonable estimation than the expert approach. Also, an experiment on extracting metrics from malicious bots of the VKontakte social network using the proposed approach is described, and an analysis of the metrics' dependence is carried out. The experiment demonstrates the possibility of metrics extracting and analysis. In general, the proposed metrics and the approach to their extraction can become the basis for the transition from binary attack detection in social networks to a qualitative description of the attacker and his capabilities, as well as an analysis of the evolution of bots.

Keywords: *social media security, social bots, social engineering, metrics, disinformation, fake accounts, risk analysis*

Funding: The study was supported by the Russian Science Foundation grant No. 18-71-10094.

For citation: Kolomeets M., Chechulin A. Properties of Malicious Social Bots. *Proc. of Telecom. Universities.* 2023;9(1):94–104. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-94-104

Введение

Вредоносные боты являются одним из основных инструментов проведения атак в социальных сетях. Несмотря на существенный прогресс в развитии методик выявления и противодействия ботам, методы определения их характеристик развиты недостаточно для их практического применения. Данная работа направлена на изучение видов ботов социальных сетей, а также способах их параметризации, что также позволяет описать свойства атаки ботов в социальных сетях и возможностей атакующего. При этом, в основе исследования лежит явление возрастающей гетерогенности ботов – когда боты начинают «эволюционировать» по различным параметрам, что сказывается как на способности их детектирования, так и на возможности причинения ущерба.

Для того, чтобы успешно противодействовать таким атакам, когда используются боты различных видов, необходимо систематизировать функционал и особенности ботов в виде метрик, от которых может зависеть набор выбранных контрмер или выводы расследования уже совершенной атаки. Учитывая особенности функционирования ботов, предлагается подход к извлечению метрик ботов, который построен на двух методиках: на базе контрольной закупки и на основе теста Тьюринга. Научная новизна предложенного подхода лежит в концепции того, что вредоносные боты подлежат качественному описанию в виде метрик, которые в последствии можно использовать в системах противодействия, анализе рисков и расследованиях атак постфактум. Научная значимость состоит в предложенных методиках извлечения метрик, а практическая значимость в самих метриках, которые можно использовать в существующих системах выявления ботов.

Для поддержки результатов и выводов данной концепции, в работе также приводятся алгоритмы расчета метрик, эксперименты по расчету метрик вредоносных ботов социальной сети ВКонтакте.

Данная работа состоит из следующих разделов: второй раздел описывает контекст научной проблемы и релевантные исследования – обсуждается проблема параметризации ботов в контексте анализа и противодействия атакам в социальных сетях; в третьем разделе представлена методика на основе контрольной закупки, которая позволяет рассчитать такие метрики ботов как *цена, скорость, тип продавца, экспертное качество и выживаемость* бота; в четвертом разделе представлена методика на основе теста Тьюринга, которая позволяет рассчитать метрику *доверия* и ее вариации; в пятом разделе представлена экспериментальная часть по расчетам метрик ботов социальной сети ВКонтакте; в шестом разделе приводится анализ рассчитанных метрик и обсуждается их интерпретация; последний раздел – это заключение.

Контекст научной проблемы и релевантные исследования

В целом существует множество определений ботов, которые включают в себя *social bots, spambots, sybils, autobots, trolls*, и др. Данная несогласованность в терминологии связана с тем, что ранее под ботами понимали такие аккаунты социальных сетей, которые действуют исключительно автоматически и у которых характер взаимодействий с легитимными пользователями ограничен определенным алгоритмом, а прочие виды вредоносных аккаунтов подразделяли в отдельные виды. Постепенное усложнение [1–3] поведения ботов создало большое количество их разновидностей, которые выходят за пределы первоначального определения. В данном исследовании боты определяются как аккаунты социальных медиа, которые используют для социоинженерных атак [4]. Результатом таких атак является создание процесса, явления и отдельного события, которые не могут образоваться естественным образом. Такие аккаунты действуют не по воле человека, которого данный аккаунт представляет.

Таким образом, в данную категорию попадают:

1) взломанные аккаунты – когда злоумышленник получает доступ к чужому аккаунту и от имени предыдущего владельца осуществляет искусственные воздействия в социальной сети;

2) специально созданные аккаунты – когда злоумышленник генерирует или крадет контент, и на его основе создает фейковую идентичность, от имени которой осуществляет искусственные воздействия в социальной сети;

3) аккаунты, владельцы которых подкуплены злоумышленником – когда пользователи получают деньги или другие блага за осуществление искусственных воздействий в социальной сети.

При этом, необходимо учитывать, что не все боты вредоносны. Например, под вышеперечисленные критерии не попадают аккаунты ботов коммерческих компаний, выдуманных персонажей поп-культуры и ботов-сервисов. Данные аккаунты не несут угрозы пользователям.

Ключевыми признаками [4] вредоносности ботов является:

- сокрытие факта того, что аккаунт является ботом (вредоносные боты стремятся выдавать себя за реально существующих людей, так как доверие пользователя является одним из элементов успешности проведения атаки, в то время как невредоносные боты не стремятся обмануть пользователя);

- инициатива по отношению к пользователям (вредоносные боты первыми осуществляют взаимодействие с пользователем, в то время как невредоносные боты лишь отвечают на запросы пользователя);

- искажение естественных процессов (вредоносные боты стремятся исказить естественные либо имитировать социальные процессы, в то время как невредоносные боты предоставляют сервисы).

При этом многие исследователи отмечают явление эволюции ботов [2, 5] – когда с ростом научно-технических возможностей атакующего, возрастает сложность поведения ботов [6–7] и методов их создания [8], что в свою очередь влияет на возможности детектирования и противодействия [3, 5, 9]. Наиболее наглядно эволюция ботов проявляется в дифференциации серого рынка ботов [8, 10] – когда покупатель может выбрать ботов определенного вида из имеющихся на рынке предложений, чтобы придать атаке желаемые свойства (например, сопротивляемость ботов блокировке, большая схожесть с целевой аудиторией и др.).

Другая проблема, будучи производной особенности эволюции ботов, состоит в том, что наиболее популярным способом выявления ботов является использование методов машинного обучения с учителем [5]. Несмотря на развитие и других методов, например, машинного обучения без учителя

[11–12] или аналитической статистики [13–15], данные методы уступают в результативности [5]. При этом одной из ключевых проблем существующих методов обучения с учителем является отсутствие корректных наборов данных, на основе которых обучаются и/или тестируются разрабатываемые модели.

На основе 41 публикации [5] на тему обнаружения ботов, были выделены следующие методы разметки, которые используют исследователи.

1) Ручная разметка. Эксперт осуществляет разметку на основе своего мнения, таким образом, ее качество напрямую зависит от способности эксперта распознать бота (*англ.* True Positive Rate) и не принять реального пользователя за бота [16] (*англ.* True Negative Rate).

2) Закупка. Боты покупаются у продавца ботов, таким образом, исследователь может быть уверен в качестве разметки.

3) Аномальное поведение. Разметка осуществляется на основе формальных признаков аномального поведения аккаунтов. Качество разметки зависит от видов ботов, и от того, насколько сложное поведение они могут воспроизводить.

4) Декларация. Разметка осуществляется третьей стороной на основе другого средства обнаружения ботов. Например, исследователи могут отнести к ботам все заблокированные социальной сетью аккаунты, в таком случае разметка осуществляется функционирующей системой защиты социальной сети. Таким образом, качество разметки напрямую зависит от эффективности средства обнаружения ботов, а разрабатываемые на основе таких данных решения не смогут превысить точность используемого метода обнаружения.

Также некоторые исследователи не указывали, какой метод они использовали, или использовали свой собственный метод разметки. Также получить наборы ботов можно на основе инсайдерской информации – например, при получении доступа к отчетам продавцов ботов. Популярность того или иного метода разметки по проанализированным работам представлена на рисунке 1.

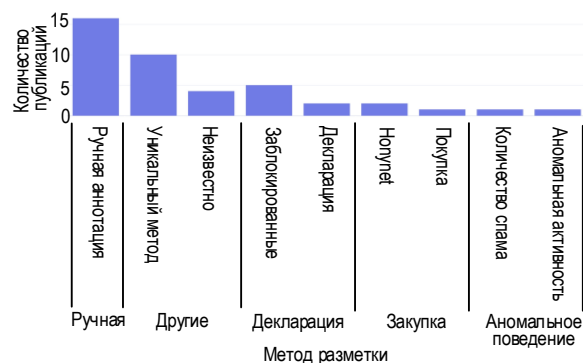


Рис. 1. Популярность методов разметки ботов

Fig. 1. The Popularity of Bot Markup Methods

Единственным надежным методом, который позволяет получить достоверную разметку (*англ.* Ground Truth Data), является метод закупки и получение меток на основе инсайдерской информации. Среди проанализированных работ метод закупки использовался один раз. Применение других методов приводит к тому, что в наборе оказываются легитимные пользователи, а некоторые виды ботов могут отсутствовать, и таким образом, модель не сможет их распознать.

Одним из путей решения вышеперечисленных проблем является переход от бинарного представления (бот/не бот) к описанию ботов, основанном на объективно извлекаемых метриках, способных описать свойства ботов. При использовании метрик становится возможным: во-первых, качественно описывать процесс эволюции ботов – как меняются метрики ботов, найденных в результате мониторинга; во-вторых, качественно описывать свойства атак – какие характеристики имеют боты, участвующих в атаке, и как это влияет на ущерб и защищенность; в-третьих, дифференцировать оценку эффективности методов обнаружения – какие виды ботов система обнаружения распознает лучше и какие – хуже.

Методика извлечения характеристик ботов на основе метода закупки

Данная методика основана на создании фейкового сообщества, для которого в контролируемых исследователем условиях закупаются боты и исключаются реальные пользователи. Таким образом становится возможным получить чистые наборы данных, гарантированно состоящие исключительно из ботов – Ground Truth Labels, а также определить метрики ботов, исходя из процесса сбора наборов данных. Данная методика состоит из 6 шагов, а сами метрики выделены полужирным курсивом.

Шаг 1. Создание списка продавцов ботов и их услуг с указанием описания набора ботов от продавца [8]. Как правило, один продавец предлагает на выбор ботов нескольких разных качеств. Список включает:

- название продавца;
- описание ботов от продавца;
- качество ботов, декларируемое продавцом (может крайне отличаться, например, «Отличное», «Ультима», «Живые», и др.);
- **экспертное качество** ботов по категориальной шкале [НИЗКОЕ, СРЕДНЕЕ, ВЫСОКОЕ], определяемой экспертом на основании описания продавца и качества декларируемым продавцом;
- **тип продавца** по шкале по категориальной шкале [МАГАЗИН, БИРЖА]; магазины – продавцы ботов, у которых можно купить вредоносную активность, исходя из предложения, биржи ботов – площадки, где размещается запрос о вредоносной

активности и любой продавец (или частный владелец аккаунта) может выполнить запрос или его часть за вознаграждение;

– вид активности (лайк, комментарий и др. – зависит от вида социальной сети);

– **цена** за единицу активности бота (количественная шкала [0, +INF] в рублях на день покупки).

Шаг 2. Создание фейкового сообщества и наполнения его контентом. Сообщество должно удовлетворять двум условиям:

– должно выглядеть настоящим, чтобы не вызывать у продавца ботов подозрений; для этого сообщество наполняется контентом (фотографии, посты, другие фейковые пользователи); некоторые продавцы ботов отказывают в услугах, если в сообществе состоит мало людей, либо у сообщества низкая активность;

– сообщество не должно быть привлекательным для реального пользователя, чтобы исключить вероятность того, что реальные пользователи проявят активность в сообществе; для этого сообщество должно обладать абсурдной / непривлекательной тематикой (например, перевозки между несуществующими городами и др.).

Шаг 3. Закупка в сообщество партии ботов (один продавец, одно качество) и сохранение идентификаторов аккаунтов, осуществивших активность с сохранением метки продавца и качества для данной партии. При закупке продавцу дается задание, например – поставить *N* лайков посту *X*. По завершении закупки также размечается **скорость** ботов, как разница во времени между моментом оплаты и завершением задачи. Скорость размечается как категориальная мера по шкале [МОМЕНТАЛЬНО, ЧАС, СУТКИ] – задание завершено:

- моментально (менее минуты);
- за несколько часов;
- за сутки и более;

Шаг 4. Удаление активности в сообществе.

Шаг 5. Повторение шага 3 для других продавцов ботов и предоставляемых ими видов аккаунтов.

Шаг 6. Ожидание некоторого времени (несколько недель или месяцев), и последующая проверка того, какое соотношение ботов из определенного набора оказалось заблокированным системами защиты социальной сети. Выражает **выживаемость** (количественная шкала [0, 1] как вероятность блокировки).

В результате формируется множество наборов данных, где каждый элемент множества представляет собой одно предложение от продавца ботов. Каждый набор данных, в свою очередь, имеет следующие идентифицирующие его свойства:

- название продавца;
- качество ботов, декларируемое продавцом.

Кроме общих свойств, каждый набор данных содержит список аккаунтов с метриками:

- id аккаунта бота;
- заблокирован ли аккаунт [ДА, НЕТ];
- вид активности: [лайк, комментарий и др.];
- **экспертное качество бота**, по категориальной шкале [НИЗКОЕ, СРЕДНЕЕ, ВЫСОКОЕ];
- **тип продавца**, по категориальной шкале [МАГАЗИН, БИРЖА];
- **цена** за единицу активности, количественная шкала [0, +INF];
- **скорость**, категориальная шкала [МОМЕНТАЛЬНО, ЧАС, СУТКИ];
- **выживаемость**, количественная шкала [0, 1].

Методика извлечения характеристик ботов на основе теста Тьюринга

Одним из свойств бота является стремление маскировать свои действия под активность реальных пользователей. От этого зависит успех атаки, так как пользователь не станет взаимодействовать с аккаунтом, если будет знать, что это бот. Например, он не будет верить отзыву о товаре, не будет передавать банковские данные, или не будет вступать в дискуссию, если известно, что собеседник – бот. Методика предлагает рассчитать метрику доверия, которая будет описывать способность человека распознавать анализируемый вид ботов. Для того, чтобы получить эту оценку, была создана методика на основе теста Тьюринга [17].

Методика основывается на разметке наборов ботов аннотаторами. За счет разницы между ответами аннотаторов и реальными лейблами можно определить способность человека распознать ботов анализируемого вида – по аналогии с тестом Тьюринга. Для того чтобы оценить эту разницу, был разработан следующий дизайн теста:

1) наборы для разметки формируются из трех наборов по X случайных пользователей:

- репрезентативных (случайные пользователи генеральной совокупности всех пользователей социальной сети);
- смещенных (пользователи, проявившие какую-либо активность: в сообществе, чате и др.);
- верифицированных (аккаунты, проверенные исследователем);

2) из Y наборов по Z случайных ботов.

Таким образом, один набор будет содержать $3 * X + Y * Z = N$ аккаунтов, среди которых необходимо обнаружить ботов. Использование трех разных наборов пользователей связано с тем, что свойства пользователей в наборе влияют на ответы аннотаторов. Например, распознать ботов среди верифицированных пользователей проще, в сравнении со случайными аккаунтами. Данные 3 набора гарантируют, что в итоговый набор попадут пользователи различной схожести с ботами и с

разной степенью социальной гомофилии [18], что соответствует основным сценариям анализа (вся социальная сеть, сообщество, близкая группа людей). Y обеспечивает ситуацию, когда всякий аннотатор разметит хотя бы по одному боту из каждого набора.

Таким образом, во-первых, итоговый набор из N аккаунтов перемешивается и подается на разметку одному аннотатору. Во-вторых, каждый ответ аннотатора сохраняется в файл с ответами с идентификатором размеченного аккаунта и одним из ответов аннотатора:

- бот (данный аккаунт является ботом);
- пользователь (аккаунт является реальным пользователем);
- я не знаю (аннотатор сомневается в ответе).

Для каждого набора можно рассчитать метрики эффективности обнаружения аннотаторами ботов определенного набора (таблица 1).

ТАБЛИЦА 1. Метрики эффективности обнаружения ботов пользователями

TABLE 1. Performance Metrics of Bot Recognition by Users

Ответ аннотатора	Тип аккаунта	Метрика
Бот распознан корректно (успех)	все аккаунты	TP
	аккаунт заблокирован	TP_Z
	аккаунт не заблокирован	TP_{NZ}
Бот распознан некорректно (провал)	все аккаунты	FN
	аккаунт заблокирован	FN_Z
	аккаунт не заблокирован	FN_{NZ}
Ответ «я не знаю»	все аккаунты	IDN
	аккаунт заблокирован	IDN_Z
	аккаунт не заблокирован	IDN_{NZ}

На основе метрик таблицы 1 можно рассчитать метрики доверия, которые описывают способность пользователя распознать бота (таблица 2).

ТАБЛИЦА 2. Метрики доверия и способы их расчета

TABLE 2. Trust Metrics and How to Calculate Them

Метрика	Формула	Обработка	
		ответов «не знаю»	заблокированных аккаунтов
$Trust$	$\frac{TP}{TP+FN}$	не учитываются	учитываются
$Trust^{IDN}$	$\frac{TP}{TP+FN+IDN}$	учитываются как провал	учитываются
$Trust_{NZ}$	$\frac{TP_{NZ}}{TP_{NZ}+FN_{NZ}}$	не учитываются	не учитываются
$Trust_{NZ}^{IDN}$	$\frac{TP_{NZ}}{TP_{NZ}+FN_{NZ}+IDN_{NZ}}$	учитываются как провал	не учитываются
$Trust_Z$	$\frac{TP+FN_Z}{TP+FN}$	не учитываются	учитываются как успех
$Trust_Z^{IDN}$	$\frac{TP+FN_Z+IDN_Z}{TP+FN+IDN}$	учитываются как провал	учитываются как успех

Примечание. В таблице: *Trust* – доверие (здесь и далее); *Trust^{IDN}* – учитывает ответы «не знаю»; *Trust^{NZ}* – учитывает только незаблокированные аккаунты; *Trust^{IDN,NZ}* – учитывает ответы «не знаю» и только незаблокированные аккаунты; *Trust_Z* – незаблокированные аккаунты считаются ботами независимо от ответа; *Trust^{IDN,NZ}_Z* – учитывает ответы «не знаю», а незаблокированные аккаунты считаются ботами независимо от ответа.

Для оценки доверия были собраны 100 000 случайных аккаунтов, которые считались как репрезентативный список пользователей. Для формирования набора смещенных пользователи были взяты аккаунты из набора ботов MKVK2021 [19], в которых содержатся пользователи, проявившие активность в одной из групп ВКонтакте. В качестве верифицированных пользователей использовались аккаунты студентов из исследования [20].

Экспериментальная проверка методик

С использованием методики контрольной закупки были собраны 65 размеченных наборов ботов от 25 компаний, предлагающих услуги активности ботов в социальной сети ВКонтакте. Экспертное качество было размечено тремя аннотаторами, исходя из описаний продавцов. Время ожидания для оценки выживаемости составило 3 месяца. В совокупности были собрано 22325 аккаунтов ботов, из которых 18444 аккаунта являются уникальными. Итоговое распределение метрик изображено на рисунке 2.

Для разметки аккаунтов аннотаторами был реализован бот в мессенджере Telegram, где можно в

удобной форме размечать аккаунты. При запуске бота, для каждого аннотатора индивидуально формировался набор из 101 аккаунта (по 12 – из репрезентативного, смещенного и верифицированного набора пользователей и по одному боту из 65 наборов) и поочередно предлагалось оставить метку для аккаунта. При завершении разметки 101 аккаунта, формировался еще один набор; таким образом аннотатор смог разместить больше 101 аккаунта. В качестве аннотаторов выступили 30 студентов СПбГУТ им. проф. М.А. Бонч-Бруевича. В результате эксперимента были получены 3168 меток. Метрики по каждому аннотатору представлены на рисунке 3, где ось X представляет скрытые имена аннотаторов.

Для расчета метрики доверия таким же образом были рассчитаны метрики эффективности обнаружения для каждого набора, которые схематично объяснены на рисунке 4.

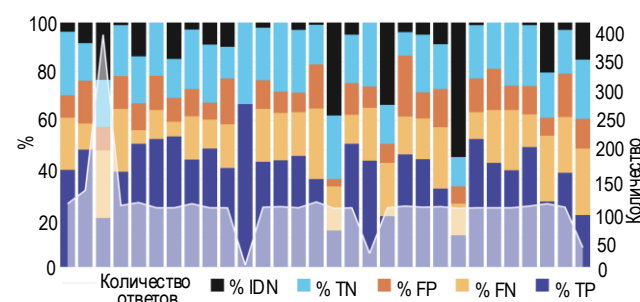


Рис. 3. Метрики эффективности обнаружения по аннотаторам

Fig. 3. Metrics of Detection Efficiency by Annotators

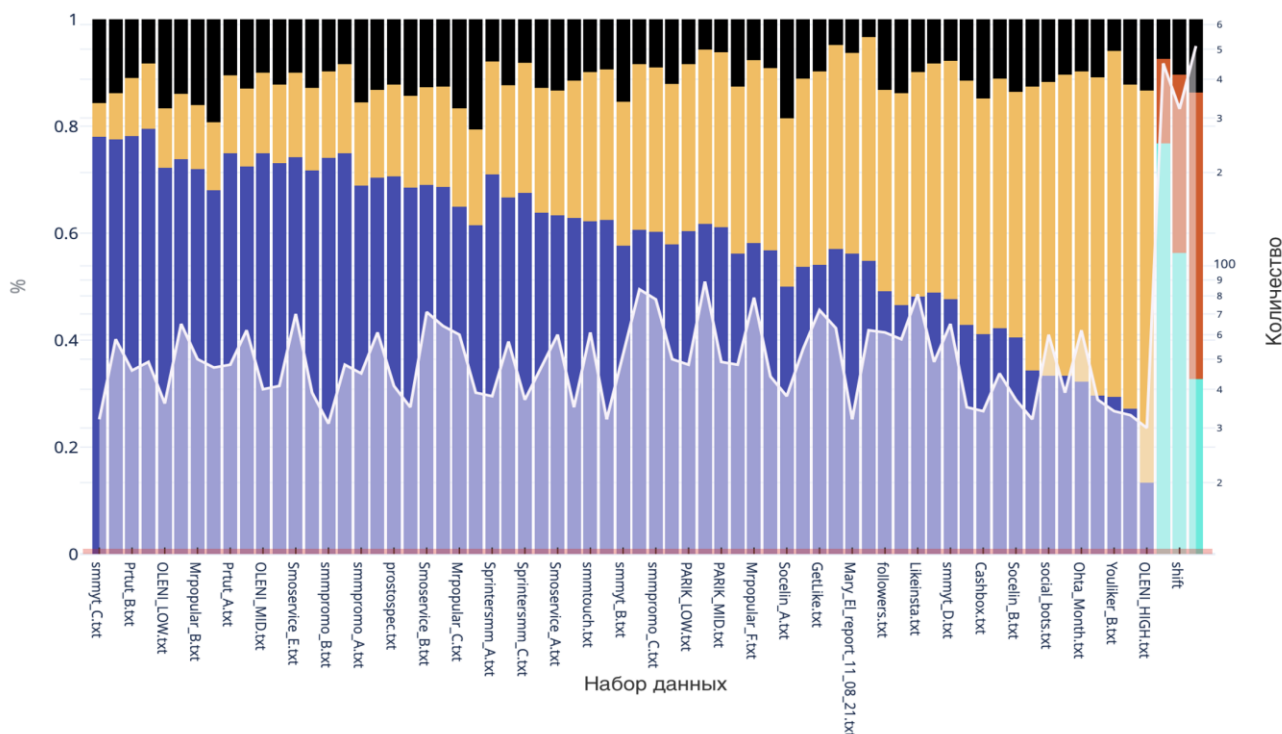


Рис. 4. Метрики эффективности обнаружения для наборов данных

Fig. 4. Metrics of Detection Efficiency for Datasets



ЭК – Экспертное качество
СК – Скорость
ТП – Тип продавца

Legend:

- $\text{Trust}^{\text{IDN}}$ (Blue line)
- $\text{Trust}^{\text{IDN7}}$ (Red line)
- $\text{Trust}^{\text{IDN7}}$ (Green line)
- $\text{Trust}^{\text{IDN7}}$ (Yellow line)
- $\text{Trust}^{\text{IDN}}$ (Black line)

☐ Средн./Час/Биржа ☐ Низкое/Мин/Магаз.

Рис. 2. Распределение метрик ботов социальной сети ВКонтакте

Fig. 2. Distribution of Bot Metrics for VKontakte Social Network

Как видно из рисунка 4, для наборов, представленных в левой части, пользователи смогли выявить около 80 % всех ботов, в то время как в правой части – ниже 30 %. Исходя из данных метрик, и были рассчитаны метрики доверия, представленные на рисунке 2.

Анализ подхода

Для того, чтобы иметь возможность характеризовать атаки, в социальных сетях был разработан ряд метрик ботов, которые можно использовать как характеристики атаки. Несмотря на их большое разнообразие, они были построены только на тех характеристиках, которые возможно однозначно извлечь из наборов данных: данные метрики рассчитываются на основе закупок ботов, экспериментов, экспертной разметки, и аннотации, произведенной в ходе сбора наборов ботов.

Метрики из таблицы 3 можно интуитивно интерпретировать следующим образом.

Доверие. Выражает качество бота с точки зрения способности человека распознать бота. Представляет собой ряд метрик, рассчитанных на основе экспериментов по выявлению ботов людьми – ответов аннотатора с учетом заблокированных аккаунтов и ответов «я не знаю». Из рисунка 2 следует, что вариации метрики доверия сильно коррелируют между собой, поэтому на практике целесообразно использовать только некоторые из них. Данная метрика наиболее хорошо характеризует вероятность успеха атаки, так как ботов с низким значением метрики жертве сложнее распознать.

Выживаемость. Доля незаблокированных аккаунтов в наборе. Выражает качество бота с точки зрения его способности противостоять блокировке средствами защиты социальной сети. Рассчитывается на основе анализа аккаунта и представляет собой процентное отношение. Данная метрика наиболее хорошо характеризует способность бота противостоять используемым на момент анализа методам обнаружения.

Цена. Стоимость бота в рублях. Выражает стоимость атаки. Рассчитывается на основе стоимости, уплаченной в результате закупки ботов. Данная метрика наиболее хорошо характеризует возможности атакующего.

Тип продавца. Выражает стратегию управления ботами [4, 8] и включает 2 значения: магазин и биржа. Боты из магазинов чаще всего управляются автоматически и создаются в автоматическом или полуавтоматическом режиме, а также не всегда могут генерировать сложный текстовый контент. Боты из биржи главным образом управляются людьми и создаются в ручном режиме, и как следствие, могут генерировать сложный текстовый контент. Данная метрика наиболее хорошо коррелирует с подходом к управлению ботами.

Скорость. Выражает скорость атаки, которая зависит от сложности поведения ботов. Автоматические боты могут совершить атаку моментально (в течение нескольких секунд), а боты, имитирующие естественное поведение, совершают атаку в течение часа или суток. Вручную управляемые боты могут совершать атаку более суток. Данная метрика наиболее хорошо характеризует маневренность атакующего и характер управления ботами.

Экспертное качество. Отражает мнение эксперта, интерпретирующего рекламное описание ботов: насколько сложным в контексте создания и управления является бот с точки зрения продавца. Данная метрика наиболее хорошо характеризует сложность технологий, используемых для создания бота или управления им.

Исходя из их нормирования экспериментальных данных по количественной шкале, что представлено в таблице 3, были также рассчитаны корреляции Спирмена между метриками ботов.

ТАБЛИЦА 3. Пример нормирования метрик ботов

TABLE 3. Bot Metrics Normalization Example

Метрика	Шкала	Интерпретация	
		Чем меньше значение	Чем больше значение
Доверие (Trust)	[0:1]	Пользователи доверяют больше	Пользователи доверяют меньше
Выживаемость	[0:1]	Вероятность блокировки ниже	Вероятность блокировки выше
Цена	[0: inf]	Дешевая атака	Дорогая атака
Тип продавца	МАГАЗИН = 0 БИРЖА = 1	Боты из магазина / вероятно, управляются алгоритмически	Боты из биржи / вероятно, управляются вручную
Скорость	МОМЕНТАЛЬНО = 0 ЧАС = 0.5 СУТКИ = 1	Быстрая атака	Медленная атака
Экспертное качество	НИЗКОЕ = 0 СРЕДНЕЕ = 0.5 ВЫСОКОЕ = 1	Боты низкого качества / простые технологии	Боты высокого качества / сложные технологии

Результаты корреляционного анализа для социальной сети ВКонтакте по состоянию на 2022 г. представлены в виде матрицы на рисунке 5, где блоками бирюзового цвета выделены наиболее значимые блоки.

Блок 1. Корреляция экспертного качества между метриками трех экспертов (e1, e2, e3). По данному блоку можно сделать вывод, что мнения экспертов плохо согласуются, и метрика все еще остается сильно субъективной.

Блок 2. Метрика доверия: чем доверие выше (больше вероятность распознать бота) – тем меньше цена, меньше экспертное качество, а сам бот,

вероятно, покупался через магазин, а не биржу. Это в целом сходится с ожидаемыми характеристиками ботов низкого качества. У метрик $Trust_{NZ}$ и $Trust_{IDN}^{IDN}$, из-за того, что при расчете отсутствуют заблокированные аккаунты, пропала корреляция со скоростью бота, что соответствует ожиданиям: автоматические боты, способные совершать быстрые атаки, чаще блокируются соцсетью.

Блок 3. Метрика выживаемости: наборы, в которых много заблокированных аккаунтов, по большей части приобретены в магазинах, а не на биржах, а боты в них обладают высокой скоростью и хорошо распознаются людьми.

Блок 4. Метрики цены, скорости и типа продавца взаимно коррелируют, за исключением корреляции цены и типа продавца.

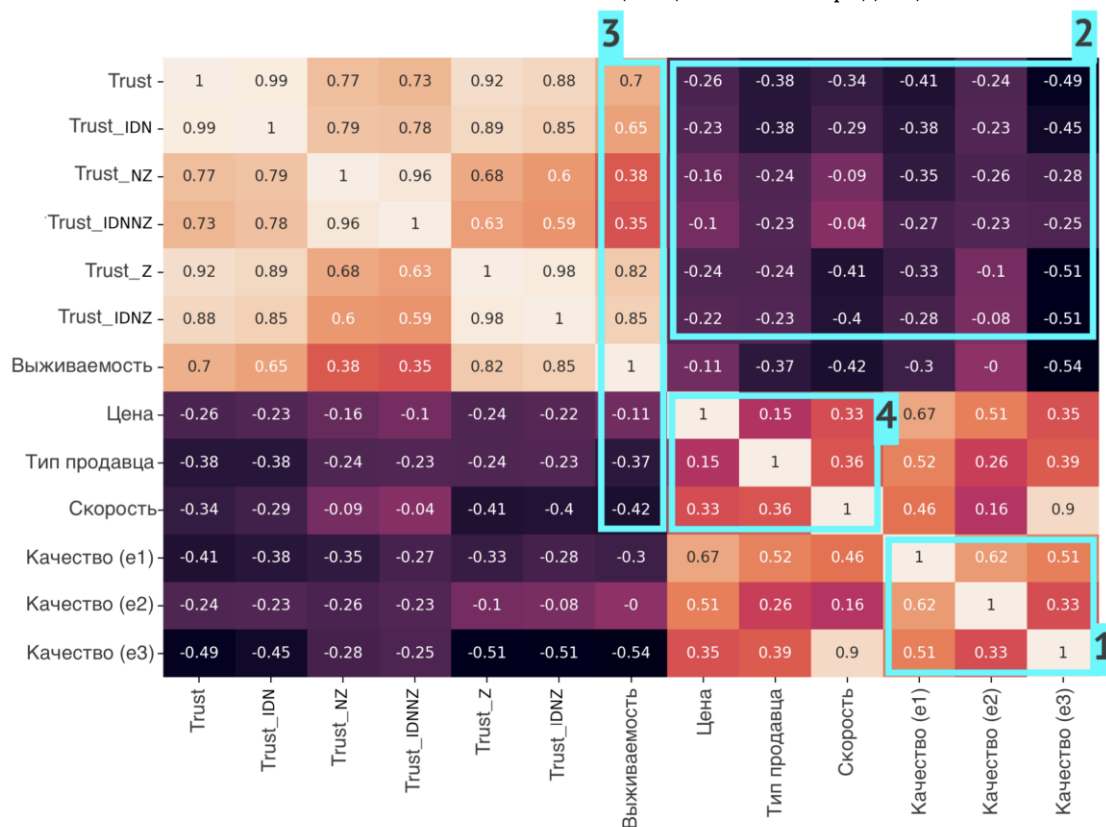


Рис. 5. Матрица корреляций метрик ботов

Fig. 5. Bot Metrics Correlation Matrix

Основной метрикой, влияющей на успешность атаки, является доверие. При этом в ходе корреляционного анализа видно, что метрика не имеет среднюю или сильную корреляцию по Чеддоку с какой-либо другой, полученной в ходе закупки ботов – ценой, скоростью и типом продавца. Сильная и средняя корреляция наблюдается между доверием и выживаемостью – это объясняется тем, что легко распознаваемые людьми боты также легко блокируются применяемыми в социальной сети ВКонтакте системами защиты. В целом можно сделать вывод, что для полноценного описания атаки нельзя обойтись какой-либо одной метрикой.

Заключение

В работе рассмотрена возможность описания вредоносных ботов с помощью следующих метрик: цена, скорость, тип продавца, экспертное качество, выживаемость и доверие. Для их извлечения предложен подход, основанный на методиках кон-

трольной закупки и теста Тьюринга. Эксперименты показали, что с их использованием можно извлечь метрики ботов, позволяющее дифференцировать вредоносные аккаунты на различные виды. Ожидается, что предложенные метрики могут стать, во-первых, основой для качественного описания процесса эволюции ботов – по аналогии с проведенным корреляционным анализом, во-вторых, качественно описывать свойства атак – какие характеристики имеют боты участвующих в атаке и как это влияет на ущерб и защищенность, и в третьих, дифференцировать оценку эффективности методов обнаружения – какие виды ботов система обнаружения распознает лучше и какие хуже.

В дальнейшей работе планируется провести дополнительные эксперименты для выявления дополнительных метрик, характеризующих ботов. Кроме того, планируется использование полученных результатов для выявления каналов, формируемых ботами для распространения информации [21].

Список источников

1. Cresci S. A decade of social bot detection // *Communications of the ACM*. 2020. Vol. 63. Iss. 10. PP. 72–83. DOI:10.1145/3409116
2. Ferrara E., Varol O., Davis C., Menczer F., Flammini A. The rise of social bots // *Communications of the ACM*. 2016. Vol. 59. Iss. 7. PP. 96–104. DOI:10.1145/2818717
3. Yang C., Harkreader R., Gu, G. Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers // *IEEE Transactions on Information Forensics and Security*. 2013. Vol. 8. Iss. 8. PP. 1280–1293. DOI:10.1109/TIFS.2013.2267732
4. Vitkova L. Kolomeec M., Chechulin A. Taxonomy and Bot Threats in Social Networks // *Proceedings of the International Russian Automation Conference (RusAutoCon, Sochi, Russia, 04–10 September 2022)*. IEEE, 2022. PP. 814–819. DOI:10.1109/RusAutoCon54946.2022.9896268
5. Orabi M., Mouheb D., Al Aghbari Z., Kamel I. Detection of Bots in Social Media: A Systematic Review // *Information Processing & Management*. 2020. Vol 57. Iss. 4. P. 102250. DOI:10.1016/j.ipm.2020.102250
6. Varol O., Ferrara E., Davis C., Menczer F., Flammini A. Online Human-Bot Interactions: Detection, Estimation, and Characterization // *Proceedings of the 11th International AAAI Conference on Web and Social Media*. 2017. Vol. 11. Iss. 1. PP. 280–289. DOI:10.1609/icwsm.v11i1.14871
7. Stieglitz S., Brachten F., Berthel'e D., Schlaus M., Venetopoulou C., Veutgen D. Do Social Bots (Still) Act Different to Humans? – Comparing Metrics of Social Bots with those of Humans // *Proceedings of the 9th International Conference on Social Computing and Social Media. Human Behavior (SCSM 2017, Vancouver, Canada, 9–14 July 2017)*. Lecture Notes in Computer Science. Vol. 10282. Cham: Springer, 2017. PP. 379–395. DOI:10.1007/978-3-319-58559-8_30
8. Kolomeets M., Chechulin A. Analysis of the Malicious Bots Market // *Proceedings of the 29th Conference of Open Innovations Association (FRUCT, Tampere, Finland, 12–14 May 2021)*. IEEE, 2021. PP. 199–205. DOI:10.23919/FRUCT52173.2021.9435421
9. Perdana R.S., Muliawati T.H., Alexandro R. Bot spammer detection in twitter using tweet similarity and time interval entropy // *Jurnal Ilmu Komputer dan Informasi*. 2015. Vol. 8. Iss. 1. PP. 19–25. DOI:10.21609/jiki.v8i1.280
10. The Black Market for Social Media Manipulation. Riga: NATO StratCom COE, 2018.
11. Chavoshi N., Hamooni H., Mueen A. DeBot: Twitter Bot Detection via Warped Correlation // *Proceedings of the 16th International Conference on Data Mining (ICDM, Barcelona, Spain, 12–15 December 2016)*. IEEE, 2016. PP. 817–822. DOI:10.1109/ICDM.2016.0096
12. Dorri A., Abadi M., Dadfarnia M. SocialBotHunter: Botnet Detection in Twitter-Like Social Networking Services Using Semi-Supervised Collective Classification // *Proceedings of the 16th International Conference on Dependable, Autonomic and Secure Computing, 16th International Conference on Pervasive Intelligence and Computing, 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech, Athens, Greece, 12–15 August 2018)*. IEEE, 2018. PP. 496–503. DOI:10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00097
13. Vitkova L., Kotenko I., Kolomeets M., Tushkanova O., Chechulin A. Hybrid Approach for Bots Detection in Social Networks Based on Topological, Textual and Statistical Features // *Proceedings of the Fourth International Scientific Conference Intelligent Information Technologies for Industry (ITI'19, Ostrava – Prague, Czech Republic, 2–7 December 2019)*. *Advances in Intelligent Systems and Computing*. Vol. 1156. Cham: Springer, 2020. PP. 412–421. DOI:10.1007/978-3-030-50097-9_42
14. García-Orosa B., Gamallo P., Martín-Rodilla P., Martínez-Castaño R. Hybrid Intelligence Strategies for Identifying, Classifying and Analyzing Political Bots // *Social Sciences*. 2021. Vol. 10. Iss. 10. P. 357. DOI:10.3390/socsci10100357
15. Yang K.C., Hui P.M., Menczer F. Bot Electioneering Volume: Visualizing Social Bot Activity During Elections // *Companion Proceedings of The 2019 World Wide Web Conference (WWW '19, San Francisco, USA, 13–17 May 2019)*. New York: Association for Computing Machinery, 2019. PP. 214–217. DOI:10.1145/3308560.3316499
16. Adrian R., Kaiser J. The False positive problem of automatic bot detection in social science research // *PLoS ONE*. 2020. Vol. 15. Iss. 10. P. e0241045. DOI:10.1371/journal.pone.0241045
17. Boneh D., Grotto A.J., McDaniel P., Papernot N. How Relevant is the Turing Test in the Age of Sophisbots? // *IEEE Security & Privacy*. 2019. Vol. 17. Iss. 6. PP. 64–71. DOI:10.1109/MSEC.2019.2934193
18. Aiello L.M., Barrat A., Schifanella R., Cattuto C., Markines B., Menczer F. Friendship prediction and homophily in social media // *ACM Transactions on the Web*. 2012. Vol. 6. Iss. 2. PP. 1–33. DOI:10.1145/2180861.2180866
19. Kolomeets M. Security Datasets – MKVK2021. URL: <https://github.com/guardeec/datasets#mkvk2021> (дата обращения 28.02.2023)
20. Branitskiy A., Levshun D., Krasilnikova N., Doynikova E., Kotenko I., Tishkov A., Vanchakova N., Chechulin A. Determination of Young Generation's Sensitivity to the Destructive Stimuli based on the Information in Social Networks // *Journal of Internet Services and Information Security*. 2019. Vol. 9. Iss. 3. PP. 1–20.
21. Проноза А.А., Виткова Л.А., Чечулин А.А., Котенко И.В., Сахаров Д.В. Методика выявления каналов распространения информации в социальных сетях // *Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления*. 2018. Т.14. № 4. С. 362–377. DOI:10.21638/11702/spbu10.2018.409.

References

1. Cresci S. A decade of social bot detection. *Communications of the ACM*. 2020;63(10):72–83. DOI:10.1145/ 3409116
2. Ferrara E., Varol O., Davis C., Menczer F., Flammini A. The rise of social bots. *Communications of the ACM*. 2016;59(7): 96–104. DOI:10.1145/2818717
3. Yang C., Harkreader R., Gu G. Empirical evaluation and new design for fighting evolving twitter spammers. *IEEE Transactions on Information Forensics and Security*. 2013;8(8):1280–1293. DOI:10.1109/TIFS.2013.2267732
4. Vitkova L. Kolomeec M., Chechulin A. Taxonomy and Bot Threats in Social Networks. *Proceedings of the International*

Russian Automation Conference, RusAutoCon, 04–10 September 2022, Sochi, Russia. IEEE; 2022. p.814–819. DOI:10.1109/RusAutoCon54946.2022.9896268

5. Orabi M., Mouheb D., Al Aghbari Z., Kamel I. Detection of bots in social media: a systematic review. *Information Processing & Management*. 2020;57(4):102250. DOI:10.1016/j.ipm.2020.102250

6. Varol O., Ferrara E., Davis C., Menczer F., Flammini A. Online Human-Bot Interactions: Detection, Estimation, and Characterization. *Proceedings of the 11th International AAAI Conference on Web and Social Media*. 2017;11(1):280–289. DOI:10.1609/icwsm.v11i1.14871

7. Stieglitz S., Brachten F., Berthel'e D., Schlaus M., Venetopoulou C., Veutgen D. Do Social Bots (Still) Act Different to Humans? – Comparing Metrics of Social Bots with those of Humans. *Proceedings of the 9th International Conference on Social Computing and Social Media. Human Behavior, SCSM 2017, 9–14 July 2017, Vancouver, Canada. Lecture Notes in Computer Science*. vol.10282. Cham: Springer; 2017. p.379–395. DOI:10.1007/978-3-319-58559-8_30

8. Kolomeets M., Chechulin A. Analysis of the Malicious Bots Market. *Proceedings of the 29th Conference of Open Innovations Association, FRUCT, 12–14 May 2021, Tampere, Finland*. IEEE; 2021. p.199–205. DOI:10.23919/FRUCT52173.2021.9435421

9. Perdana R.S., Muliawati T.H., Alexandro R. Bot spammer detection in twitter using tweet similarity and time interval entropy. *Jurnal Ilmu Komputer dan Informasi*. 2015;8(1):19–25. DOI:10.21609/jiki.v8i1.280

10. *The Black Market for Social Media Manipulation*. Riga: NATO StratCom COE; 2018.

11. Chavoshi N., Hamooni H., Mueen A. DeBot: Twitter Bot Detection via Warped Correlation. *Proceedings of the 16th International Conference on Data Mining, ICDM, 12–15 December 2016, Barcelona, Spain*. IEEE; 2016. p.817–822. DOI:10.1109/ICDM.2016.0096

12. Dorri A., Abadi M., Dadfarnia M. SocialBotHunter: Botnet Detection in Twitter-Like Social Networking Services Using Semi-Supervised Collective Classification. *Proceedings of the 16th International Conference on Dependable, Autonomic and Secure Computing, 16th International Conference on Pervasive Intelligence and Computing, 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech, 12–15 August 2018, Athens, Greece*. IEEE; 2018. p.496–503. DOI:10.1109/DASC/PiCom/DataCom/CyberSciTech.2018.00097

13. Vitkova L., Kotenko I., Kolomeets M., Tushkanova O., Chechulin A. Hybrid Approach for Bots Detection in Social Networks Based on Topological, Textual and Statistical Features. *Proceedings of the Fourth International Scientific Conference Intelligent Information Technologies for Industry, IITI'19, 2–7 December 2019, Ostrava – Prague, Czech Republic. Advances in Intelligent Systems and Computing*. vol.1156. Cham: Springer; 2020. p.412–421. DOI:10.1007/978-3-030-50097-9_42

14. García-Orosa B., Gamallo P., Martín-Rodilla P., Martínez-Castaño R. Hybrid Intelligence Strategies for Identifying, Classifying and Analyzing Political Bots. *Social Sciences*. 2021;10(10):357. DOI:10.3390/socsci10100357

15. Yang K.C., Hui P.M., Menczer F. Bot Electioneering Volume: Visualizing Social Bot Activity During Elections. *Companion Proceedings of The 2019 World Wide Web Conference, WWW '19, 13–17 May 2019, San Francisco, USA*. New York: Association for Computing Machinery; 2019. p.214–217. DOI:10.1145/3308560.3316499

16. Adrian R., Kaiser J. The False positive problem of automatic bot detection in social science research. *PLoS ONE*. 2020;15(10):e0241045. DOI:10.1371/journal.pone.0241045

17. Boneh D., Grotto A.J., McDaniel P., Papernot N. How Relevant is the Turing Test in the Age of Sophisbots? *IEEE Security & Privacy*. 2019;17(6):64–71. DOI:10.1109/MSEC.2019.2934193

18. Aiello L.M., Barrat A., Schifanella R., Cattuto C., Markines B., Menczer F. Friendship prediction and homophily in social media. *ACM Transactions on the Web*. 2012;6(2):1–33. DOI:10.1145/2180861.2180866

19. Kolomeets M. *Security Datasets – MKVK2021*. URL: <https://github.com/guardeec/datasets#mkvk2021> [Accessed 28th February 2023]

20. Branitskiy A., Levshun D., Krasilnikova N., Doynikova E., Kotenko I., Tishkov A., Vanchakova N., Chechulin A. Determination of Young Generation's Sensitivity to the Destructive Stimuli based on the Information in Social Networks. *Journal of Internet Services and Information Security*. 2019;9(3):1–20.

21. Pronoza A.A., Vitkova L.A., Chechulin A.A., Kotenko I.V., Saharov D.V. Methodology for disseminating information channels analysis in social networks. *Vestnik of Saint-Petersburg University applied mathematics. Computer science. Control processes*. 2018;14(4):362–377. (In Russ). DOI:10.21638/11702/spbu10.2018.409

Статья поступила в редакцию 06.02.2023; одобрена после рецензирования 14.02.2023; принята к публикации 15.02.2023.

The article was submitted 06.02.2023; approved after reviewing 14.02.2023; accepted for publication 15.02.2023.

Информация об авторах:

КОЛОМЕЕЦ
Максим Вадимович

старший научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук,
 <https://orcid.org/0000-0002-7873-2733>

ЧЕЧУЛИН
Андрей Алексеевич

кандидат технических наук, ведущий научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
 <https://orcid.org/0000-0001-7056-6972>

Научная статья

УДК 004.056

DOI:10.31854/1813-324X-2023-9-1-105-115



Иерархическая модель для проектирования систем на основе микроконтроллеров защищенными от киберфизических атак

Дмитрий Сергеевич Левшун, levshun@comsec.spb.ru

¹Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, 199178, Российская Федерация

Аннотация: В статье предложена иерархическая модель для проектирования систем на основе микроконтроллеров защищенными от киберфизических атак. В рамках данной модели система на основе микроконтроллеров представляется в виде иерархического реляционного множества взаимодействующих блоков с различными свойствами и связями между ними. Предложенная модель включает в себя модели аппаратных, программных и программно-аппаратных элементов, интерфейсов, протоколов и связей между элементами системы на различных ее уровнях, модели атакующего и атакующих действий. Ключевое отличие разработанной модели заключается в возможности представления систем на основе микроконтроллеров в целом, что позволяет нивелировать основной недостаток аналогов – проектирование систем на основе микроконтроллеров без учета взаимодействия их устройств друг с другом. Кроме того, разработанная модель является модульной и расширяемой, направлена на обеспечение защищенности проектируемого решения от киберфизических атак, а также рассматривает элементы защиты как неотъемлемую часть спроектированной системы.

Ключевые слова: информационная безопасность, проектирование защищенных систем, система на основе микроконтроллеров, теоретико-множественная модель, киберфизическая атака, иерархическая модель

Источник финансирования: Исследование выполнено за счет гранта Российского Научного Фонда № 22-71-00107, <https://rscf.ru/project/22-71-00107>.

Ссылка для цитирования: Левшун Д.С. Иерархическая модель для проектирования систем на основе микроконтроллеров защищенными от киберфизических атак // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 105–115. DOI:10.31854/1813-324X-2023-9-1-105-115

Hierarchical Model for the Design of Microcontroller-Based Systems Protected from Cyber-Physical Attacks

Dmitry Levshun, levshun@comsec.spb.ru

¹Saint-Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, 199178, Russian Federation

Abstract: The article proposes a hierarchical model for the design of microcontroller-based systems protected from cyber-physical attacks. Within the framework of this model, a microcontroller-based system is represented as a hierarchical relational set of interacting building blocks with different properties and links between them. The proposed model includes models of hardware, software and hardware-software elements, interfaces, protocols and

links between system elements, models of attacker and attack actions. The key difference of the developed model lies in the possibility of full representation of microcontroller-based systems, while other solutions have a drawback of designing such systems without taking into account the interactions of their devices with each other and other systems. In addition, the developed model is modular and extensible, aims to ensure the security of the designed solution from cyber-physical attacks, and considers security elements as an integral part of the final solution.

Keywords: *information security, secure by design, microcontroller-based system, set-theoretic approach, cyber-physical attack, hierarchical model*

Funding: The study was supported by the grant of the Russian Science Foundation No. 22-71-00107, <https://rscf.ru/en/project/22-71-00107>.

For citation: Levshun D. Hierarchical Model for the Design of Microcontroller-Based Systems Protected from Cyber-Physical Attacks. *Proc. of Telecom. Universities*. 2023;9(1):105–115. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-105-115

1. Введение

В настоящее время системы на основе микроконтроллеров – неотъемлемая часть любой сферы жизнедеятельности человека, что обуславливает критическую важность обеспечения их защищенности [1]. Последствия отказа подобных систем, в том числе связанные с деятельностью злоумышленников, включают в себя как финансовый и репутационный ущерб, так и угрозу жизни и здоровью человека. Одним из возможных направлений атаки является использование уязвимостей, наличие которых в подобных системах обусловлено различными факторами.

Уязвимости, возникающие из-за ошибок на этапе проектирования, являются наиболее опасными, т. к. их устранение, как правило, представляет собой трудно решаемую задачу [2]. Особенно когда устранение ошибки подразумевает изменения в аппаратной или программной составляющих отдельных устройств, в то время как их фирм-производителей уже не существует. Распространенность таких уязвимостей связана с тем, что системы на основе микроконтроллеров зачастую проектируются без участия специалистов в области информационной безопасности с применением слабозащищенных протоколов передачи данных, выходом в сеть Интернет и использованием непроверенного на наличие ошибок кода [3].

Например, согласно отчету компании SonicWall, количество атак с помощью устройств на основе микроконтроллеров подскочило на 215,7 %: до 32,7 миллионов в 2018 г. (по сравнению с 10,3 миллионами в 2017 г.). В 2019 г. атаки продолжились, но, согласно отчету данной компании, их количество увеличились только на 5 %. Также, согласно отчету «Unit 42 Threat Report» компании Palo Alto Networks за 2020 г., «98 % трафика устройств не зашифровано, что открывает нарушителям доступ к личным и конфиденциальным данным их пользователей».

Решение данной проблемы является важной задачей, именно поэтому были разработаны и при-

меняются на практике различные методики проектирования [4]. При этом одним из ключевых элементов любого подхода к проектированию систем на основе микроконтроллеров является используемая в них модель системы.

В отличие от существующих решений, предлагаемая в данной работе расширяемая иерархическая, основанная на множествах, реляционная модель позволяет описывать системы на основе микроконтроллеров, а не отдельные устройства данных систем. Данная особенность позволяет нивелировать один из недостатков аналогов – проектирование устройств на основе микроконтроллеров без учета их взаимодействия друг с другом.

Кроме того, разработанная модель, будучи модульной, расширяемой и иерархической, направлена на обеспечение защищенности проектируемого решения, а также рассматривает элементы защиты как неотъемлемую часть проектируемой системы. Расширение данной модели возможно за счет введения новых уровней абстракции. Модульность решения позволяет изменять отдельные части модели без необходимости полной ее переработки. Например, могут быть изменены параметры модели злоумышленника или анализируемые классы атакующих действий. Иерархический характер решения позволяет осуществлять прямые (от всей системы к отдельным элементам) и обратные (от отдельного элемента к системе в целом) переходы в рамках модели.

Статья организована следующим образом. В разделе 2 проанализированы существующие решения в области моделирования систем на основе микроконтроллеров. В разделе 3 предложена новая иерархическая модель для проектирования систем на основе микроконтроллеров защищенными от киберфизических атак. В разделе 4 показаны взаимосвязи между элементами представленной модели. В разделе 5 показаны достоинства, недостатки и область применения предложенной модели. В разделе 6 содержатся основные выводы и направления дальнейших исследований.

2. Анализ существующих решений

В современных исследованиях, для отображения различных аспектов сложных систем и анализа возможности реализации различных атакующих действий используется компонентное [5–7], полунатурное [8–10], имитационное [11–13] и аналитическое [14–16] моделирование. При этом каждый подход к моделированию имеет свой уровень полноты и детализации, а также назначение при представлении системы (таблица 1).

ТАБЛИЦА 1. Сравнение подходов к моделированию

TABLE 1. Comparison of Modeling Approaches

Полнота	Уровень детализации	Подход к моделированию	Атаки
↑	↓	Аналитическая	Многошаговые на систему в целом
		Имитационная	Затрагивающие ряд устройств системы
		Полунатурная	Затрагивающие отдельные устройства системы
		Компонентная	Затрагивающие отдельные элементы системы

Компонентная модель является наиболее подробным способом представления систем на основе микроконтроллеров, однако требует много времени и усилий для описания больших систем. Более того, с помощью данной модели невозможно представить различные динамические процессы. С другой стороны, с помощью аналитического моделирования можно достаточно быстро представить систему целиком, однако уровень детализации будет совершенно иным. Рассмотрим несколько примеров работ.

Модель для проектирования отказоустойчивых систем на основе микроконтроллеров представлена в [17]. По мнению авторов, устойчивая система обладает тремя основными характеристиками: стабильность, защищенность и системность. Стабильность означает, что система на основе микроконтроллеров со временем всегда достигает предсказуемого состояния. Защищенность означает, что разработанная система способна обнаруживать киберфизические атаки и противодействовать им. Системность означает, что программные и аппаратные элементы системы интегрированы вместе. При этом модель, предложенная авторами, включает шесть уровней: 1) восприятие; 2) обработка; 3) анализ; 4) объединение решений; 5) оператор и его взаимодействие с системой. Для достижения системой состояния отказоустойчивости, необходимо обеспечить следующие характеристики: надежность, безотказность, согласованность, совместимость и интегрированность.

Возможность расширения мехатронных систем до киберфизических проанализированы в работе [18]. Авторы рассмотрели общие черты таких

систем и подчеркнули возрастающую роль киберфизических систем в производственном секторе. Кроме того, авторы представили ключевые сложности в процессе проектирования таких систем, а именно необходимость комплексного и масштабируемого подхода. Данный подход необходим для предотвращения междисциплинарных конфликтов в процессе разработки киберфизических систем. При этом описание требования масштабируемости дано на основе внешних и внутренних взаимодействий, управления процессами, моделирования поведения, топологических отношений и функциональной совместимости. Предлагаемый авторами подход к проектированию включает семь основных этапов, а именно: определение границ системы, многоуровневое моделирование, моделирование взаимодействий, топологическое моделирование, семантическое взаимодействие, мультиагентное моделирование и моделирование взаимодействий. В качестве примера авторы использовали процесс изготовления планшетов.

В [19] авторы определили требования к защищенному, надежному и отказоустойчивому контроллеру SDN (аббр. от англ. Software-Defined Network [20]). Была проанализирована архитектура контроллеров этого типа, даны рекомендации по улучшению их защищенности. При этом атрибуты защищенности были разделены на три основные группы: архитектура, интерфейсы и сервисы. С точки зрения архитектуры, авторами были проверены следующие функциональные особенности: уровень изоляции процессов управления (приложения), способы разрешения конфликтов политик безопасности, использование защищенного хранилища данных, дублирование элементов контроллеров, надежность приложений.

Подход для проектирования систем шифрования и дешифрования видео в режиме реального времени предложен в [21]. Авторы также разработали и протестировали аппаратную реализацию системы. При этом параметры защищенности были протестированы на основе критериев Национального института стандартов и технологий (NIST, аббр. от англ. National Institute of Standards and Technology [22]). Основываясь на теоретическом анализе и экспериментальных результатах, авторы пришли к выводу о целесообразности применения разработанного подхода для проектирования и разработки новых защищенных систем видеосвязи.

Модель для проектирования защищенных и эффективных с точки зрения ресурсопотребления устройств на основе микроконтроллеров представлена в работе [23]. В ней авторы предложили подход к объединению отдельных алгоритмов и методик, реализующих разные функции средств

обеспечения информационной безопасности. При этом разработанные авторами модель и подход предлагается использовать как часть процесса проектирования систем на основе микроконтроллеров. В основе моделирования устройств лежит MARTE – UML-профиль для моделирования и анализа систем реального времени [24]. Данный профиль состоит из следующих частей:

- необработанные данные (спецификация устройства на основе микроконтроллеров, описание элементов безопасности);
- входные данные, извлеченные из необработанных данных (функциональные и нефункциональные свойства, модели злоумышленников и угроз, требования к защищенности, необходимые ресурсы и совместимость устройств);
- функции процесса конфигурации (фильтрация, проверка, анализ совместимости и компоновка на основе критериальной оптимизации).

Методика анализа защищенности сетевых информационных потоков в системах на основе микроконтроллеров представлена в [25]. По мнению авторов, основная проблема обеспечения защищенности систем такого типа заключается в их работе в потенциально враждебной среде, в то время как их вычислительные возможности сильно ограничены. При этом для анализа защищенности предлагается моделирование данных потоков на следующих основных уровнях: уровень электронных схем (аппаратные потоки); уровень прошивок, операционных систем и приложений (программные потоки); а также уровень взаимодействия устройств (сетевые потоки). При этом предлагаемая методика состоит из двух основных элементов: топологического анализа и анализа информационных потоков на основе политик безопасности. Топологический подход основан на выявлении всех элементов систем, лежащих между двумя узлами графа – источником и получателем данных. Подход на основе политик использует правила фильтрации трафика, конфигурацию сети и описание аномалий для обнаружения конфликтов в политиках безопасности. Данная методика была разработана в рамках проекта SecFutur [26].

Проведенный анализ позволяет отметить следующие недостатки существующих решений для моделирования и проектирования защищенных систем на основе микроконтроллеров:

- 1) учитываются только отдельные аспекты обеспечения защищенности систем на основе микроконтроллеров;
- 2) не рассматриваются сильные зависимости между программным и аппаратным обеспечением устройств на основе микроконтроллеров;
- 3) устройства на основе микроконтроллеров проектируются без учета параметров системы, элементов которой они являются;

4) защищенная связь между устройствами обеспечивается только внутри системы на основе микроконтроллеров, в то время как взаимодействие данных устройств с внешними системами не рассматривается.

Это означает, что единый подход к моделированию систем на основе микроконтроллеров для решения задачи их проектирования защищенными от киберфизических атак еще не сформирован и активно исследуется. В следующем разделе данной работы предложена оригинальная иерархическая модель, в рамках которой системы на основе микроконтроллеров представляются в виде иерархического реляционного множества взаимодействующих блоков с различными свойствами и связями между ними.

3. Системы на основе микроконтроллеров

В данной работе для представления систем на основе микроконтроллеров используется разделение их элементов на *компоненты*, *контроллеры* и *устройства*, взаимодействующие друг с другом (рисунк 1).

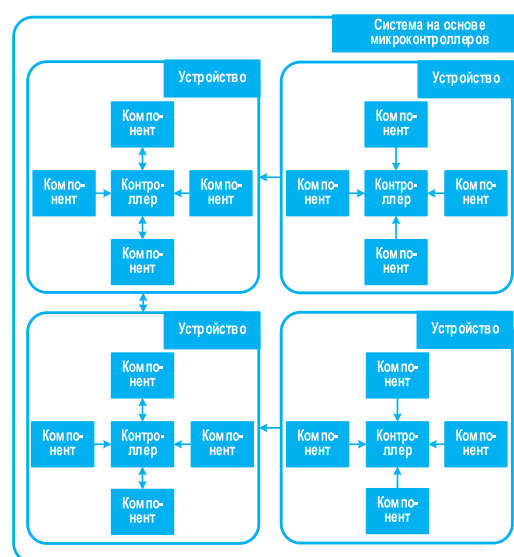


Рис. 1. Представление систем на основе микроконтроллеров

Fig. 1. Architecture of Microcontroller-Based Systems

Рассмотрим каждый тип элемента более подробно, для чего дадим их определения.

Компонент – это то, что возможно подключить к контроллеру для отправки данных на него, либо получения данных от него и последующей реакции. *Компоненты* могут обмениваться данными только с теми *контроллерами*, к которым они подключены. *Компоненты* могут быть представлены в виде различных датчиков, приемников, передатчиков, считывателей, двигателей и т. д. Важно отметить, что в данном представлении рассматриваются только готовые компоненты, без учета составляющих электронных схем, например, резисторов, конденсаторов, транзисторов, диодов и др.

Контроллер – это то, что можно запрограммировать для работы с *компонентами* и другими *контроллерами*. *Контроллеры* могут обмениваться данными с *компонентами* и другими *контроллерами*, которые к ним подключены. *Контроллеры* могут быть представлены в виде различных микроконтроллеров и одноплатных компьютеров.

Устройство – это то, что представляет собой совокупность *контроллеров* и *компонентов*, взаимодействующих друг с другом для решения определенных задач. *Устройства* могут взаимодействовать только с другими *устройствами*. *Устройства* могут быть представлены в виде серверов, роботов, станций, дронов, терминалов и т. д.

Подобное представление позволяет в начале проектировать системы на основе микроконтроллеров на уровне устройств, а затем отдельно рассмотреть их внутреннюю структуру. При этом внутри каждого устройства возможно в начале смоделировать взаимосвязи между контроллерами и только после этого рассматривать связь между контроллерами и компонентами.

Допустимы следующие среды передачи данных: *контроллер* ↔ *компонент*, *контроллер* ↔ *контроллер*, *устройство* ↔ *устройство*, *система* ↔ *система*.

4. Иерархическая модель

Для моделирования систем на основе микроконтроллеров защищенными от киберфизических атак был выбран компонентный подход, как наиболее подходящий для учета требований к защищенности системы на ранних стадиях ее жизненного цикла. Модель, предложенная в данном разделе, представляет системы на основе микроконтроллеров в качестве расширяемой иерархической реляционной структуры на основе множеств. При этом для описания модели был использован теоретико-множественный подход. Рассмотрим данное представление более подробно.

Любая система на основе микроконтроллеров $mbs \in MBS$ может быть представлена как:

$$mbs = (MBS', BB, L_{mbs}, a, AA, p_{mbs}),$$

где MBS' – множество подсистем на основе микроконтроллеров системы mbs ; BB – блоков системы; L_{mbs} – связей между BB и MBS' системы; a – злоумышленник, атакующий систему; AA – атакующих действий, которые могут быть направлены на систему; p_{mbs} – свойства системы.

В качестве примера mbs могут быть использованы такие системы, как система контроля и управления доступом, система пожарной и/или охранной сигнализации, система видеонаблюдения, система контроля периметра и т. д. При этом ситуация, когда mbs содержит MBS' , относится к интегрированным системам, объединяющим,

например, контроль доступа с системами пожарной и охранной сигнализации.

Блок системы mbs может быть представлен следующим образом:

$$bb = (BB', HW, SW, L_{bb}, p_{bb}),$$

где BB' – множество подблоков блока bb ; HW – аппаратных элементов блока bb ; SW – программных элементов блока bb ; L_{bb} – связей между программными и аппаратными элементами блока bb ; p_{bb} – свойства блока bb .

В качестве примера bb могут быть использованы контроллеры, а также их комбинации с различными компонентами. Это может быть одноплатный компьютер Raspberry Pi, microSD карта памяти с предустановленной операционной системой, микроконтроллер ESP8266 или Iskra JS, а также полноценные устройства – сервер, хаб, робот, станция, дрон и т. п.

Аппаратный элемент системы mbs может быть представлен следующим образом:

$$hw = (HW', L_{hw}, p_{hw}),$$

где HW' – множество аппаратных подэлементов аппаратного элемента hw ; L_{hw} – связей между элементами hw ; p_{hw} – свойства аппаратного элемента hw . В качестве примера hw могут быть использованы любые компоненты: датчики, приемники, передатчики, считыватели, моторы, аккумуляторы и т. п., а также их комбинации.

Программный элемент системы mbs может быть представлен следующим образом:

$$sw = (SW', L_{sw}, p_{sw}),$$

где SW' – множество программных подэлементов программного элемента sw ; L_{sw} – связей между элементами sw ; p_{sw} – свойства программного элемента sw . В качестве примера sw может быть использован любой алгоритм, библиотека, прошивка, база данных, приложение или конфигурация.

Связи между элементами системы mbs могут быть представлены следующим образом:

$$L = (R, I, E, p_L),$$

где R – множество протоколов связи, задействованных в L ; I – интерфейсов связи, задействованных в L ; E – сторон связи, задействованных в L ; p_L – свойства связей L . При этом связи между элементами mbs в рамках модели разделены следующим образом:

- L_{mbs} – между устройствами системы;
- L_{bb} – между контроллерами устройств;
- L_{hw} – между контроллерами и компонентами;
- L_{sw} – между программными элементами.

Это указывает на то, что модель позволяет представлять протоколы низкого уровня между контроллерами и компонентами вместе с соеди-

нениями между различными алгоритмами внутри прошивки одного из контроллеров, при этом имея возможность представлять протоколы высокого уровня между устройствами (таблица 2).

ТАБЛИЦА 2. Типы связей между элементами моделей

TABLE 2. Link Types between Model Elements

T_{un}	Пример	R	I	E
L_{mbs}	Wi-Fi	IEEE 800.11	wireless 2,4 GHz	устройство ↔ устройство
	ZigBee	IEEE 802.15.4	wireless 2,4 GHz	
	Bluetooth	IEEE 802.15.1	wireless 2,4 GHz	
	nRF24L01+	ESB	wireless 2,4 GHz	
	Infrared	NEC	wireless 38 kHz	
L_{bb}	I2C	SDA + SCL	TWI	контроллер ↔ контроллер
	Serial	TxRx	UART	
	RS-232	RS232	UART	
	RS-485	RS485	UART	
L_{bb}	pin-to-pin	общее питание	shield	контроллер ↔ компонент
	SVG	AVR I/O pin	трехпроводной	
	VG	AVR I/O pin	трехпроводной	
L_{bb}	метод	функции	компилятор	программный элемент ↔ программный элемент
	база данных	SQL-запросы	psycorp2	
	API	JSON-структуры	POST/GET	

В рамках разработанной модели все элементы связаны друг с другом через свойства. Данные свойства могут быть представлены следующим образом:

$$p = (FR, NL, PF, PR),$$

где FR – множество функциональных требований, выполнение которых необходимо для работы элемента; NL – нефункциональных ограничений, выполнение которых необходимо для работы элемента; PF – предоставляемых функциональных возможностей; PR – предоставляемых ресурсов.

В качестве FR может быть использована любая функциональность, необходимая для работы элемента системы – источник питания, защищенное соединение, протокол, интерфейс, загрузчик, библиотека, операционная система, компилятор, драйвер и т. п.; NL – ограничения, необходимые для его работы – место размещения, условия среды, напряжение, ток, флэш-память, цифровое или аналоговое подключение, место на жестком диске, оперативная память и т. п.; PF – функционал, предоставляемый элементом системы – контроль доступа, мониторинг периметра, навигация, обнаружение препятствий, работа с компонентом, шифрование, аутентификация, обработка сигнальных данных и т. п.; PR – ресурс, предоставляемый элементом системы – хранилище данных, вычислительные ресурсы, среда для запуска приложений, возможность добавления / удаления / замены компонентов, возможность взаимодействия со средой и т. п.

Злоумышленник, от которого необходимо защитить систему mbs , может быть представлен следующим образом:

$$a = (ac, kn, rs),$$

где ac – тип доступа a к mbs (от 1 до 5, таблица 3); kn – тип знаний a о mbs (от 1 до 4, таблица 4); rs – тип ресурсов, доступный a для компрометации mbs (от 1 до 3, таблица 5). При этом в разработанной модели структура типов доступа, знаний и ресурсов злоумышленника носит иерархический характер.

ТАБЛИЦА 3. Возможные типы доступа

TABLE 3. Access Types

№ п/п	Описание
1	Нет доступа к системе
2	Доступ к системе через глобальные сети
3	Доступ к системе через локальные сети
4	Физический доступ к системе
5	Полный доступ к системе

ТАБЛИЦА 4. Возможные типы знаний

TABLE 4. Knowledge Types

№ п/п	Описание
1	Общие знания о системе из публично доступных источников
2	Знания о параметрах системы
3	Знания о средствах защиты системы
4	Знания о программном и аппаратном обеспечении системы

ТАБЛИЦА 5. Возможные типы ресурсов

TABLE 5. Resources Types

№ п/п	Описание
1	Общеизвестные программные инструменты и уязвимости
2	Специализированные инструменты и уязвимости нулевого дня
3	Возможность исследования системы

Атакующее действие, направленное на систему mbs , можно представить следующим образом:

$$aa = (cl, oj, sj),$$

где cl – класс aa ; oj – объект aa , связывает aa с элементом или элементами системы mbs ; sj – субъект aa , связывает aa с a , характеристики которого достаточны для успешной реализации aa .

Классы атакующих действий могут быть представлены на следующих уровнях:

$$cl = \{cn, cr, dv, st\},$$

где cn – компонентов и их взаимосвязей с контроллерами системы; cr – контроллеров и их взаимосвязей с другими контроллерами системы; dv – устройств и их взаимосвязей с другими устройствами системы; st – системы и их взаимосвязей с другими системами.

В качестве атакующих действий могут быть приведены следующие примеры:

– на уровне *cn*: $cn = \{gie, bcd, rpt, rmt\}$,

где *gie* – создание некорректных событий от компонентов системы; *bcd* – обход алгоритмов обнаружения компонентов системы; *rpt* – замена компонентов системы; *rmt* – извлечение компонентов системы;

– на уровне *cr*: $cr = \{rfw, rbl, mup, imw\}$,

где *rfw* – замена прошивки контроллера; *rbl* – переустановка загрузчика (bootloader) контроллера; *mup* – вмешательство в работу системы обновления контроллера; *imw* – вмешательство в работу проводных каналов связи контроллера.

– на уровне *dv*: $dv = \{vau, cad, iec, iws\}$,

где *vau* – вмешательство в работу системы аутентификации устройства; *cad* – криптографический анализ передаваемых устройством данных; *iec* – атака, направленная на повышение энергопотребления устройства; *iws* – вмешательство в работу беспроводных каналов связи устройства.

– на уровне *st*: $st = \{soc, pwr, web, dbd\}$,

где *soc* – применение социальной инженерии для получения доступа к системе; *pwr* – прекращение энергоснабжения системы; *web* – вмешательство в

работу веб-сервисов системы; *dbd* – вмешательство в работы баз данных системы.

Отметим, что в данной модели компоненты, обеспечивающие защищенность системы, не выделены в качестве отдельного элемента теоретико-множественного представления. Это связано с тем, что большинство таких компонентов представимы как программных и аппаратных элементов, в то время как остальные – как рекомендаций по работе с системой, ее обслуживанием и поддержкой.

4. Взаимосвязи моделей

Рассмотрим, как классы атакующих действий (*cl*) связаны с параметрами злоумышленников (*ac*, *kn*, *rs*), необходимыми для их реализации (таблица 6). В качестве примера рассмотрим ситуацию, когда проектируемая *mbs* должна быть защищена от *a* с параметрами $ac = 4$, $kn = 2$ и $rs = 2$. Выделение границ ячеек таблицы толщиной линий и цветом показывает значения параметров злоумышленника. Связи между возможностью реализации атакующих действий и достаточными значениями параметров злоумышленника показаны знаком «+». В соответствии с содержанием таблицы, проектируемая *mbs* должна быть защищена от *rpt*, *rmt*, *imw*, *iec*, *iws*, *soc*, *pwr*, *web* и *dbd*. Данные атакующие действия также выделены в таблице.

ТАБЛИЦА 6. Связи между атакующими действиями и параметрами злоумышленника

TABLE 6. Connections between Attack Actions and Attacker Parameters

Атакующие действия			<i>a</i>											
			<i>ac</i>					<i>kn</i>				<i>rs</i>		
			1	2	3	4	5	1	2	3	4	1	2	3
<i>cl</i>	<i>cn</i>	<i>gie</i>			+	+	+		+	+	+			+
		<i>bcd</i>			+	+	+			+	+		+	+
		<i>rpt</i>				+	+		+	+	+	+	+	+
		<i>rmt</i>				+	+	+	+	+	+	+	+	+
	<i>cr</i>	<i>rfw</i>				+	+				+			+
		<i>rbl</i>				+	+				+			+
		<i>mup</i>			+	+	+			+	+		+	+
		<i>imw</i>				+	+	+	+	+	+	+	+	+
	<i>dv</i>	<i>vau</i>			+	+	+			+	+		+	+
		<i>cad</i>			+	+	+			+	+		+	+
		<i>iec</i>			+	+	+		+	+	+	+	+	+
		<i>iws</i>			+	+	+	+	+	+	+		+	+
	<i>st</i>	<i>soc</i>	+	+	+	+	+	+	+	+	+	+	+	+
		<i>pwr</i>				+	+	+	+	+	+	+	+	+
		<i>web</i>		+	+	+	+		+	+	+	+	+	+
		<i>dbd</i>		+	+	+	+		+	+	+	+	+	+

Как было упомянуто ранее, в разработанной модели структура параметров злоумышленника иерархична. Иерархичность параметров влияет на то, что злоумышленник с определенным типом доступа к системе имеет возможность осуществить любое атакующее действие, которое возможно

для злоумышленников с таким же типом доступа, но с меньшими знаниями/ресурсами. Такая зависимость позволяет хранить данные только о пороговых значениях параметров, необходимых для успешной реализации атакующих действий. При этом разработанная модель позволяет использо-

вать различные модели атакующих и атакуемых действий, изменяя количество параметров и диапазоны их значений. Точно так же для атакуемых действий можно использовать другую классифика-

цию, а примеры можно расширить. Также рассмотрим, как классы атакуемых действий связаны с элементами защиты систем на основе микроконтроллеров (таблица 7).

ТАБЛИЦА 7. Связи между атакующими действиями и элементами защиты

TABLE 7. Connections between Attack Actions and Security Elements

Атакующие действия			Элементы защиты
cl	cn	gie	алгоритм обнаружения аномалий, скрытое размещение датчиков
		bcd	алгоритм корреляции событий, скрытое размещение датчиков
		rpt	антивандальный корпус, аппаратная аутентификация
		rmt	антивандальный корпус
	cr	rftw	антивандальный корпус, шифрование прошивки
		rbl	антивандальный корпус, шифрование загрузчика
		mup	антивандальный корпус, удаление физического интерфейса обновления
		imw	антивандальный корпус, шифрование, аутентификация
	dv	vau	надежные учетные данные для входа, политика паролей, защита от грубой силы
		cad	надежные алгоритмы шифрования, безопасный механизм распределения ключей
		iec	обнаружение аномалий на основе поведения, изоляция/ограничение устройств
		iws	надежный алгоритм шифрования в точке доступа, надежные учетные данные для входа в систему, аутентификация на основе пары открытых ключей
	st	soc	обучение операторов и пользователей, политика безопасности
		pwr	источники бесперебойного питания, резервный источник питания
		web	брандмауэр, механизм обновления, механизм резервного копирования, механизм ведения журнала
		dbd	проверка ввода, строгая политика доступа, надежные учетные данные для входа, отдельные пользователи базы данных для разных операций

В разработанной модели возможные атакуемые действия определяются элементами системы, а также параметрами злоумышленника, от которого данную систему необходимо защитить. При этом для предотвращения возможности реализации атакуемых действий могут быть использованы различные элементы защиты, интерпретация которых в качестве программных (например, алгоритм обнаружения аномалий) и аппаратных (антивандальный корпус) элементов, а также рекомендаций (обучение операторов и пользователей) позволяет в рамках разработанной модели сделать их встраивание неотъемлемой частью процесса проектирования защищенных систем.

Рассмотрим, как возможность реализации классов атакуемых действий зависит от наличия в системе элементов, не относящихся к элементам защиты (таблица 8). Важно отметить, что взаимосвязи таких элементов с возможностью реализации атакуемых действий, дополненные информацией о параметрах злоумышленника, определяют совокупность атакуемых действий, защиту от которых необходимо обеспечить.

Данные о релевантных атакуемых действиях позволяют проработать защиту от них еще на ранних стадиях жизненного цикла системы, что повышает не только текущий уровень ее безопасности, но и облегчает дальнейший процесс поддержки уровня защищенности при эксплуатации системы.

5. Область применения

Результаты сравнения разработанной модели с другими решениями сведены в единую таблицу 9, где использованы следующие условные обозначения: «+» – поддержка анализируемого параметра; «-» – отсутствие поддержки; «*» – потенциальная возможность поддержки данного параметра. Сравнение было выполнено по уровням систем на основе микроконтроллеров, описание которых возможно с помощью проанализированных моделей, а также классам атак, учет которых возможен в рамках данных моделей.

При этом выделены следующие уровни системы:

- $cn \leftrightarrow cr$, т. е. контроллеры, компоненты и их взаимодействия;
- $cr \leftrightarrow cr$, т. е. контроллеры и их взаимодействие друг с другом;
- $dv \leftrightarrow dv$, т. е. устройства и их взаимодействие друг с другом;
- $st \leftrightarrow st$, т. е. система и ее взаимодействие с другими системами.

В свою очередь, атакуемые действия (атаки) разделены на следующие классы:

- cn (на компоненты и их связь с контроллерами);
- cr (на контроллеры и их связь с другими контроллерами);
- dv (на устройства и их связь с другими устройствами);
- st (на систему и ее связь с другими системами).

ТАБЛИЦА 8. Связи между атакующими действиями и элементами систем

TABLE 8. Connections between Attack Actions and System Elements

Атакующие действия			<i>mbs</i>
<i>cl</i>	<i>cn</i>	<i>gie</i>	компоненты, измеряющие параметры окружающей среды
		<i>bcd</i>	компоненты, контролирующие изменение параметров окружающей среды
		<i>rpt</i>	любой компонент
		<i>rmt</i>	любой компонент
	<i>cr</i>	<i>r fw</i>	любой контроллер с возможностью перезаписи прошивки
		<i>r bl</i>	любой контроллер с возможностью перезаписи загрузчика
		<i>mu p</i>	любой контроллер с системой обновления
		<i>im w</i>	контроллер ↔ контроллер, контроллер ↔ компонент
	<i>dv</i>	<i>vau</i>	устройство ↔ устройство, если в процессе взаимодействия используется аутентификация
		<i>cad</i>	устройство ↔ устройство, если в процессе взаимодействия используется шифрование
		<i>ie c</i>	любое устройство с возможностью гибберации и/или беспроводными интерфейсами
		<i>iws</i>	устройство ↔ устройство
	<i>st</i>	<i>soc</i>	любая система с пользователями и/или операторами
		<i>pwr</i>	любая система с питанием по сети
		<i>web</i>	любая система с веб-сервисами
		<i>dbd</i>	любая система с базой данных

ТАБЛИЦА 9. Сравнение с другими решениями

TABLE 9. Comparison with Other Solutions

Решения	Уровни системы				Классы атак			
	<i>cn ↔ cr</i>	<i>cr ↔ cr</i>	<i>dv ↔ dv</i>	<i>st ↔ st</i>	<i>cn</i>	<i>cr</i>	<i>dv</i>	<i>st</i>
[17]	–	–	–	–	–	*	*	–
[18]	–	–	–	–	–	*	*	–
[19]	+	+	–	–	+	+	–	–
[21]	+	+	–	–	–	+	–	–
[23]	+	+	–	–	+	+	–	–
[26]	–	–	+	–	–	+	+	–
Предлагаемое	+	+	+	+	+	+	+	+

Сравнение показало, что разработанная модель обеспечивает учет всех анализируемых классов атакующих действий, а также позволяет описать проектируемую систему на основе микроконтроллеров на всех представленных уровнях, в то время как другие решения уступают в данных параметрах.

6. Заключение

В данной работе предложена иерархическая модель для проектирования систем на основе мик-

роконтроллеров защищенными от киберфизических атак. Описание модели выполнено в рамках теоретико-множественного подхода.

При этом были представлены следующие элементы модели: система в целом, программно-аппаратные блоки, программные и аппаратные элементы, связи между элементами (на уровне устройств, контроллеров, компонентов и программного обеспечения), свойства элементов (предоставляемый и запрашиваемый функционал/ресурсы), злоумышленник, атакующие действия, а также их классификация. Были показаны взаимосвязи между элементами модели: параметры злоумышленника, достаточные для успешной реализации атакующих действий; элементы систем на основе микроконтроллеров, необходимые для реализации атакующих действий; элементы защиты, достаточные для предотвращения атакующих действий.

В рамках дальнейших исследований планируется расширение предлагаемой модели инструментами имитационного моделирования для динамического анализа защищенности систем. Также планируется апробация предложенной модели в различных приложениях.

Список источников

1. Левшун Д.С., Гайфулина Д.А., Чечулин А.А., Котенко И.В. Проблемные вопросы информационной безопасности киберфизических систем // Информатика и автоматизация. 2020. Т. 19. № 5. С. 1050–1088. DOI:10.15622/ia.2020.19.5.6
2. Левшун Д.С., Чечулин А.А., Котенко И.В. Жизненный цикл разработки защищенных систем на основе встроженных устройств // Защита информации. Инсайд. 2017. № 4. С. 53–59.
3. Котенко И.В., Чечулин А.А., Левшун Д.С. Анализ защищенности инфраструктуры железнодорожного транспорта на основе аналитического моделирования // Защита информации. Инсайд. 2017. № 6. С. 48–57.
4. Левшун Д.С., Чечулин А.А., Котенко И.В. Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи. 2019. Т. 5. № 4. С. 114–123. DOI:10.31854/1813-324X-2019-5-4-114-123
5. Левшун Д.С., Чечулин А.А., Котенко И.В. Проектирование безопасной среды передачи данных на примере протокола I2C // Защита информации. Инсайд. 2018. № 4. С. 54–62.

6. Islam J., Habiba U., Kabir H., Martuza KG., Akter F., Hafiz F., et al. Design and Development of Microcontroller Based Wireless Humidity Monitor // IOSR Journal of Electrical and Electronics Engineering // 2018. Vol. 13. Iss. 2. PP. 41–46. DOI:10.9790/1676-1302034146
7. Sowah RA., Boahene DE., Owoh DC., Addo R., Mills G.A., Owusu-Banahene W., et al. Design of a Secure Wireless Home Automation System with an Open Home Automation Bus (OpenHAB 2) Framework // Journal of Sensors. 2020. Vol. 2020. PP. 1–22. DOI:10.1155/2020/8868602
8. Tebueva F.B., Rosenko A.P., Nechvoloda V.E. Development of Methods and Software Modules Security Assessment Information of Limited Distribution // Proceedings of the Young Scientist's Third International Workshop on Trends in Information Processing (YSIP3 2019, Stavropol, Russia, 17–20th September 2019). CEUR, 2019.
9. Mutharasu S., Divya V., Bharathi D.K., Elakkiya M.V., Janani E. Design and implementation of agrobot by using IoT // International Journal of Advance Research, Ideas and Innovations in Technology. 2019. Vol. 5. Iss. 2. PP. 10–13.
10. Kovtunen A., Bilyalov A., Valeev S. Distributed Streaming Data Processing in IoT Systems Using Multi-agent Software Architecture // Proceedings of the 18th International Conference on Next Generation Wired/Wireless Networking, NEW2AN 2018, and 11th Conference on Internet of Things, Smart Spaces, and Next Generation Networks and Systems, ruSMART 2018, (St. Petersburg, Russia, 27–29 August 2018). Lecture Notes in Computer Science. Vol. 11118. Cham: Springer, 2018. PP. 572–583. DOI:10.1007/978-3-030-01168-0_51
11. Ceken C., Abdurahman D. Simulation Modeling of An IoT Based Cold Chain Logistics Management System // Sakarya University Journal of Computer and Information Sciences. 2019. Vol. 2. Iss. 2. PP. 89–100. DOI:10.35377/saucis.02.02.598963
12. Ashouri M., Lorig F., Davidsson P., Spalazzese R. Edge Computing Simulators for IoT System Design: An Analysis of Qualities and Metrics // Future Internet. 2019. Vol. 11. Iss. 11. P. 235. DOI:10.3390/fi11110235
13. Giménez P., Molína B., Palau C.E., Esteve M. SWE Simulation and Testing for the IoT // Proceedings of the International Conference on Systems, Man, and Cybernetics (Manchester, UK, 13–16 October 2013). IEEE, 2013. PP. 356–361. DOI:10.1109/SMC.2013.67
14. Andres-Maldonado P., Lauridsen M., Ameigeiras P., Lopez-Soler J.M. Analytical Modeling and Experimental Validation of NB-IoT Device Energy Consumption // IEEE Internet of Things Journal. 2019. Vol. 6. Iss. 3. PP. 5691–5701. DOI:10.1109/JIOT.2019.2904802
15. Udoh S.J., Srivastava V.M. Analytical Modeling of Radio Network Performance for 5G (Non-Standalone) and It's Network Connectivity // Journal of Communications. 2020. Vol. 15. Iss. 12. PP. 886–895. DOI:10.12720/jcm.15.12.886-895
16. Bhavana A., Nandha Kumar A.N. An Analytical Modeling for Leveraging Scalable Communication in IoT for Inter-Domain Routing // Proceedings of the Computational Methods in Systems and Software (CoMeSySo 2018, 12–14 September 2018). Advances in Intelligent Systems and Computing. Vol. 859. Cham: Springer, 2018. PP. 1–11. DOI:10.1007/978-3-030-00211-4_1
17. Hu F., Lu Y., Vasilakos A.V., Hao Q., Ma R., Patil Y., et al. Robust Cyber-Physical Systems: Concept, models, and implementation // Future Generation Computer Systems. 2016. Vol. 56. PP. 449–475. DOI:10.1016/j.future.2015.06.006
18. Penas O., Plateaux R., Patalano S., Hammadi M. Multi-scale approach from mechatronic to Cyber-Physical Systems for the design of manufacturing systems // Computers in Industry. 2017. Vol. 86. PP. 52–69. DOI:10.1016/j.compind.2016.12.001
19. Scott-Hayward S. Design and deployment of secure, robust, and resilient SDN controllers // Proceedings of the 1st Conference on Network Softwarization (London, UK, 13–17 April 2015). IEEE, 2015. PP. 1–5. DOI:10.1109/NETSOFT.2015.7258233
20. Hu F., Hao Q., Bao K. A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation // IEEE Communications Surveys & Tutorials. 2014. Vol. 16. Iss. 4. PP. 2181–2206. DOI:10.1109/COMST.2014.2326417
21. Lin Z., Yu S., Lü J., Cai S., Chen G. Design and ARM-Embedded Implementation of a Chaotic Map-Based Real-Time Secure Video Communication System // IEEE Transactions on Circuits and Systems for Video Technology. 2014. Vol. 25. Iss. 7. PP. 1203–1216. DOI:10.1109/TCSVT.2014.2369711
22. National Institute of Standards and Technology // NIST. URL: <https://www.nist.gov> (дата обращения 3.02.2023)
23. Desnitsky V., Kotenko I., Chechulin A. Configuration-based approach to embedded device security // Proceedings of the 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2012, St. Petersburg, Russia, 17–19 October 2012). Lecture Notes in Computer Science. Vol. 7531. Berlin, Heidelberg: Springer, 2012. PP. 270–285. DOI:10.1007/978-3-642-33704-8_23
24. UML Profile for MARTE: Modeling and Analysis of Real-Time Embedded Systems. 2011. URL: <https://www.omg.org/spec/MARTE/1.1/PDF> (дата обращения 3.02.2023)
25. Chechulin A., Kotenko I., Desnitsky V. An Approach for Network Information Flow Analysis for Systems of Embedded Components // Proceedings of the 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2012, St. Petersburg, Russia, 17–19 October 2012). Lecture Notes in Computer Science. Vol. 7531. Berlin, Heidelberg: Springer, 2012. PP. 146–155. DOI:10.1007/978-3-642-33704-8_13
26. Design of Secure and Energy-Efficient Embedded Systems for Future Internet Applications // CORDIS. URL: <https://cordis.europa.eu/project/id/256668> (дата обращения 3.02.2023)

References

1. Levshun D., Gaifulina D., Chechulin A., Kotenko I. Problematic Issues of Information Security of Cyber-Physical Systems. *Informatics and Automation*. 2020;19(5):1050–1088. (in Russ.) DOI:10.15622/ia.2020.19.5.6
2. Levshun D., Chechulin A., Kotenko I. Design lifecycle for secure cyber-physical systems based on embedded devices. *Zašita informacii. Inside*. 2017;4(76):53–59. (in Russ.)
3. Kotenko I., Chechulin A., Levshun D. Security analysis of railway transport infrastructure on the base of analytical modeling. *Zašita informacii. Inside*. 2017;6(78):48–57. (in Russ.)
4. Levshun D., Chechulin A., Kotenko I. A Comprehensive Model of Secure Cyber-Physical Systems for their Design and Verification. *Proc. of Telecom. Universities*. 2019;5(4):114–123 (in Russ.) DOI:10.31854/1813-324X-2019-5-4-114-123
5. Levshun D., Chechulin A., Kotenko I. Design of Secure Data Transfer Environment Using the I2C Protocol as an Example. *Zašita informacii. Inside*. 2018; 4(82):54–62. (in Russ.)

6. Islam J., Habiba U., Kabir H., Martuza KG., Akter F., Hafiz F., et al. Design and Development of Microcontroller Based Wireless Humidity Monitor. *IOSR Journal of Electrical and Electronics Engineering*. 2018;13(2):41–46. DOI:10.9790/1676-1302034146
7. Sowah RA., Boahene DE., Owoh DC., Addo R., Mills G.A., Owusu-Banahene W., et al. Design of a Secure Wireless Home Automation System with an Open Home Automation Bus (OpenHAB 2) Framework. *Journal of Sensors*. 2020;2020:1–22. DOI:10.1155/2020/8868602
8. Tebueva F.B., Rosenko A.P., Nechvoloda V.E. Development of Methods and Software Modules Security Assessment Information of Limited Distribution. *Proceedings of the Young Scientist's Third International Workshop on Trends in Information Processing, YSIP3 2019, 17–20th September 2019, Stavropol, Russia*. CEUR; 2019.
9. Mutharasu S., Divya V., Bharathi D.K., Elakkiya M.V., Janani E. Design and implementation of agrobot by using IoT. *International Journal of Advance Research, Ideas and Innovations in Technology*. 2019;5(2):10–13.
10. Kovtunen A., Bilyalov A., Valeev S. Distributed Streaming Data Processing in IoT Systems Using Multi-agent Software Architecture. *Proceedings of the 18th International Conference on Next Generation Wired/Wireless Networking, NEW2AN 2018, and 11th Conference on Internet of Things, Smart Spaces, and Next Generation Networks and Systems, ruSMART 2018, 27–29 August 2018, St. Petersburg, Russia. Lecture Notes in Computer Science. vol.11118*. Cham: Springer; 2018. p.572–583. DOI:10.1007/978-3-030-01168-0_51
11. Ceken C., Abdurahman D. Simulation Modeling of An IoT Based Cold Chain Logistics Management System. *Sakarya University Journal of Computer and Information Sciences*. 2019;2(2):89–100. DOI:10.35377/saucis.02.02.598963
12. Ashouri M., Lorig F., Davidsson P., Spalazzese R. Edge Computing Simulators for IoT System Design: An Analysis of Qualities and Metrics. *Future Internet*. 2019;11(11):235. DOI:10.3390/fi11110235
13. Giménez P., Molína B. Palau C.E., Esteve M. SWE Simulation and Testing for the IoT. *Proceedings of the International Conference on Systems, Man, and Cybernetics, 13–16 October 2013, Manchester, UK*. IEEE; 2013. PP. 356–361. DOI:10.1109/SMC.2013.67
14. Andres-Maldonado P., Lauridsen M., Ameigeiras P., Lopez-Soler J.M. Analytical Modeling and Experimental Validation of NB-IoT Device Energy Consumption. *IEEE Internet of Things Journal*. 2019;6(3):5691–5701. DOI:10.1109/JIOT.2019.2904802
15. Udoh S.J., Srivastava V.M. Analytical Modeling of Radio Network Performance for 5G (Non-Standalone) and It's Network Connectivity. *Journal of Communications*. 2020;15(12):886–895. DOI:10.12720/jcm.15.12.886-895
16. Bhavana A., Nandha Kumar A.N. An Analytical Modeling for Leveraging Scalable Communication in IoT for Inter-Domain Routing. *Proceedings of the Computational Methods in Systems and Software, CoMeSySo 2018, 12–14 September 2018. Advances in Intelligent Systems and Computing. vol.859*. Cham: Springer; 2018. p.1–11. DOI:10.1007/978-3-030-00211-4_1
17. Hu F., Lu Y., Vasilakos A.V., Hao Q., Ma R., Patil Y., et al. Robust Cyber-Physical Systems: Concept, models, and implementation. *Future Generation Computer Systems*. 2016;56:449–475. DOI:10.1016/j.future.2015.06.006
18. Penas O., Plateaux R., Patalano S., Hammadi M. Multi-scale approach from mechatronic to Cyber-Physical Systems for the design of manufacturing systems. *Computers in Industry*. 2017;86:52–69. DOI:10.1016/j.compind.2016.12.001
19. Scott-Hayward S. Design and deployment of secure, robust, and resilient SDN controllers. *Proceedings of the 1st Conference on Network Softwarization, NetSoft, 13–17 April 2015, London, UK*. IEEE; 2015. p.1–5. DOI:10.1109/NETSOFT.2015.7258233
20. Hu F., Hao Q., Bao K. A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation. *IEEE Communications Surveys & Tutorials*. 2014;16(4):2181–2206. DOI:10.1109/COMST.2014.2326417
21. Lin Z., Yu S., Lü J., Cai S., Chen G. Design and ARM-Embedded Implementation of a Chaotic Map-Based Real-Time Secure Video Communication System. *IEEE Transactions on Circuits and Systems for Video Technology*. 2014;25(7):1203–1216. DOI:10.1109/TCSVT.2014.2369711
22. NIST. National Institute of Standards and Technology. URL: <https://www.nist.gov> [Accessed 3rd February 2023]
23. Desnitsky V., Kotenko I., Chechulin A. Configuration-based approach to embedded device security. *Proceedings of the 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012, 17–19 October 2012, St. Petersburg, Russia. Lecture Notes in Computer Science. vol.7531*. Berlin, Heidelberg: Springer; 2012. p.270–285. DOI:10.1007/978-3-642-33704-8_23
24. UML Profile for MARTE: Modeling and Analysis of Real-Time Embedded Systems. 2011. URL: <https://www.omg.org/spec/MARTE/1.1/PDF> [Accessed 3rd February 2023]
25. Chechulin A., Kotenko I., Desnitsky V. An Approach for Network Information Flow Analysis for Systems of Embedded Components. *Proceedings of the 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012, 17–19 October 2012, St. Petersburg, Russia. Lecture Notes in Computer Science. vol.7531*. Berlin, Heidelberg: Springer; 2012. p.146–155. DOI:10.1007/978-3-642-33704-8_13
26. CORDIS. Design of Secure and Energy-Efficient Embedded Systems for Future Internet Applications. URL: <https://cordis.europa.eu/project/id/256668> [Accessed 3rd February 2023]

Статья поступила в редакцию 06.02.2023; одобрена после рецензирования 14.02.2023; принята к публикации 15.02.2023.

The article was submitted 06.02.2023; approved after reviewing 14.02.2023; accepted for publication 15.02.2023.

Информация об авторе:

**ЛЕВШУН
Дмитрий Сергеевич**

старший научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук,
 <https://orcid.org/0000-0003-1898-6624>

77 РЕГИОНАЛЬНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ
СТУДЕНТОВ, АСПИРАНТОВ И МОЛОДЫХ УЧЕНЫХ

СТУДЕНЧЕСКАЯ ВЕСНА

23–24 МАЯ 2023

Научные направления:

-  Радиотехнологии связи
-  Инфокоммуникационные сети и системы
-  Информационные системы и технологии
-  Теоретические основы радиоэлектроники
-  Цифровая экономика, управление и бизнес-информатика
-  Социальные цифровые технологии
-  Сети связи специального назначения
-  Перспективные разработки для применения в беспилотных комплексах



РЕГИСТРАЦИЯ
и подробности
о конференции на сайте:
VESNA.SUT.RU

СПбГУТ)))



22³¹
десятилетие
науки и технологий

11–14 апреля 2023

СВЯЗЬ

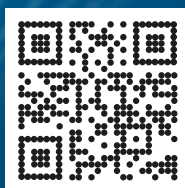
35-я юбилейная международная
выставка «Информационные
и коммуникационные технологии»



Экспозиция «Навитех» —
«Навигационные системы, технологии и услуги»



www.sviaz-expo.ru



Россия, Москва,
ЦВК «ЭКСПОЦЕНТР»

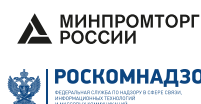


12+
Реклама

Организатор



При поддержке



Под патронатом



В рамках



Выходные данные

Дизайн обложки – ООО «Комильфо»

План издания научной литературы 2023 г., п. 7

Дата выхода в свет	Усл.-печ. л.	Формат	Тираж	Заказ	Свободная цена
20.03.2023	16	60×84 _{1/8}	1000 экз.	№ 1432	

Ответственный редактор **Татарникова И.М.**
Выпускающий редактор **Яшугин Д.Н.**

Адрес СПбГУТ:
193232, Санкт-Петербург, пр. Большевиков, 22/1

Учредитель и издатель:

Федеральное государственное бюджетное образовательное учреждение
высшего образования "Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича"

E-mail: tuzs@spbgut.ru Web: tuzs.sut.ru VK: vk.com/spbtuzs



Подписной индекс в Объединенном каталоге "ПРЕССА РОССИИ" - 59983