Научно-технический журнал

H&ES RESEARCH

Scientific and Technical Journal

НАУКОЕМКИЕ ТЕХНОЛОГИИ В КОСМИЧЕСКИХ ИССЛЕДОВАНИЯХ ЗЕМЛИ

HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH

Журнал **H&ES Research** издается с 2009 года, освещает достижения и проблемы российских инфокоммуникаций, внедрение последних достижений отрасли в автоматизированных системах управления, развитие технологий в информационной безопасности, исследования космоса, развитие спутникового телевидения и навигации, исследование Арктики. Особое место в издании уделено результатам научных исследований молодых ученых в области создания новых средств и технологий космических исследований Земли.

Журнал H&ES Research входит в перечень изданий, публикации в которых учитываются Высшей аттестационной комиссиейРоссии (ВАК РФ), в систему российского индекса научного цитирования (РИНЦ), а также включен в Международный классификатор периодических изданий.

Тематика публикуемых статей в соответствии с перечнем группспециальностей научных работников по Номенклатуре специальностей:

- 2.2.15 Системы, сети и устройства телекоммуникаций (техн. науки)
- 2.3.1 Системный анализ, управление и обработка информации (техн. науки)
- 2.3.5 Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (техн. науки)
- 2.3.6 Методы и системы защиты информации, информационная безопасность (техн. науки)
- 2.5.13 Проектирование, конструкция и производство летательныхъ аппаратов (техн. науки)
- 2.5.16 Динамика, баллистика, управление движением летательных аппаратов (техн. науки)

ИНДЕКСИРОВАНИЕ ЖУРНАЛА H&ES RESEARCH

H&ES Research is published since 2009. The journal covers achievements and problems of the Russian infocommunication, introduction of the last achievements of branch in automated control systems, development of technologies in information security, space researches, development of satellite television and navigation, research of the Arctic. The special place in the edition is given to results of scientific researches of young scientists in the field of creation of new means and technologies of space researches of Earth.

The journal H&ES Research is included in the list of scientific publications, recommended Higher Attestation Commission Russian Ministry of Education for the publication of scientific works, which reflect the basic scientific content of candidate and doctoral theses. IF of the Russian Science Citation Index.

Subject of published articles according to the list of branches of science and groups of scientific specialties in accordance with the specialties:

- 2.2.15 Telecommunication systems, networks and devices
- 2.3.1 System analysis, management and information processing
- 2.3.5 Mathematical and software support for computing systems, complexes and computer networks
- 2.3.6 Methods and systems of information security
- 2.5.13 Design, construction and production of aircraft
- 2.5.16 Dynamics, ballistics, aircraft motion control

JOURNAL H&ES RESEARCH INDEXING

• NEICON • CyberLenika (Open Science) • Google Scholar • OCLC WorldCat • Ulrich's Periodicals Directory • • Bielefeld Academic Search Engine (BASE) • eLIBRARY.RU • Registry of Open Access Repositories (ROAR)

Все номера журнала находятся в свободном доступе на сайте журнала **www.hes.ru** и библиотеке **elibrary.ru.**

Всем авторам, желающим разместить научную статью в журнале, необходимо оформить ее согласно требованиям и направить материалы на электронную почту: **HT-ESResearch@yandex.ru.**
С требованиями можно ознакомиться на сайте: **www.H-ES.ru.**

Язык публикаций: русский, английский.
Периодичность выхода – 6 номеров в год.
Свидетельство о регистрации СМИ ПИ № ФС 77-60899 от 02.03.2015
Территория распространения: Российская Федерация, зарубежные страны

Тираж 1000 экз. Цена 1000 руб.
Плата с аспирантов за публикацию рукописи не взимается.

All issues of the journal are in a free access on a site of the journal **www.hes.ru** and **elibrary.ru.**

All authors wishing to post a scientific article in the journal, you must register it according to the requirements and send the materials to your email: **HT-ESResearch@yandex.ru.**
The requirements are available on the website: **www.H-ES.ru.**

Language of publications: Russian, English.
Periodicity – 6 issues per year.
Media Registration Certificate PI No. FS77-60899. Date of issue: March 2, 2015.
Distribution Territory: Russian Federation, foreign countries

Circulation of 1000 copies. Price of 1000 Rur.
Postgraduate students for publication
of the manuscript will not be charged

ISSN 2409-5419 (Print) ISSN 2412-1363 (Online) WWW.H-ES.RU Дата выхода: 25 апреля 2023

3 2023 Т.15

Учредитель:
ООО "ИД Медиа Паблишер"

Издатель:
ДЫМКОВА С.С.

Адрес издателя:
111024, Россия, Москва,
ул. Авиамоторная, д. 8, корп. 1, офис 323.

Адрес редакции:
194044, Россия, Санкт-Петербург,
Лесной Проспект, 34-36, к. 1,
Тел.: +7(911) 194-12-42.

Адрес типографии:
Россия, Москва, ул. Складочная, д. 3, кор. 6.

СОДЕРЖАНИЕ

CONTENTS

Founder:
"Media Publisher", LLC

Publisher:
DYMKOVA S.S.

Address of publisher:
111024, Russia, Moscow,
st. Aviamotornaya, 8, bild. 1, office 323

Address of edition:
194044, Russia, St. Petersburg,
Lesnoy av., 34-36, h.1,
Phone: +7 (911) 194-12-42.

Address of printing house:
Russia, Moscow, st. Skladochnaya, 3, h. 6

doi: 10.36724/2409-5419-2023-15-3-4-10

ВЛИЯНИЕ НЕОДНОРОДНОЙ ТЕПЛОЗАЩИТЫ НА ХАРАКТЕРИСТИКИ ИЗЛУЧЕНИЯ АНТЕННЫ КОСМИЧЕСКОГО АППАРАТА

МИХАЙЛОВ
Виктор Федорович[1]

МАЖНИК
Илья Валерьевич[2]

АННОТАЦИЯ

Введение: Знание электрических характеристик бортовой антенны на траектории спуска космического аппарата позволяет оценить наличие или отсутствие радиосвязи. В условиях аэродинамического нагрева теплозащита бортовой антенны прогревается неравномерно по толщине и становится электрически неоднородной. **Цель работы:** Определение радиотехнических характеристик бортовых антенн возвращаемых космических аппаратов, с воздействием высокотемпературного нагрева на теплозащиту антенны, на основании расчетов по разработанной математической модели антенны с теплозащитой. **Методы:** Выражения для структуры поля излучения прямоугольного волновода при названных условиях выведены методом ВКБ. Из известных аналитических методов решения возможно применение метода интегральных преобразований и метода собственных функций. Оба эти метода и использованы в работе. **Результаты:** Полученные теоретические результаты являются новыми, они позволяют прогнозировать радиотехнические характеристики бортовой антенны с учетом неравномерного нагрева по толщине теплозащиты при малых температурных градиентах. Разработана математическая модель бортовой антенны космического аппарата на траектории спуска с учетом неоднородности теплозащиты в условиях аэродинамического нагрева. **Практическая значимость:** Разработка математической модели основных радиотехнических характеристик бортовых антенн, с учетом воздействия высокотемпературного аэродинамического нагрева, а также результаты численных расчетов, могут быть применены при разработке рекомендаций выбора теплозащиты и рекомендации по уменьшению влияния температурного изменения электрических параметров теплозащиты на характеристики бортовых антенн и снижению времени потери радиосвязи или устранения потери.

Сведения об авторах:

[1] д.т.н., профессор
Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия, vmikhailov@pochta.tvoe.tv

[2] аспирант, ассистент, Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия, ilya.mazhnik@yandex.ru

КЛЮЧЕВЫЕ СЛОВА: *прямоугольный волновод; неоднородная теплозащита; ВКБ-метод; диаграмма излучения, КПД.*

Для цитирования: *Михайлов В.Ф., Мажник И.В.* Влияние неоднородной теплозащиты на характеристики излучения антенны космического аппарата // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 3. С. 4-10. doi: 10.36724/2409-5419-2023-15-3-4-10

Введение

Возвращаемые космические аппараты для связи с внешним пространством используют бортовые антенны, называемые антенными окнами, которые конструктивно представляют собой слабонаправленный излучатель, закрытый плоской радиопрозрачной нагревостойкой теплозащитой [1-9]. Знание электрических характеристик антенного окна на траектории спуска космического аппарата позволяет оценить наличие или отсутствие радиосвязи и разработать рекомендации по устранению потери связи. В ряде работ получены математические модели бортовых антенн, представляющих собой излучатель в виде открытого конца прямоугольного волновода, закрытого плоской однородной теплозащитой. [10-11]. В условиях аэродинамического нагрева теплозащита прогревается неравномерно по толщине и становится электрически неоднородной (рис. 1).

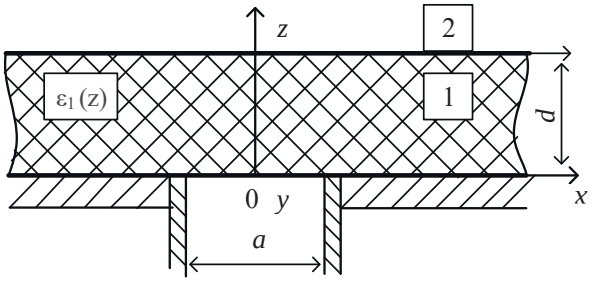

Рис. 1. Волновод с неоднородной теплозащитой:
d – толщина теплозащиты; a – длина широкой стенки прямоугольного волновода; x, y, z – декартовы координаты; 1 – область, занимаемая диэлектрической защитой; 2 – область за теплозащитой

В этом случае для определения характеристик излучения антенного окна необходимо решать волновое уравнение для произвольного изменения волнового числа по координате, нормальной теплозащите. Строгое изложение теории распространения электромагнитных волн через неоднородные диэлектрические среды имеется в работе [12], в которой решение задачи сводится к решению гипергеометрического уравнения. Данное уравнение имеет решение в конечном виде только для немногих видов функции волнового числа от координаты, перпендикулярной теплозащите.

В ряде других работ строгие решения волнового уравнения получены для некоторых частных законов изменения параметров диэлектриков в направлении распространения радиоволн [13,14]. Основные трудности применения известных решений заключаются в том, что, во-первых, не представляется возможным, даже комбинируя полученные решения, перейти к случаю произвольного изменения параметров среды и, во-вторых, полученные решения являются весьма сложными. Применение их в интегральном преобразовании Фурье для получения радиотехнических характеристик антенного окна дает настолько громоздкие выражения, что использование практически невозможным. Поэтому существенное значение приобретает возможность применения приближенных методов расчета. В данном случае целесообразно обратиться к волновым методам расчета.

При достаточно слабой зависимости электрических свойств теплозащиты от координат характеристики поля излучения могут быть получены методом фазовых интегралов (ВКБ-метод). Медленные изменения свойств среды от координат означает, что свойства среды меняются мало на расстоянии порядка длины волны. Фактически в этом методе используется приближение геометрической оптики.

Методы и решения

Решение волнового уравнения будем производить для углового спектра плоских волн, который получаем путем двойного преобразования Фурье составляющих электромагнитного поля излучения по угловым координатам волнового вектора [15].

Для ВКБ-метода решение волнового уравнения для угловых спектральных составляющих электрического поля может быть записано в следующем виде для областей в теплозащите (1) и за теплозащитой (2):

$$\hat{E}_x^{(1)} = -\frac{k'_{z_1}(z)\sqrt{k}\left(\mathrm{D}e^{-j\left(\int_0^d k_{z_1}(z)\,dz\right)} + Le^{j\left(\int_0^d k_{z_1}(z)\,dz\right)}\right)}{2\omega\varepsilon_0\varepsilon_1(z)k_{z_1}(d)^{3/2}} - \frac{jk_{z_1}(z)\sqrt{k}\left(\mathrm{D}e^{-j\left(\int_0^d k_{z_1}(z)\,dz\right)} - Le^{j\left(\int_0^d k_{z_1}(z)\,dz\right)}\right)}{\omega\varepsilon_0\varepsilon_1(z)\sqrt{k_{z_1}(d)}}, \quad (1)$$

$$\hat{E}_x^{(2)} = -\frac{k_z}{\omega\varepsilon_0}M\cdot exp\left(-jk_z z\right), \quad (2)$$

$$\hat{E}_y^{(1)} = \frac{k'_{z_1}(z)\sqrt{k}\left(\mathrm{A}e^{-j\left(\int_0^d k_{z_1}(z)\,dz\right)} + Be^{j\left(\int_0^d k_{z_1}(z)\,dz\right)}\right)}{2\omega\varepsilon_0\varepsilon_1(z)k_{z_1}(d)^{3/2}} - \frac{jk_{z_1}(z)\sqrt{k}\left(\mathrm{A}e^{-j\left(\int_0^d k_{z_1}(z)\,dz\right)} - Be^{j\left(\int_0^d k_{z_1}(z)\,dz\right)}\right)}{\omega\varepsilon_0\varepsilon_1(z)\sqrt{k_{z_1}(d)}}, \quad (3)$$

$$\hat{E}_y^{(2)} = \frac{k_z}{\omega\varepsilon_0}C\cdot exp\left(-jk_z z\right), \quad (4)$$

где *A, B, C, D, L, M* - постоянные интегрирования, k – волновое число, $k_z = \sqrt{k^2 - k_x^2 - k_y^2}$, $k_{z_1} = \sqrt{k^2\varepsilon_1(z) - k_x^2 - k_y^2}$, d – толщина слоя теплозащиты, $\varepsilon_1(z)$ – относительная диэлектрическая – проницаемость теплозащиты, z-координата перпендикулярная теплозащите, ω – угловая частота, на которой производятся исследования, ε_0 – электрическая постоянная.

Неизвестные постоянные интегрирования определяются из граничных условий для $z = 0$ и $z = d$ для поля в апертуре, определяемого волной типа H_{10}.

$$-\frac{k_{z_1}(0)(\mathrm{D}-L)}{we_0e_1(0)}\Big|_{z=0}=0,\frac{k_{z_1}(0)(A-B)}{we_0e_1(0)}\Big|_{z=0}=\hat{E}_{y_0},$$

$$\frac{\sqrt{k}\left(\mathrm{D}e^{-j\left(\int_0^d k_{z_1}(z)\,dz\right)}+Le^{j\left(\int_0^d k_{z_1}(z)\,dz\right)}\right)}{2k_{z_1}(d)^{3/2}}-$$

$$-\frac{j\sqrt{k}\left(\mathrm{D}e^{-j\left(\int_0^d k_{z_1}(z)\,dz\right)}-Le^{j\left(\int_0^d k_{z_1}(z)\,dz\right)}\right)}{\sqrt{k_{z_1}(d)}}|_{z=d}=$$

$$=\frac{e_1(d)k_z(d)Me^{-jk_zd}}{k_{z_1}(d)},$$

$$\frac{\sqrt{k}\left(Ae^{-j\left(\int_0^d k_{z_1}(z)\,dz\right)}+Be^{j\left(\int_0^d k_{z_1}(z)\,dz\right)}\right)}{2k_{z_1}(d)^{3/2}}-$$

$$\frac{j\sqrt{k}\left(Ae^{-j\left(\int_0^d k_{z_1}(z)\,dz\right)}-Be^{j\left(\int_0^d k_{z_1}(z)\,dz\right)}\right)}{\sqrt{k_{z_1}(d)}}\Bigg|_{z=d}=$$

$$=\frac{\varepsilon_1(d)k_z(d)Ce^{-jk_zd}}{k_{z_1}(d)},$$

$$-\frac{k_xk_y\sqrt{k}\left(\mathrm{D}e^{-j\left(\int_0^d k_{z_1}(d)\,dz\right)}+Le^{j\left(\int_0^d k_{z_1}(d)\,dz\right)}\right)}{\sqrt{k_{z_1}(d)}}+$$

$$+\frac{\left(k_1^2-k_x^2\right)\sqrt{k}\left(Ae^{-j\left(\int_0^d k_{z_1}(d)\,dz\right)}+Be^{j\left(\int_0^d k_{z_1}(d)\,dz\right)}\right)}{\sqrt{k_{z_1}(d)}}\Bigg|_{z=d}=$$

$$=\varepsilon_1(d)\left(\left(k^2-k_x^2\right)Ce^{-jk_zd}-k_xk_yMe^{-jk_zd}\right),$$

$$\frac{\left(k_1^2-k_y^2\right)\sqrt{k}\left(\mathrm{D}e^{-j\left(\int_0^d k_{z_1}(d)\,dz\right)}+Le^{j\left(\int_0^d k_{z_1}(d)\,dz\right)}\right)}{\sqrt{k_{z_1}(d)}}-$$

$$-\frac{k_xk_y\sqrt{k}\left(Ae^{-j\left(\int_0^d k_{z_1}(d)\,dz\right)}+Be^{j\left(\int_0^d k_{z_1}(d)\,dz\right)}\right)}{\sqrt{k_{z_1}(d)}}\Bigg|_{z=d}=$$

$$=\varepsilon_1(d)\left(\left(k^2-k_y^2\right)Me^{-jk_zd}-k_xk_yCe^{-jk_zd}\right).$$

Здесь $\hat{E}_{y_0}=\iint_{\Pi}E_y\left(x',y',0\right)\exp\left(-j(k_x x'+k_y y')\right)dx'dy'$,

где П – область интегрирования по раскрыву волновода, *x'*, *y'* – координаты, отсчитываемые в раскрыве изучаемого волновода.

Найдем выражение неизвестной постоянной интегрирования A, B, C для электрического поля $E_y^{(1,2)}$

$$\begin{aligned}
A=&(e^{j\phi}\varepsilon_0\hat{E}_{y_0}k_{z_1}(0)\varepsilon_1(0)w(-j\,k^2\left(k^2-k_x^2-k_y^2\right)k_{z_1}\times\\
&\times(d)^4-jk_z(d)\left(k_x-k_y\right)\left(k_x+k_y\right)\times\\
&\times(k-k_1)(k+k_1)k_{z_1}(d)^3+k_z(d)^2k_1^2\left(k_1^2-k_x^2-k_y\right)k_{z_1}(d)^2-\\
&-k_z(d)k'_{z_1}(d)\left(\left(k_1^2-\frac{k_x^2}{2}-\frac{k_y^2}{2}\right)k^2-\frac{k_1^2\left(k_x^2+k_y^2\right)}{2}\right)k_{z_1}(d)+\\
&+\frac{k'_{z_1}(d)^2k^2\left(k^2-k_x^2-k_y^2\right)}{4})e^{-j\phi}+e^{j\phi}\times\\
&\times\left(-k_{z_1}(d)^2\,jk^2+k_z(d)k_{z_1}(d)k_1^2-\frac{k'_{z_1}(d)k^2}{2}\right)\times\\
&\times\left(-j\left(k^2-k_x^2-k_y\right)k_{z_1}(d)^2+k_z(d)\left(k_1^2-k_x^2-k_y^2\right)k_{z_1}(d)\right.\\
&\left.-\frac{k'_{z_1}(d)\left(k^2-k_x^2-k_y^2\right)}{2}\right))/\Delta,
\end{aligned}$$

$$\begin{aligned}
B=&-(\left(j\left(k^2-k_x^2-k_y^2\right)k_{z_1}(d)^2+k_z(d)\left(k_1^2-k_x^2-k_y^2\right)k_{z_1}(d)-\right)\times\\
&\times\frac{k'_{z_1}(d)\left(k^2-k_x^2-k_y^2\right)}{2}\Big)\times\\
&\times\left(k_{z_1}(d)^2\,jk^2+k_z(d)k_{z_1}(d)k_1^2-\frac{k'_{z_1}(d)k^2}{2}\right)e^{-j\phi}+\\
&+e^{j\varphi}(-j\,k^2\left(k^2-k_x^2-k_y^2\right)k_{z_1}(d)^4+\\
&+k_z(d)\,j\left(k_x-k_y\right)\left(k_x+k_y\right)(k-k_1)(k+k_1)k_{z_1}(d)^3+\\
&+k_z(d)^2k_1^2\left(k_1^2-k_x^2-k_y^2\right)k_{z_1}(d)^2-\\
&-k_z(d)k'_{z_1}(d)\left(\left(k_1^2-\frac{k_x^2}{2}-\frac{k_y^2}{2}\right)k^2-\frac{k_1^2\left(k_x^2+k_y^2\right)}{2}\right)k_{z_1}(d)+\\
&+\frac{k'_{z_1}(d)^2k^2\left(k^2-k_x^2-k_y^2\right)}{4}))\varepsilon_0E_{y_0}k_{z_1}(0)\varepsilon_1(0)e^{-j\varphi}\omega/\Delta,
\end{aligned}$$

$$\begin{aligned}
C=&-(\left(\left(\left(k_1^2-k_x^2\right)k^2-k_1^2k_y^2\right)jk_{z_1}(d)^2+k_z(d)k_1^2\left(k_1^2-k_x^2-k_y\right)k_{z_1}(d)-\right.\\
&\left.-\frac{k'_{z_1}(d)\left(\left(k_1^2-k_x^2\right)k^2-k_1^2k_y^2\right)}{2}\right)e^{-j\phi}+\\
&+e^{j\phi}\left(-\left(\left(k_1^2-k_x^2\right)k^2-k_1^2k_y^2\right)jk_{z_1}(d)^2+k_z(d)k_1^2\left(k_1^2-k_x^2-k_y\right)k_{z_1}(d)-\right.\\
&\left.-\frac{k'_{z_1}(d)\left(\left(k_1^2-k_x^2\right)k^2-k_1^2k_y^2\right)}{2}\right)\times\\
&\times2\omega e^{-j\phi}\varepsilon_0k_{z_1}(0)\hat{E}_{y_0}k_{z_1}(d)^{3/2}\sqrt{k}e^{j\phi}j\varepsilon_1(0)/e^{jk_zd}\Delta.
\end{aligned}$$

В выражениях использована следующая замена переменных:

$$k_x = \beta\cos\alpha,\ k_y = \beta\sin\alpha, k_z = \sqrt{k^2-\beta^2}\ , k_{z_1}(d) = \sqrt{k^2\varepsilon_1(d)-\beta^2},$$

$$k_1 = \sqrt{k^2\varepsilon_1(d)}\ , \varphi = \int_0^d k_{z_1}(z)\,\mathrm{d}z,$$

$$\Delta = \left(\left(k_{z_1}(d)^2\ jk^2 + k_z(d)k_{z_1}(d)k_1^2 - \frac{k'_{z_1}(d)k^2}{2}\right)\mathrm{e}^{-j\phi} + \right.$$

$$\left. + \mathrm{e}^{j\phi}\left(-k_{z_1}(d)^2\ jk^2 + k_z(d)k_{z_1}(d)k_1^2 - \frac{k'_{z_1}(d)k^2}{2}\right)\right)$$

$$\left(\left(j\left(k^2-k_x^2-k_y^2\right)k_{z_1}(d)^2 + k_z(d)\left(k_1^2-k_x^2-k_y\right)k_{z_1}(d) - \right.\right.$$

$$\left.\left. - \frac{k'_{z_1}(d)\left(k^2-k_x^2-k_y^2\right)}{2}\right)\mathrm{e}^{-j\varphi} + \right.$$

$$\left. + \mathrm{e}^{j\phi}\left(-j\left(k^2-k_x^2-k_y^2\right)k_{z_1}(d)^2 + k_z(d)\left(k_1^2-k_x^2-k_y\right)k_{z_1}(d) - \right.\right.$$

$$\left.\left. \frac{k'_{z_1}(d)\left(k^2-k_x^2-k_y^2\right)}{2}\right)\right)k'_{z_1}(0).$$

Используя полученные выражения углового спектра плоских волн и применяя обратное преобразование Фурье, с учетом (4) запишем

$$E_y^{(1,2)} = \frac{1}{4\pi^2}\iint_{\Pi} F_y^{(1,2)}(x,y,z,x',y',0)E_y(x',y',0)dx'dy'. \quad (5)$$

Подынтегральные выражения имеют вид

$$F_y^{(1)} = \int_{-\infty}^{\infty}\int_0^{2\pi} \frac{k'_{z_1}(z)\sqrt{k}\left(\mathrm{A}\mathrm{e}^{-j\left(\int_0^d k_{z_1}(z)\,\mathrm{d}z\right)} + B\mathrm{e}^{j\left(\int_0^d k_{z_1}(z)\,\mathrm{d}z\right)}\right)}{2\omega\varepsilon_0\varepsilon_1(z)k_{z_1}(d)^{3/2}} -$$

$$- \frac{jk_{z_1}(z)\sqrt{k}\left(\mathrm{A}\mathrm{e}^{-j\left(\int_0^d k_{z_1}(z)\,\mathrm{d}z\right)} - B\mathrm{e}^{j\left(\int_0^d k_{z_1}(z)\,\mathrm{d}z\right)}\right)}{\omega\varepsilon_0\varepsilon_1(z)\sqrt{k_{z_1}(d)}}\times \quad (6)$$

$$\times\exp(-jk_z z)\times\exp\left[-j\beta\left[(x'-x)\cos a + (y'-y)\sin a\right]\beta\,d\beta\,da;\right.$$

$$F_y^{(2)} = \int_{-\infty}^{\infty}\int_0^{2\pi} \frac{k_z}{\omega\varepsilon_0} C\times\exp(-jk_z z)\times \quad (7)$$

$$\times\exp\left[-j\beta\left[(x'-x)\cos a + (y'-y)\sin a\right]\beta\,d\beta\,da.\right.$$

Составляющие электрического поля в раскрыве при $z = 0$ для волны типа H_{10} имеют следующий вид:

$$E_y(x',y',0) = -\frac{jZ_0 ak}{\pi}\sin\left(\frac{\pi x'}{a}\right), \quad (8)$$

где Z_0 – волновое сопротивление свободного пространства.

Выражение $E_y^{(2)}$ для второй среды при известных функциях $F_y^{(2)}$ определяют поле излучения через теплозащиту прямоугольного волновода через касательные составляющие электрического поля в раскрыве волновода [16,17].

Рассмотрим некоторые наиболее характерные случаи изменения относительной диэлектрической проницаемости диэлектрической теплозащитной вставки в направлении оси *Z*. Возможные законы изменения определяются температурной стабильностью параметров диэлектрика и законом изменения температуры в направлении нормали к поверхности нагрева [18]. Рассмотрим наиболее вероятные зависимости - экспоненциальную и линейную. Для этих случаев и конкретизируем полученные выражения функций *A, B* и *C* и перейдем к нахождению математических зависимостей радиотехнических характеристик антенного окна. Для закона $\mathcal{E}_1(z) = \mathcal{E}_1(0)\exp(\gamma z)$ получаем

$$k_{z_1}(z) = \sqrt{k^2\varepsilon_1(0)(1+\alpha z) - k_x^2 - k_y^2},.$$

Для линейного закона изменения диэлектрической проницаемости

Интеграл F можно рассматривать как сумму трех интегралов

$$F = \frac{1}{2\pi}\int_l \ldots d\beta + U(C_b)\int_{l_в} \ldots d\beta + U(C_p)\int_{l_p} \ldots d\beta, \quad (9)$$

$U(C_{в.р})$ – единичная функция Хевисайда, равная единице при положительных $C_в$ и $C_р$ и нулю – при отрицательных, $C_в$, $C_р$ – величины, определяемые координатами точек ветвления и полюсов.

Первый интеграл выражения (9) по контуру *l* вычисляется методом перевала и определяет поле излучения.

Боковые волны можно определить по результату интегрирования по берегам разрезов, охватывающих точки ветвления. Это можно учесть, вычисляя интегралы (6) и (7) по контуру l_B (9).

Из анализа выражения $F_y^{(2)}$ очевидно, что точки ветвления первого порядка расположены при $\beta_{B1} = \pm k$ и $\beta_{B2} = \pm k\sqrt{\varepsilon_1(d)}$. Из названных точек необходимо в расчете взять точки ветвления с координатами $\beta_2 = \pm\mathrm{k}\sqrt{\varepsilon_1(0)\exp(\gamma d)}$ для экспоненциального закона изменения ε_1 диэлектрической проницаемости по толщине теплозащиты и $\beta_2 = \pm\mathrm{k}\sqrt{\varepsilon_1(0)(1+\alpha d)}$ для линейного закона, чтобы удовлетворять условиям излучения.

Анализ подинтегральных выражений (6) и (7) показал, что разработанные и известные методы асимптотической оценки интегралов по берегам разрезов, охватывающих точки ветвления, справедливые для перевального пути, в данном случае оказываются неприменимыми.

По этой причине определить вклад боковой волны в диаграмму излучения и потери мощности на излучение можно только численным интегрированием (6) и (7) по контуру l_B.

Анализ подинтегральных выражений $F_y^{(1)}$ и $F_y^{(2)}$ показал, что разрез целесообразно выбрать так, чтобы это была прямая, параллельная мнимой оси на комплексной плоскости β. Тогда интеграл (9) по берегам разреза $\int\limits_{l_{B_1}} ...d\beta$ для $F_y^{(1)}$ и $F_y^{(2)}$ примет вид

$$\int\limits_{l_{B_1}} ...d\beta = \frac{1}{4\pi^2}\left(\int\limits_{\mathrm{Re}k+j\infty}^{k} v_1(\beta)d\beta + \int\limits_{k}^{\mathrm{Re}k+j\infty} v_2(\beta)d\beta \right), \qquad (10)$$

где $v_1(\beta)$ и $v_2(\beta)$ – подынтегральное выражение или $F_y^{(1)}$, или $F_y^{(2)}$, отличающееся знаками перед $\sqrt{k^2-\beta^2}$. Аналогично $\int\limits_{l_{B_2}} ...d\beta$ для выражений с экспоненциальным законом изменениями $F_y^{(2)}$ запишется

$$\int\limits_{l_{e2}} ...d\beta = \frac{1}{4\pi^2}\left(\int\limits_{\mathrm{Re}k\sqrt{\varepsilon_1(0)\exp(\gamma d)}+j\infty}^{k\sqrt{\varepsilon_1(0)\exp(\gamma d)}} \eta_1(\beta) + \int\limits_{k\sqrt{\varepsilon_1(0)\exp(\gamma d)}}^{\mathrm{Re}k\sqrt{\varepsilon_1(0)\exp(\gamma d)}+j\infty} \eta_2(\beta) \right), \quad (11)$$

где $\eta_1(\beta)$ и $\eta_2(\beta)$ – подынтегральное выражение или $F_y^{(1)}$, или , для экспоненциального закона изменения, отличающееся знаками перед $\sqrt{k^2\varepsilon_1(0)\exp(\gamma d) - \beta^2}$. Аналогично получается выражение для линейного закона изменения относительной диэлектрической проницаемости теплозащиты с заменой пределов интегрирования

$$\int\limits_{l_{e2}} ...d\beta = \frac{1}{4\pi^2}\left(\int\limits_{\mathrm{Re}k\sqrt{\varepsilon_1(0)(1+\alpha d)}+j\infty}^{k\sqrt{\varepsilon_1(0)(1+\alpha d)}} \eta_1(\beta) + \int\limits_{k\sqrt{\varepsilon_1(0)(1+\alpha d)}}^{\mathrm{Re}k\sqrt{\varepsilon_1(0)(1+\alpha d)}+j\infty} \eta_2(\beta) \right).$$

Соотношения (10) и (11) необходимы для последующей подстановки в (5) с целью определения поля $E_{y,бок}^{(1,2)}$ ли $E_{y,бок.изл}^{(1,2)}$. Расчет $E_{y,бок}^{(1,2)}$ производится по (10), (11) без множителей в виде функции Хевисайда.

Расчет показывает, что $C_B > 0$ для всех точек ветвления, пересекаемых перевальным путем, за исключением случая, когда ε_1 – комплексна и потери в теплозащите достаточно велики ($tg\delta > 0{,}5$), что может иметь место при интенсивном нагреве теплозащиты.

В результате имеем влияние боковых волн на излучение прямоугольного волновода в дальней зоне [19].

Таким образом, вклад боковых волн в мощность излучения может стать заметным при достаточно интенсивном нагреве теплозащиты.

Потери излучаемой мощности на боковые волны можно оценить соотношением

$$\psi = \frac{P_{бок} - P_{бок.изл}}{P_{пад}},$$

где $P_{бок}$, $P_{пад}$ – мощности боковых волн и падающей (подводимой к излучателю), $P_{бок.изл}$ – мощность боковых волн, излученных в дальнюю зону.

Третий интеграл (8) находится по теореме Коши из расположения полюсов подинтегральной функции и определяет поверхностные и вытекающие волны [20].

Излучаемая мощность для дальней зоны может быть рассчитана по следующему выражению

$$P_{изл} = \frac{1}{2Z_0}\int\limits_0^{\pi/2}\int\limits_0^{2\pi}\left(|E_\theta|^2 + |E_\varphi|^2\right) r^2 \sin\theta d\theta d\varphi, \qquad (12)$$

где

$$r = \sqrt{z^2 + (x'-x)^2 + (y'-y)^2}.$$

Для прямоугольного волновода с волной H_{10} имеем [3]

$$P_{пад} = Z_0 H_0^2 \frac{ba^3}{\lambda^2}\sqrt{1-(\lambda/2a)^2}, \qquad (13)$$

где H_0 – амплитуда, определяемая мощностью источника поля.

КПД исследуемой антенны определяется уравнениями (12) и (13), и рассчитывается как

$$\eta = P_{изл} / P_{пад}.$$

Заключение

Расчет по разработанным математическим моделям диаграммы направленности и КПД бортовых антенн, защищенных неоднородным слоем теплозащиты, базируется на известных температурных зависимостях теплозащиты. Температурные зависимости определяются видом теплозащиты антенны, а значение температуры траекторией полета. Для численного расчета необходимо знать закон изменения диэлектрической проницаемости по толщине теплозащиты, её толщину, размеры излучающего волновода, длину волны на которой производятся исследования.

Полученные модели и результаты численных расчетов по ним определяют время потери радиосвязи на траектории спуска и позволяют разработать рекомендации по уменьшению или устранению потери радиосвязи.

Литература

1. *Sharma A.K., Kumar A.* Nonlinear gain of a millimetre wave antenna array mounted on a re-entry vehicle // Journal of Physics D: Applied Physics. 2007. Vol. 40. No. 7, pp. 2033-2036.

2. *Liu Y., Li H., Li Y.* et al. Transmission properties and physical mechanisms of X-ray communication for blackout mitigation during spacecraft reentry. 2017. Vol. 24, No. 11. P. 113507. DOI 10.1063/1.4998786.

3. *Liu Z., Bao W., Li X.* et al. Influence of plasma pressure fluctuation on RF wave propagation // Plasma Science and Technology. 2016. Vol. 18, No. 2, pp. 131-137. DOI 10.1088/1009-0630/18/2/06

4. *He G., Zhan Y., Ge N.* Adaptive transmission method for alleviating the radio blackout problem // Progress in Electromagnetics Research. 2015. Vol. 152, pp. 127-136. DOI 10.2528/PIER15072702

5. *Takahashi Y., Enoki N., Takasawa H., Oshima N.* Surface catalysis effects on mitigation of radio frequency blackout in orbital reentry // 2020. Vol. 53. No. 23. P. 235203. DOI 10.1088/1361-6463/ab79e0

6. *Meseguer J., Perez-Grande I., Sanz-Andres A.* Thermal protection systems. Spacecraft Thermal Control, 2012, pp. 305-325.

7. *Михайлов В.Ф., Победоносцев К.А., Брагин И.В.* Прогнозирование эксплуатационных характеристик антенн с теплозащитой. СПб.: Судостроение. 1994. 300 с.

8. *Михайлов В.Ф.* Характеристики излучения круглого волновода через плоскую однородную теплозащиту // Электромагнитные волны и электронные системы. 2019. №1. С. 12-19.

9. *Mikhailov V.F.* Characteristics of radiation of a round waveguides through a flat homogeneousheat shield. Propagation and Wave- guides in Photonics and Microwave Engineering. London, United Kingdom. 2020, pp. 167-173.

10. *Михайлов В.Ф.* Радиотехнические характеристики бортовой антенны с учетом поверхностных волн // Волновая электроника и инфокоммуникационные системы : Материалы XXIV Международной научной конференции. Часть 2. Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2021.

11. *Михайлов В.Ф., Мажник И.В.* Влияние боковых волн на радиотехнические характеристики прямоугольного волновода с теплозащитой // Волновая электроника и инфокоммуникационные системы: Материалы XXV Международной научной конференции. Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2022. С. 193-198.

12. *Бреховских Л.М.* Волны в слоистых средах. М.: Изд-во АН СССР, 1957. 215 с.

13. *Альперт Я.А* Распространение радиоволн. М.: Наука, 1972. 564 стр.

14. *Виноградов М.В., Руденко С.В., Сухоруков А.П.* Теория волн. М.: Наука, 1979. 383 с.

15. *Collin E.R.* Foundations for Microwave Engineering, 2nd Edition. Wiley-IEEE Press, 2001, pp. 194-197.

16. *Малых М.Д.* Разработка методов численного анализа закрытых электромагнитных волноводов. Дисс. … докт. физ.-мат. наук. М. 2018. 215 с.

17. *Архангельский Ю.С., Огурцов К.Н.* Высокотемпературный нагрев диэлектриков с фазовыми переходами // Вестник Саратовского государственного технического университета. 2012. Т. 2. № 2(66). С. 34-37.

18. *Заргано Г.Ф., Земляков В.В., Кривопустенко В.В.* Электродинамический анализ собственных волн в прямоугольном волноводе с двумя выступами // Радиотехника и электроника. 2011. Т. 56. № 3. С. 285-294.

19. Программа расчёта поля излучения боковых волн прямоугольного волновода с теплозащитой : № 2022615308 : заявл. 31.03.2022 : опубл. 31.03.2022 / И. В. Мажник, В. Ф. Михайлов ; заявитель ФГАОУ ВО ГУАП.

20. Программа расчёта потерь энергии на поверхностные волны в теплозащите прямоугольного волновода : № 2021668773 : заявл. 25.11.2021 : опубл. 25.11.2021 / И. В. Мажник, В. Ф. Михайлов ; заявитель ФГАОУ ВО ГУАП.

INFLUENCE OF INHOMOGENEOUS THERMAL PROTECTION ON THE RADIATION CHARACTERISTICS OF A SPACECRAFT ANTENNA

VIKTOR F. MIKHAILOV
St. Petersburg, Russia, vmikhailov@pochta.tvoe.tv

ILYA V. MAZHNIK
St. Petersburg, Russia, ilya.mazhnik@yandex.ru

KEYWORDS: *rectangular waveguide; heterogeneous thermal protection; WKB method; radiation pattern, efficiency*

ABSTRACT

Introduction: Knowledge of the electrical characteristics of the onboard antenna on the trajectory of the descent of the spacecraft makes it possible to assess the presence or absence of radio communication. Under conditions of aerodynamic heating, the thermal protection of the onboard antenna heats up unevenly in thickness and becomes electrically inhomogeneous. **Purpose of the work:** Determination of the radio technical characteristics of the onboard antennas of the returning spacecraft with the effect of high-temperature heating on the thermal protection of the antenna based on calculations using the developed mathematical model of the antenna with thermal protection. **Methods:** Expressions for the structure of the radiation field of a rectangular waveguide under the above conditions were derived by the WKB method. Of the well-known analytical methods of solution, it is possible to use the method of integral transformations and the method of eigenfunctions. Both of these methods were used in this work. Results: The obtained theoretical results are new, they allow predicting the radio technical characteristics of the onboard antenna, taking into account uneven heating across the thickness of the thermal protection at low temperature gradients. A mathematical model of the spacecraft's onboard antenna on the descent trajectory has been developed, taking into account the inhomogeneity of thermal protection under conditions of aerodynamic heating. **Practical significance:** The development of a mathematical model of the main radio technical characteristics of onboard antennas, taking into account the impact of high-temperature aerodynamic heating, as well as the results of numerical calculations, can be applied in the development of recommendations for choosing thermal protection and recommendations for reducing the effect of temperature changes in the electrical parameters of thermal protection on the characteristics of onboard antennas and reducing time loss of radio communication or loss recovery.

REFERENCES

1. A. K. Sharma, A. Kumar (2007). Nonlinear gain of a millimetre wave antenna array mounted on a re-entry vehicle. *Journal of Physics D: Applied Physics.* -Vol. 40, No. 7, pp. 2033-2036

2. Y. Liu, H. Li, Y. Li et al. (2017). Transmission properties and physical mechanisms of X-ray communication for blackout mitigation during spacecraft reentry. Vol. 24, No. 11, pp. 113507. DOII 10.1063/1.4998786.

3. Y. Liu, H. Li, Y. Li et al. (2016). Influence of plasma pressure fluctuation on RF wave propagation. *Plasma Science and Technology*. Vol. 18, No. 2, pp. 131-137. DOI 10.1088/1009-0630/18/2/06

4. G. He, Y. Zhan, N. Ge (2015). Adaptive transmission method for alleviating the radio blackout problem. *Progress in Electromagnetics Research*. Vol. 152, pp. 127-136. DOI 10.2528/PIER15072702

5. Y. Takahashi, N. Enoki, H. Takasawa, N. Oshima (2020). Surface catalysis effects on mitigation of radio frequency blackout in orbital reentry. Vol. 53, No. 23, pp. 235203. DOI 10.1088/1361-6463/ab79e0

6. J. Meseguer, I. Perez-Grande, A. Sanz-Andres (2012). Thermal protection systems. *Spacecraft Thermal Control,* pp. 305-325.

7. V.F. Mikhailov, K.A. Pobedonostsev, I.V. Bragin (1994). Forecasting the performance characteristics of antennas with thermal protection. St. Petersburg: Shipbuilding. 300 p.

8. V.F. Mikhailov (2019). Radiation characteristics of a round waveguide through a flat homogeneous heat shield. *Electromagnetic waves and electronic systems.* No. 1, pp. 12-19.

9. V.F. Mikhailov (2020). Characteristics of radiation of a round waveguides through a flat homogeneousheat shield. *Propagation and Waveguides in Photonics and Microwave Engineering*. London, United kingdom, pp. 167-173.

10. V.F. Mikhailov (2021). Radio technical characteristics of the onboard antenna taking into account surface waves. *Wave electronics and infocommunication systems: Proceedings of the XXIV International Scientific Conference.* Part 2. St. Petersburg: St. Petersburg State University of Aerospace Instrumentation.

11. V.F. Mikhailov, I. V. Mazhnik (2022). Influence of lateral waves on the radio technical characteristics of a rectangular waveguide with thermal protection. *Wave electronics and infocommunication systems: Proceedings of the XXV International scientific conference*, St. Petersburg: St. Petersburg State University of Aerospace Instrumentation, pp. 193-198.

12. L.M. Brekhovskikh. (1957). Waves in Layered Media. Moscow: Publishing House of the Academy of Sciences of the USSR. 215 p.

13. A. Ya.A (1972). Alpert Propagation of radio waves. Moscow: Nauka, 564 p.

14. M. V. Vinogradov, S. V. Rudenko, A. P. Sukhorukov (1979). Acoust. Wave theory. Moscow: Nauka. 383 p.

15. E.R.Collin (2001). Foundations for Microwave Engineering, 2nd Edition. Wiley-IEEE Press, pp. 194-197.

16. M.D.Malykh (2018). Development of methods for numerical analysis of closed electromagnetic waveguides. Diss. ... doc. Phys.-Math. Sciences. Moscow. 215 p.

17. Yu. S. Arkhangelsky, K. N. Ogurtsov (2012). High-temperature heating of dielectrics with phase transitions. *Bulletin of the Saratov State Technical University*. Vol. 2, No. 2 (66), pp. 34-37.

18. G.F. Zargano, V.V Zemlyakov, V.V. Krivopustenko (2011). Electrodynamic analysis of eigenwaves in a rectangular waveguide with two projections. *Radiotekhnika i elektronika*. Vol. 56. No. 3, pp. 285-294.

19. Program for calculating the radiation field of side waves of a rectangular waveguide with thermal protection: No. 2022615308: Appl. 03/31/2022 : publ. March 31, 2022 / I. V. Mazhnik, V. F. Mikhailov; applicant FGAOU VO GUAP".

20. Program for calculating energy losses due to surface waves in the thermal protection of a rectangular waveguide: No. 2021668773: Appl. 11/25/2021 : publ. November 25, 2021 / I. V. Mazhnik, V. F. Mikhailov; applicant FGAOU VO GUAP

INFORMATION ABOUT AUTHORS:

V.F. Mikhailov, PhD, professor, St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia, ikhailov@pochta.tvoe.tv

I.V. Mazhnik, student, St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia, ilya.mazhnik@yandex.ru

For citation: Mikhailov V.F., Mazhnik I.V. Influence of inhomogeneous thermal protection on the radiation characteristics of a spacecraft antenna. *H&ES Reserch*. 2023. Vol. 15. No. 3. P. 4-10. doi: 10.36724/2409-5419-2023-15-3-4-10 (In Rus)

doi: 10.36724/2409-5419-2022-15-3-11-19

СЕТЕВАЯ МОДЕЛЬ ДЛЯ УПРАВЛЕНИЯ ДВИЖЕНИЕМ ВОЗДУШНОГО СУДНА ПО ЛОГИСТИЧЕСКИМ МАРШРУТАМ

КОЗЛОВ
Сергей Витальевич [1]

КУБАНКОВ
Александр Николаевич [2]

ШАБАНОВ
Александр Петрович [3]

АННОТАЦИЯ

Введение: Предметной областью являются логистические процессы в системах технической эксплуатации на предприятиях наукоемких производств электронной, машиностроительной и других отраслей экономики, чьи изделия и их компоненты используются в эксплуатируемых авиационных технических системах и аппаратах. Настоящая работа посвящена исследованию вопросов использования беспилотных воздушных судов в логистических процессах для транспортировки изделий и их компонентов, которым требуется ремонт, техническое обслуживание, модернизация или внедрение новых версий программ и интегральных схем. **Цель работы:** Для обеспечения непрерывности управления движением воздушного судна в условиях сильного негативного влияния аддитивных помех, мультипликативных возмущений и других противодействующих процессов на отдельных участках в сети логистических маршрутов решается задача о разработке новой модели управления движением воздушного судна. Целеполаганием данной модели является воспроизводство и исполнение в реальном масштабе времени команды о недопущении перерыва в управлении движением воздушного судна, обусловленного негативным влиянием противодействующих процессов. Проведен научно-патентный поиск и определены наиболее близкие к разрабатываемой модели и наукоемкие аналоги. Поиск производился на массиве опубликованных в 2018-2023 годы статей, изобретений, программ для ЭВМ и баз данных, относящихся к исследуемой теме. **Научным результатом исследования** является разработанная сетевая процессная модель для управления движением воздушного судна в логистических маршрутах, которая обладает новизной и обеспечивает решение поставленной задачи. Главный эффект от применения новой сетевой модели заключается в обеспечении непрерывности управления движением воздушного судна в условиях противодействующих процессов в сети логистических маршрутов. Предлагаемое научно-техническое решение может быть интересным для руководителей предприятий, научных сотрудников и инженеров в других предметных областях, в которых используются логистические процессы и беспилотные транспортные системы.

КЛЮЧЕВЫЕ СЛОВА: *система технической эксплуатации изделий, логистический процесс, управление движением воздушного судна, передача данных*

Сведения об авторах:

[1] к.т.н, с.н.с., руководитель отделения, Федеральный исследовательский центр "Информатика и управление" РАН, . Москва, Россия, skozlov@ipiran.ru

[2] д.в.н., профессор, заведующий кафедрой, Московский технический университет связи и информатики, Москва, Россия, a.n.kubankov@mtuci.ru

[3] д.т.н., с.н.с., ведущий научный сотрудник, Федеральный исследовательский центр "Информатика и управление" РАН, Москва, Россия, apshabanov@mail.ru

Для цитирования: *Козлов С.В., Кубанков А.Н., Шабанов А.П.* Сетевая модель для управления движением воздушного судна по логистическим маршрутам // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 3. С. 11-19. doi: 10.36724/2409-5419-2023-15-3-11-19

Введение

Одним из наиболее эффективных инструментов при проведении проектов по производству высокотехнологичных изделий является структурный анализ методов, моделей и объектов интеллектуальной собственности – изобретений, программ для ЭВМ и баз данных, проводимый на основе модуля для принятия решений, построенного по технологии сетевого управления [1]. В настоящем исследовании этот инструмент применён к *предметной области* по управлению движением воздушных судов в логистических маршрутах систем технической эксплуатации авиастроительных корпораций и их партнеров – предприятий наукоемких производств электронной, машиностроительной и других отраслей экономики, чьи изделия и их компоненты используются в эксплуатируемых авиационных технических системах и аппаратах.

Направление настоящего исследования относится к направлению научно-технологического развития России, в котором решаются задачи по формированию эффективной системы коммуникации в области науки, технологий и внедрения инноваций [2]. В этом направлении существует ряд авторских научно-технических решений для высокотехнологичных и наукоемких производств, которые опубликованы в работах [3-6] и являются заделом для настоящего исследования. Например, инновационное решение, которое создано в исследовательской работе [6], обеспечивает повышенную скрытность факта передачи данных на борт роботизированного объекта и данных контроля в обратном направлении при заданных значениях параметров своевременности представления информации, и является аналогом научно-технического решения, представленного в статье.

Используется терминология, которая присуща документам федеральных проектов «Информационная инфраструктура», «Цифровые технологии», «Цифровое государственное управление», Программа фундаментальных научных исследований в Российской Федерации на долгосрочный период (2021 - 2030 годы), и нормативным документам, относящимся к области беспилотных авиационных систем и логистических процессов. Важными смысловыми технологическими сущностями, которые положены в основание для создания нового научно-технического решения являются следующие сущности.

– Интегрированная логистическая поддержка, как совокупность логистических процессов, осуществляемых Разработчиками изделий авиастроительной промышленности и их партнерами совместно с Эксплуатантами и другими участниками жизненного цикла изделий, и направленных на формирование системы технической эксплуатации, обеспечивающей эффективное использование изделий при приемлемой стоимости их жизненных циклов.

– База данных, в которой размещаются структурированные и взаимосвязанные данные о цифровых моделях, построенных для процесса управления движением воздушного судна в сети логистических маршрутов. Примеры данных: значения параметров $N_1\{n1i\}$, i=1, 2, …, N_1 каналов связи между наземными объектами и воздушным судном; команды $S[\Delta C_{2j}(t, i, j)]$, i=1, 2, …, N_1, j=1, 2, …, C^2 управления, предназначенные для изменения значений параметров $N_1\{n_{1i}\}$ в зависимости от уровня негативного влияния противодействующих процессов.

– Сетевое управление, как одна из практик информационных технологий, которая обеспечивает автоматическое воспроизведение управляющего воздействия на бортовой механизм управления движением воздушного судна вследствие изменения значений параметров, записанных в базе данных. Примером такого изменения являются данные об условии $Y[\Delta C_{2j}(t, i, j)]=\{u(t, i, j)\}$, при наступлении которого применяется команда $S[\Delta C_{2j}(t, i, j]$ управления, в соответствии с которой изменяются установленные значения параметров $M_1\{n_{1i}\}$ на значения $M_1\{n_{1i}^*\}$ в соответствии с указанным выше условием. Следствием такого изменения является выполнение операций воздействия на бортовые механизмы управления с целью изменения режима движения, например решение [6], или изменения направления движения в сети логистических маршрутов, например решение [7], или изменения структуры сети логистических маршрутов [8].

В статье, последовательно рассматриваются следующие процессы настоящего исследования.

– Формулирование научной задачи о разработке научно-технического решения и обоснование актуальности его применения в логистических процессах с использованием беспилотных воздушных судов для транспортировки изделий технических систем, которым требуется ремонт, техническое обслуживание, модернизация и внедрение инновационных решений.

– Проведение научно-патентного поиска научно-технических решений, разработанных в 2018 – 2023 гг. в которых используются технологии сетевого управления, производство анализа и определение отличительных функций нового научно-технического решения – сетевой модели управления движением воздушного судна.

Структуризация отличительных функций сетевой модели управления движением воздушного судна.

В заключение приводится оценка научного результата, характеризуется положительные свойства новой модели управления движением беспилотных воздушных судов в логистических процессах систем технической эксплуатации авиастроительных корпораций, в перспективе в других отраслях экономики, государственных сферах.

Постановка задачи. Требования к решению

На основании задела, сформированного в результате проведения исследовательских работ [1, 3-6] по созданию новых инновационных решений с применением технологий сетевого управления, и выбранного направления по исследованию процессов управления движением воздушных судов в логистических маршрутах систем технической эксплуатации авиастроительных корпораций и их партнеров сформулирована *научная задача* о разработке новой сетевой модели для управления движением беспилотного воздушного судна в сети логистических маршрутов (далее по тексту, модель управления движением). Определены следующее функциональные требования к данной модели.

1. Модель должна обеспечивать воспроизводство и исполнение в реальном масштабе времени команд о недопущении перерыва в управлении движением воздушного судна, обусловленного сильным негативным влиянием аддитивных помех, мультипликативных возмущений и других противодействующих процессов на связь в отдельных участках сети логистических маршрутов

2. Модель должна быть цифровой, размещаться в базе C_1 данных системы технической эксплуатации Разработчика или в базе данных внешнего предприятия-партнера, предоставляющего соответствующие услуги, например в Модуле принятия решений по интеллектуальной поддержке наукоемких производств [1, рис. 2] в составе Цифровой платформы поддержки процессов организационных систем [5, рис. 4].

3. Параметры модели должны быть привязаны к параметрам цифровой карты, включая:

– координаты центров технического обслуживания и промышленных предприятий Разработчиков изделий, складов Эксплуатантов с изделиями, ожидающими транспортировку для проведения ремонта, технического обслуживания, внедрения новых компонентов, замену или утилизацию, площадок и аэродромов для базирования воздушных судов вертолётного и самолётного типов, используемых для транспортировки изделий по назначению;

– информацию дополненной реальности о допустимых и фактических значениях параметров электромагнитного излучения [9] в зонах мониторинга пунктов контроля над внешней средой, установленных в центрах технического обслуживания и промышленных предприятиях Разработчиков изделий, в складах Эксплуатантов и в местах базирования воздушных судов;

4. С целью сокращения времени на создание модели и её промышленного освоения в состав её компонентов могут входить известные научно-технические решения, которые используют технологии сетевого управления.

5. Должен быть произведён научный и патентный поиск таких решений по материалам научных библиотек и патентных ведомств.

Актуальность применения новой модели для управления движением беспилотных воздушных судов в логистических процессах обусловлена поддержкой государства с целью широкого использования и развития этих систем в ближайшей перспективе на основе наукоемких технологий, включая сквозные информационные технологии [10]. Это подтверждается следующими факторами.

1. Новым концептуальным подходом к интеграции беспилотных воздушных судов в единое воздушное пространство Российской Федерации [11] в 3 этапа – организационный в 2023 г., технологический – до 2027 г. и цифровой – до 2030 г.

2. Государственной поддержкой развития авиатранспортной отрасли Российской Федерации до 2030 г., в части разработки, испытаний и внедрения цифровых инноваций для проектирования, промышленного изготовления и эксплуатации беспилотных воздушных судов, аттестации, логистических услуг и обслуживания (http://government.ru/docs/all/141773/, http://government.ru/docs/all/139820/).

3. Созданием и поэтапной корректировкой в 2013 – 2020 годах Федерального государственного образовательного стандарта среднего профессионального образования по специальности «Эксплуатация беспилотных авиационных систем» для подготовки специалистов в отраслях экономики, сферах безопасности и государственного управления (https://www.consultant.ru/document/cons_doc_LAW_210830/).

4. Необходимостью технологического обеспечения методологии для комплексного транспортного планирования на глобальном, национальном и региональном уровнях, в особенности на территориях с меняющейся геополитической обстановкой, и тем самым повышением востребованности транспортных услуг, управления цепочками поставок [12].

5. Тенденциями к росту числа технических изделий, которым требуется ремонт, а также к росту числа научно-прикладных и технических решений, следствием которых является рост числа новых или усовершенствованных, в том числе эксплуатируемых, изделий и их компонентов. Данные тенденции способствуют росту логистических услуг и обусловлены следующими обстоятельствами:

– повторяющимися нештатными ситуациями в работе изделий, что свидетельствуют о наличии в них скрытых проблем;

– отставанием технических решений (изобретений, программ для ЭВМ, баз данных, топологий интегральных микросхем, решений “ноу-хау”), лежащих в основе функционирования транспортируемого изделия, от мировых аналогов, что может привести к отставанию от конкурентов в предпринимательстве и в сферах государственного управления;

– недостаточной автоматизацией действий, выполняемых с транспортируемым изделием, что увеличивает или срывает сроки выполнения соответствующего технологического или управляющего процессов.

Использование новой модели для управления движением беспилотных воздушных судов, в принципе является экономичной процедурой для логистических процессов в системах технической эксплуатации авиастроительных корпораций, например [13, 14]. Это обусловлено тем, что эти корпорации:

– обладают большим числом центров технического обслуживания и промышленных предприятий по производству изделий и компонентов для авиационной техники;

– имеют многочисленные взаимные договорными обязательства с партнерами в области производства и технической эксплуатации изделий, которые используются на борту воздушных судов и в службах по их техническому информационному, навигационному обслуживанию, которые предназначены для обеспечения других видов деятельности, осуществляемой с помощью авиационной техники.

Данные обстоятельства указывают на то, что объем технических изделий в организационных системах авиастроительной промышленности и их партнеров, является достаточным с точки зрения окупаемости финансовых средств, выделяемых для транспортировки изделий, которые эти же организационные системы и произвели, и будут осуществлять их ремонт, техническое обслуживание, модернизацию и замену в них программ и интегральных схем.

В течение ближайших лет новая модель управления движением воздушных судов способна обеспечить повышение эффективности технической эксплуатации для предприятий и других отраслей экономики.

Эффект достигается за счет сокращения времени и стоимости выполнения логистических процессов с применением беспилотных воздушных судов.

В перспективе применение представленной модели можно ожидать в области управления беспилотными воздушными судами в режиме их автономного движения в сети логистических маршрутов.

Научный и патентный поиск инновационных решений с сетевым управлением

Основным, принципиальным требованием, которое предъявляется к перспективному научно-техническому решению мирового уровня, что соответствует патенту на изобретение, является его новизна, полезность для области применения и реализуемость на практике (https://www1.fips.ru/about/tspti-tsentr-podderzhki-tekhnologiy-i-innovatsii/perspektivnye-izobreteniya.php?sphrase_id=647).

Ориентируясь на это утверждение проведен научный и патентный поиск инновационных технических решений, сведения о которых опубликованы в 2018 – 2022 годах, и в которых используются технологии сетевого управления с применением баз данных, структурированных по семантическим признакам взаимосвязанных сущностей.

Задачей поиска являлось определение научных и технических решений, которые можно использовать в составе новой модели управления движением воздушного судна или использовать в качестве аналогов для создания новых автоматизированных функций и средств для их реализации в составе этой модели. Такой подход позволяет сократить время на разработку данной модели, сосредоточив при этом внимание на реализацию ее отличительных свойств.

Поиск проводился в разделах международных баз данных – «Information Systems», «Computer Networks and Communications», «Electrical and Electronic Engineering», «Cognitive Neuroscience», и в разделах российских баз данных – «Информатика», «Автоматика и Вычислительная техника», «Организация и Управление». В качестве ключевых слов использованы названия основных сущностей, которые задействуются при использовании технологий сетевого управления, соответственно – «network», «engineering», «neuroscience», «информационная система», «программа», «обработка данных», «процесс», «сеть».

Основные источники информации, использованные при поиске:

– Федеральный институт промышленной собственности (https://www1.fips.ru) с массивом данных на условиях поиска публикаций об изобретениях, полезных моделях, программах для ЭВМ, базах данных;

– Электронная научная библиотека (https://elibrary.ru/) с массивом данных на условиях поиска публикаций о научных статьях, монографиях, материалах конференций, диссертаций, отчетов, патентов;

– База данных «Scopus» о научных публикациях (https://www.scopus.com/home.uri) с массивом данных на условиях поиска.

В результате проведения научно-патентного поиска отобраны публикации о научно-технических решениях, которые достаточно близки к исследуемой теме. Примеры таких публикаций:

– научные публикации о методах, моделях и инновационных решениях, относящихся к логистическим процессам с применением беспилотных авиационных систем [15, 16], к элементам беспилотных авиационных систем [17-19], к технологиям управления процессами, большими данными и жизненным циклом изделий [20-24], к разработке инновационных решений на основе цифровых платформ коллективного пользования [25-27], к формированию маршрутов [28], мониторингу, контролю и оценки уровней электромагнитного излучения [29, 30];

– описания патентов на изобретения [31-35] и программ для ЭВМ, баз данных [36-40].

На основании проведенного анализа известных научных и технических решений определен методический подход к процессу комплексного структурирования в новой модели управления движением воздушного судна известных и новых функций и средств для их реализации.

Суть методического подхода к исследованию отражает следующее утверждение:

«Не изобретай, что уже изобретено» – концентрация усилий создателей инновационного решения на выполнении работ по построению новых функций $F_{new}\{f_{ni}\}$ и на использовании данных о значениях параметров f_{wk}, которые присущи при выполнении известных функций $F_{wk}\{f_{wi}\}$.

Такой подход обеспечивает сокращение сроков T_{work} и расходов S_{work} при выполнении работ по построению модели управления движением воздушного судна, по созданию на основе модели инновационного научно-технического решения и по внедрению его в инфраструктуры предприятий-заказчиков проекта:

$$F_{new}\{f_{ni}\} \cap F_{wk}\{f_{wi}\} \rightarrow T_{work} \rightarrow S_{work}.$$

Модель для управления движением воздушного судна

Новая модель для управления движением разработана как типовое решение. При внедрении модели в инфраструктуру конкретной системы технической эксплуатации типовое решение должно быть адаптировано под потребности этой системы с его привязкой к системам навигации, компьютерного зрения и другим системам, в которых воспроизводятся процессы передачи данных с наземных объектов на борт воздушного судна и обратно.

Применяя указанный выше методический подход к процессу комплексного построения новой модели, определена её следующая функциональная структура.

На этапе подготовки воздушного судна к транспортировке изделий.

Электронная модель для управления движением воздушного судна создается на основе цифровой карты в базе C_1 данных, размещенной в инфраструктуре системы технической эксплуатации Разработчика. При этом выполняют следующие функции.

1. $F_1(C_0, C_1, C_{3i}, C_4)$ – в цифровой карте маркируют координаты местоположения:

– склада (складов) C_0 изделий Эксплуатанта, которым требуется транспортировка;

– вычислительного комплекса, в котором размещена база C_1 данных;

– центров технического обслуживания и промышленных предприятий C_{3i} Разработчика, в которых размещены пункты C_{2j} контроля над внешней средой, предназначенные для мониторинга состояния электромагнитного излучения;

– беспилотного воздушного судна $C_4\{N_4\}$, предназначенного для транспортировки изделий с параметрами $N_4=\{n_{4i}\}$.

Технические решения для реализации функции $F_1(C_0, C_1, C_{3i}, C_4)$ общеизвестны и не требуют выполнения сложных операций.

2. $F_2(C_0, C_1, C_{3i}, C_{4i}, C_{5i})$ – на основании данных о местоположении объектов (C_0, C_1, C_{3i}, C_{4i}) и данных о закреплении изделий $C_5\{n_{5i}\}$ для технического обслуживания за конкретными центрами и промышленными предприятиями $C_3\{m_{3i}\}$ в цифровой карте формируют сеть $C_6\{n_{6i}\}$ логистических маршрутов для доставки изделий со склада C_0 в предназначенные для них центры технического обслуживания и промышленные предприятия C_{3i}: $C_3\{n_{3i}\} \cap C_5\{n_{6i}\} \rightarrow C_6\{n_{5i}\}$.

Технические решения для реализации функции $F_2(C_0, C_1, C_{3i}, C_{4i}, C_{5i})$ известны, например [41, 42].

3. $F_3(C_4\{n_{4i}\})$ – в разделе цифровой карты с координатами местоположения воздушного судна размещают данные дополненной реальности, которые привязаны к интервалу времени ΔT_0 подготовки воздушного судна к транспортировке изделий, включая данные:

– о значении параметров $N_{1j}\{n_{1i}\}$, i=1, 2, …, N_j^1 каналов связи в зонах ΔC_{2j} мониторинга пунктов C_{2j} контроля, при этом значения параметров $N_{1j}\{n_{1i}\}$ определяются в зависимости от значений параметров $N_{2j}(\Delta T_{0j}, \{|n_{2j}|\})$ электромагнитных излучений и других противодействующих процессов и явлений, мониторинг которых производился в интервале времени ΔT_{0j} подготовки воздушного судна к движению по маршруту для каждой зоны ΔC_{2j} мониторинга;

– о командах $S[\Delta C_{2j}(t, i, j)]$, i=1, 2, …, N^1, j=1, 2, …, C^2, управления, предназначенные для изменения параметров каналов связи во время транспортировки воздушным судном изделий в зависимости от степени негативного влияния противодействующих процессов.

Во время транспортировки изделий инициация команд управления на борту воздушного судна осуществляется при изменении значений параметров $N_1\{n_{1i}\}$ канала связи, что происходит вследствие поступления на борт судна управляющих воздействий от пунктов C_{2j} контроля над внешней средой при возникновении таких уровней влияния противодействующих процессов в зонах ΔC_{2j} их мониторинга, которые не были предусмотрены в интервале времени ΔT_0 подготовки воздушного судна к транспортировке изделий.

4. $F_4(C_{2j}, C_{3i})$ – в цифровой карте маркируют координаты местоположения каждого пункта C_{2j} контроля над внешней средой, как координаты того центра технического обслуживания или промышленного предприятия C_{3i}, в котором они размещаются, и определяют зоны ΔC_{2j} для мониторинга внешней среды. В пунктах C_{2j} контроля над внешней средой размещают:

– устройства контроля значений параметров $N_{2j}\{n_{2j}\}$ внешних электромагнитных излучений и других противодействующих процессов в зонах ΔC_{2j};

– устройства трансформации этих значений параметров в данные;

– устройства обработки данных о значениях параметров $N_{2j}\{n_{2j}\}$.

Структурированные данные о значениях параметров $N_{2j}\{n_{2j}\}$ записывают, как дополненную реальность, в соответствующие разделы C_{2j} цифровой карты.

5. $F_5(C_{2j}, C_4)$ – в разделах цифровой карты, в которых размещены координаты местоположения пунктов C_{2j} контроля, размещают данные дополненной реальности, которые привязаны к интервалу времени ΔT_0 подготовки воздушного судна к транспортировке изделий, включая следующие данные:

– о значении параметров $N_{1j}\{n_{1ji}\}$, i=1, 2, …, N_j^1 каналов связи в зонах ΔC_{2j} мониторинга пунктов C_{2j} контроля;

– о значении параметров $N_{2j}\{n_{2ji}\}$ внешних электромагнитных излучений и других противодействующих процессов в зонах ΔC_{2j} мониторинга пунктов C_{2j} контроля;

– о командах $S[\Delta C_{2j}(t, i, j)]$, i=1, 2, …, N_j^1, j=1, 2, …, C^2, управления, предназначенные для изменения режимов в каналах связи во время транспортировки воздушным судном изделий в зависимости от степени негативного влияния противодействующих процессов в зонах ΔC_{2j} мониторинга пунктов C_{2j} контроля;

– об условиях $Y[\Delta C_{2j}(t, i, j)]=\{u(t, i, j)\}$, при наступлении которых применяются команды $S[\Delta C_{2j}(t, i, j)]$ управления.

6. $F_6(C_{2j})$ – В пунктах C_{2j} контроля размещают программу для управления движением и устройства для ее реализации, которые обеспечивают автоматическое выполнение функций по управлению движением на этапе транспортировки изделий.

7. $F_7(C_1, C_{2j}, C_4)$ – Записывают копии разделов цифровой карты, которые содержат:

– данные о реальных значениях параметров и данные дополненной реальности для пунктов C_{2j} контроля;

– данные о реальных значениях параметров и данные дополненной реальности воздушного судна C_4 из состава беспилотной авиационной системы в его бортовой вычислительный комплекс.

8. $F_8(C_1, C_{2j}, C_4)$ – Производят привязку – обеспечивают технологическое взаимодействие:

– разделов базы данных, которые размещены в пунктах C_{2j} контроля, с устройствами для реализации программы управления движением, устройствами передачи данных и связи из состава линии управления и контроля, которые размещены в этих станциях;

– раздела базы C_1 данных, который размещен в вычислительном комплексе воздушного судна C_4, с устройствами передачи данных и связи из состава линии управления и контроля, устройствами и программами для управления движением, которые размещены в этом судне.

На этапе транспортировки изделий воздушным судном.

Выполняют следующие функции по управлению движением воздушного судна.

F_9 (C_1, C_{2j},) – В зонах ΔC_{2j} мониторинга и пунктов C_{2j} контроля с помощью средств контроля и обработки данных воспроизводят следующие операции:

– регламентируемый и периодический, через интервал времени ΔT_j, мониторинг значений параметров $N_{2j}\{n_{2j}\}$ внешних электромагнитных излучений и других противодействующих процессов;

– трансформация фактических значений параметров $N_{2j}\{n_{2j}\}$ в данные и размещение этих данных в разделах цифровой карты в соответствующих C_2;

– сравнительный анализ данных мониторинга о фактических значениях параметров $N_{2j}\{n_{2j}\}$, полученных в интервале времени ΔT_j, и данных мониторинга о фактических значениях этих параметров, установленных при подготовке воздушного судна к транспортировке изделий в интервале времени ΔT_0, при котором

$$\forall j \rightarrow N_{2j}(\Delta T_j, \{|n_{2j}|\}) - N_{2j}(\Delta T_{0j}, \{|n_{2j}|\}) = \Delta N_{2j}(\Delta T_j, \{|n_{2j}|\});$$
$$If\ (\Delta T_j, |n_{2j}|) > (\Delta T_{0j}, |n_{2j}|) \cap \Delta N_{2j}(\Delta T_j, \{|n_{2j}|\} > \Delta|n_{2j}|,$$
$$Then \rightarrow F_{10}(C_1, C_{2j}),$$
$$Else \rightarrow F_9\ (C_1, C_{2j},),$$

где $\Delta|m_{2j}|$) – критерии отклонения.

$F_{10}(C_1, C_{2j})$ – формирование в соответствующем пункте C_{2j} контроля команды $S[\Delta C_{2j}(t, i, j)]$ управления, предназначенной для изменения режима канала связи с воздушным судном, которое в интервале времени ΔT_j осуществляет транспортировку изделий, находясь в зоне ΔC_{2j} мониторинга. При этом:

– если в сети логических маршрутов движение воздушного судна должно происходить через зону ΔC_{2j} мониторинга, в которой не зафиксировано сильное влияние противодействующих процессов, то формируется команда управления, следствием выполнения которой является продолжение движения воздушного судна по маршруту, исключающему движение через зону мониторинга, подверженной сильному негативному влиянию противодействующих процессов, например для этого можно использовать техническое решение [7];

– если воздушное судно находится в зоне ΔC_{2j} мониторинга, именно в которой зафиксировано сильное влияние противодействующих процессов, то формируется команда управления, следствием выполнения которой является установление режима канала связи, при котором на борт судна передаются только команды управления движением, реализации которых осуществляется, например в соответствии с инновационными техническими решениями [43, 44]. Отличительной чертой этих решений является обеспечение безусловной скрытности факта передачи данных в канале связи.

С помощью данных команд управления осуществляется переход воздушного судна на обходной маршрут или продолжается его движение в прежнем маршруте, но возможностями передачи данных только о командах управления движением на борт судна и в обратном направлении данных об исполнении этих команд.

Заключение

Проведено исследование об использовании беспилотных воздушных судов в логистических процессах по транспортировке изделий технических систем со складов их Эксплуатантов в центры технического обслуживания и промышленные предприятия Разработчиков этих изделий. Целью транспортировки изделий является проведение технического обслуживания, ремонта, модернизации изделий и внедрение в изделия новых компонентов. В качестве примера Разработчиков рассматриваются авиастроительные корпорации.

На массиве научных статей, патентов на изобретения, свидетельств о регистрации программ для ЭВМ и баз данных, использующих технологии сетевого управления, проведён сравнительный анализ выборок из этих публикаций, которые можно использовать при создании новых научно-технических решений по управлению движением беспилотного воздушного судна, осуществляющего транспортировку изделий в сети логистических маршрутов.

Решена научная задача о создании нового научно-технического решения для процесса управления движением воздушного судна при транспортировке изделий. Особое внимание при разработке нового решения уделено технологиям сетевого управления и базам данных, построенных на структурировании взаимосвязанных семантических сущностей в предметной области.

Научным результатом исследования является новая сетевая модель для управления движением воздушного судна в сети логистических маршрутов. В состав модели вошли десять новых функций на подготовительном этапе и на этапе транспортировки в жизненном цикле процесса управления движением.

Главным эффектом от использования новой модели является обеспечение непрерывности управления движением воздушного судна в условиях сильного негативного влияния аддитивных помех, мультипликативных возмущений и других противодействующих процессов. Эффект достигается за счет свойства новой модели по своевременному предотвращению негативного влияния на параметры каналов связи между наземными объектами и воздушным судном при его движении в сети логистических маршрутов.

Применение новой модели в системах технической эксплуатации авиастроительных корпораций, в перспективе и в других отраслях экономики и сферах государственного управления, позволит сократить время воспроизводства логистических процессов и снизить стоимость логистических работ.

Литература

1. *Козлов С.В., Кубанков А.Н., Шабанов А.П.* Модуль принятия решений по интеллектуальной поддержке наукоемких производств // Наукоемкие технологии в космических исследованиях Земли. 2022. № 2 (14). С. 36-43. DOI: 10.36724/2409-5419-2022-14-2-36-43. – EDN: SVLJXL.

2. Strategy of scientific and technological development of the Russian Federation. Decree of the President of the Russian Federation No. 143 dated March 15, 2021, related to changes in the Strategy. Official Internet portal of legal information [Electronic resource], 2021. http://www.kremlin.ru/acts/bank/46506 .

3. *Kozlov S.V., Kubankov A.N., Shabanov A.P.* Software-Defined Networking Model for Unmanned Systems Projects. Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF-2022). 2022. Vol. 5. No. 1, pp. 234-239. IEEE. DOI: 10.1109/WECONF55058.2022.9803556.

4. *Kozlov S.V., Kubankov A.N., Shabanov A.P.* On the Transformation of Research Data Transmission Processes in the Digital Platform. Wave Electronics and its Application in Information and Telecommunication Systems (WECONF 2021). 2021, pp. 20809673. DOI: 10.1109/WECONF51603.2021.9470757.

5. *Kozlov S.V., Kubankov A.N., Shabanov A.P.* On the role of the semantic knowledge model in ensuring the stability of reproduction of data transmission processes. Wave electronics and its application in information and telecommunication systems (WECONF 2020). 2020, pp. 9131521. DOI: 10.1109/WECONF48837.2020.913152.

6. *Kozlov S.V., Kubankov A.N., Shabanov A.P.* Innovations in control systems of actions of robotic objects in the field of emergency response. Wave electronics and its application in information and telecommunication systems (WECONF 2019). 2019, pp. 18994090. DOI: 10.1109/WECONF.2019.8840139.

7. *Васильченко А.С.* Методики повышения устойчивости маршрутного управления беспилотным летательным аппаратом в условиях применения средств огневого и радиоэлектронного поражения // Воздушно-космические силы. Теория и практика. 2020. № 13. С. 89-98. EDN LQULAW

8. *Madera A.G.* Modeling and optimization of business processes and process systems under conditions of uncertainty. Business Informatics. 2017. No. 4(42), pp. 74-82. DOI: 10.17323/1998-0663.2017.4.74.82. EDN YUOFLO.

9. *Зюко А.Г.* Помехоустойчивость и эффективность систем связи. М.: Связьиздат, 1963. 320 с. https://search.rsl.ru/ru/record/01006199520.

10. *Селиванов А.В., Вашлаев И.И., Михайлов А.Г.* Управление параметрами транспортной логистики в структуре консалтингового логистического центра // Инновационные транспортные системы и технологии. 2022. № 2 (8). С. 70-91. DOI: 10.17816/transsyst20228270-91. EDN QCMMXS.

11. Концепция интеграции беспилотных летательных аппаратов в единое воздушное пространство Российской Федерации // Постановление Правительства Российской Федерации № 2806-р от 5 октября 2021. http://publication.pravo.gov.ru/Document/View/0001202110110022.

12. *Ляшенко А.Н.* Математическая модель принятия решений на нечетком множестве данных в сфере логистики // Автоматика на транспорте. 2022. № 2 (8). С. 188-197. DOI: 10.20295/2412-9186-2022-8-2-188-197. EDN QOSJLY.

13. Вертолёты России – Национальный центр вертолетостроения имени М.Л. Миля и Н.И. Камова. 2023. https://rhc.aero/structure/nhc.

14. Объединенная авиастроительная корпорация (ОАК). 2023. https://www.uacrussia.ru/ru/.

15. *Палагин Ю.И., Зверева А.С.* Планирование маршрутов доставки грузов беспилотными летательными аппаратами // Транспорт: наука, техника, управление. Научный информационный сборник. 2022. № 8. С. 26-31. DOI: 10.36535/0236-1914-2022-08-4. – EDN ATGHUI.

16. *Горелова А.А., Костин А.С.* Исследование законодательной базы использования беспилотных авиационных систем // Системный анализ и логистика. 2021. № 4(30). С. 122-129. DOI: 10.31799/2077-5687-2021-4-122-129. EDN DBSBDC.

17. *Вишняков В.А.* Технология (вариант) использования БПЛ для совершенствования услуг почтовой связи в Республике Беларусь // Проблемы инфокоммуникаций. 2017. № 2(6). С. 22-28. EDN XSFIWL.

18. *Агеев А.М., Бондарев, В.В., Проценко В.Г.* Обоснование выбора источников излучения для системы технического зрения в задаче автоматической посадки беспилотных летательных аппаратов // Компьютерная оптика. 2022. № 2 (46). С. 239-245. DOI: 10.18287/2412-6179-CO-875. EDN RCPJGR.

19. *Исраелян Г.М., Назаров А.А., Гаранин Е.О.* Синтез и применение многоуровневой архитектуры системы управления узлами беспилотного ТС // Экстремальная робототехника. 2022. № 1 (1). С. 98-108. EDN NNCAYE.

20. *Первушина Н.А., Фролова А.Д.* Разработка адаптивной системы стабилизации для беспилотного летательного аппарата самолетного типа // Проблемы управления. 2022. № 5. С. 3-15. DOI: 10.25728/pu.2022.5.1. EDN QYNWHO.

21. *Виноградов Е.А.* Ключевые технологии связи для поддержки систем управления движением гражданских беспилотных летательных аппаратов (обзор зарубежной литературы) // Научный вестник МГТУ ГА. 2021. № 2 (24). С. 70-92. DOI: 10.26467/2079-0619-2021-24-2-70-92. EDN KBYFRT.

22. *Shao G., Latif H., Martin C., Denno P.* Standards-based integration of advanced process control and optimization. Journal of Industrial Information Integration. 2019. Vol. 13, pp. 1-12. https://doi.org/10.1016/j.jii.2018.11.006.

23. *Semenov V., Ilyin D., Morozov S., Tarlapan O.* Effective consistency management for large-scale product data. Journal of Industrial Information Integration. 2019. Vol. 13, pp. 13-21. https://doi.org/10.1016/j.jii.2018.11.006.

24. *Morshedzadeh I., Ng A. H. C., Jeusfeld M.* Managing manufacturing data and information in product lifecycle management systems considering changes and revisions. International Journal of Product Lifecycle Management. 2021. Vol. 13. No. 3. Pp. 244-264. DOI: 10.1504/IJPLM.2021.118041.

25. *Asikainen A.-L.,* Mangiarotti G. Open innovation and growth in IT sector. Service Business. 2017. Vol. 11, pp. 45-68. DOI:10.1007/s11628-015-0301-2.

26. *Auemhammer J., Bernard R.* The origin and evolution of Stanford University's design thinking: From product design to design thinking in innovation management. Journal of Product Innovation Management. 2021. Vol. 38, pp. 623-644. DOI:10.1111/jpim.12594.

27. *Lattemann C., Siemon D., Dorawa D, Redlich B.* Digitization of the design thinking process solving problems with geographically dispersed teams. Proc. Design User Experience and Usability: Theory Methodology and Management. DUXU: 2017. Vol. 10288, pp. 71-88. DOI:10.1007/978-3-319-58634-2_6.

28. *Rastegaev G.I.* Improving the Quality of Analysis and Evaluation of the Communication Performance of the Command-and-Control Data Link of an Unmanned Aerial Vehicle Based on the Results of Flight Tests. Systems of Control, Communication and Security. 2022. No. 4, pp. 103-136. DOI: 10.24412/2410-9916-2022-4-103-136. (In Russian)

29. *Кизима С.В., Руденкова Е.Г.* Оценка состояния электромагнитной обстановки и контроль качества условий распространения и приема радиосигналов // Электросвязь. 2020. № 7. С. 44-50. DOI: 10.34832/ELSV.2020.8.7.006. – EDN MTPRTZ.

30. *Kudryakov S.A., Rubtsov E.A., Belyaev S.A.* et al. Analysis of different range data links for command, control and communications with unmanned aircraft. Proceedings of Saint Petersburg Electrotechnical University. 2019. No. 1, pp. 31-38.

31. Патент № 2764389 C1. Российская Федерация. МПК G06F 17/15 (2021.08), 2022.

32. Патент № 2789153 C1. Российская Федерация. МПК B60L 15/20 (2006.01), 2022.

33. Патент № 2780541 C1. Российская Федерация. МПК G08G 5/04 (2022.05), 2022.

34. Патент № 2784884 C1. Российская Федерация. МПК G05D 1/08 (2006.01), 2022.

35. Патент № 2767605 C1. Российская Федерация. МПК H04B 7/26 (2006.01), 2022.

36. Свидетельство о регистрации программы для ЭВМ № 2022612779. Российская Федерация, 2022.

37. Свидетельство о регистрации базы данных № 2022621234. Российская Федерация, 2022.

38. Свидетельство о регистрации базы данных № 2022622327. Российская Федерация, 2022.

39. Пшеничников А.В. Интегральная модель радиолинии в конфликтной ситуации // Информация и космос. 2016. № 4. С. 39-45. – EDN XHFNAV.

40. Патент № 2749990 C1. Российская Федерация. СПК G05D 1/08 (2020.08), 2021.

41. Патент № 2751367 C1. Российская Федерация. СПК G05D 1/00 (2021.02), 2021.

42. Патент № 2638732 C1. Российская Федерация. МПКС G06F 7/76, 2017.

43. Патент № 2640332 C1. Российская Федерация. МПК G05B 19/02, 2017.

THE NETWORK MODEL FOR CONTROLLING THE MOVEMENT OF AN AIRCRAFT ALONG LOGISTICS ROUTES

SERGEY V. KOZLOV
Moscow, Russia, kozlov@ipiran.ru

ALEXANDER N. KUBANKOV
Moscow, Russia, a.n.kubankov@mtuci.ru

ALEXANDER P. SHABANOV
Moscow, Russia, apshabanov@mail.ru

KEYWORDS: *system of technical operation of items, logistics process, aircraft movement control, data transmission.*

ABSTRACT

Introduction: The subject area is logistics processes in technical operation systems at enterprises of high-tech industries of electronic, machine-building and other sectors of the economy, whose items and their components are used in operational aviation technical systems and apparatuses. This work is devoted to the research of the use of unmanned aircraft in logistics processes for the transportation of items and their components that require repair, maintenance, modernization or the introduction of new versions of programs and integrated circuits. **The purpose of the work:** To ensure the continuity of aircraft movement control in conditions of strong negative influence of additive interference, multiplicative disturbances and other counteracting processes in certain sections of the logistics route network, the task of developing the novel model of aircraft movement control is being solved. The goal-setting of this model is the reproduction and execution in real time of the command to prevent a break in the control of the movement of the aircraft due to the negative influence of counteracting processes. A scientific patent search was carried out and the closest to the developed model and high-tech analogues were identified. The search was performed on an array of articles, inventions, computer programs and databases published in 2018-2023 related to the topic under research. The scientific result of the research is the developed network process model for controlling the movement of an aircraft in logistics routes, which has a novelty and provides a solution to the task. The main effect of the application of the novel network model is to ensure the continuity of aircraft movement control in the conditions of counteracting processes in the network of logistics routes. The proposed scientific and technical solution may be of interest to managers of enterprises, researchers and engineers in other subject areas in which logistics processes and unmanned transport systems are used.

REFERENCES

1. S.V. Kozlov, A.N. Kubankov, A.P. Shabanov (2022). Decision-making module for intellectual support of high-tech industries. *H&ES Research*. Vol. 14. No. 2, pp. 36-43. DOI: 10.36724/2409&5419&2022&14&2&36&43 (In Russian)

2. Strategy of scientific and technological development of the Russian Federation. Decree of the President of the Russian Federation No. 143 dated March 15, 2021, related to changes in the Strategy. Official Internet portal of legal information [Electronic resource], 2021. http://www.kremlin.ru/acts/bank/46506 .

3. S.V. Kozlov, A.N. Kubankov, A.P. Shabanov (2022). Software-Defined Networking Model for Unmanned Systems Projects. *Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF-2022)*. Vol. 5. No. 1, pp. 234-239. DOI: 10.1109/WECONF55058.2022.9803556.

4. S.V. Kozlov, A.N. Kubankov, A.P. Shabanov (2021). On the Transformation of Research Data Transmission Processes in the Digital Platform. Wave Electronics and its Application in Information and Telecommunication Systems (WECONF 2021), pp. 20809673. DOI: 10.1109/WECONF51603.2021.9470757.

5. S.V. Kozlov, A.N. Kubankov, A.P. Shabanov (2020). On the role of the semantic knowledge model in ensuring the stability of reproduction of data transmission processes. Wave electronics and its application in information and telecommunication systems (WECONF 2020), pp. 9131521. DOI: 10.1109/WECONF48837.2020.913152.

6. S.V. Kozlov, A.N. Kubankov, A.P. Shabanov (2019). Innovations in control systems of actions of robotic objects in the field of emergency response. Wave electronics and its application in information and telecommunication systems (WECONF 2019), pp. 18994090. DOI: 10.1109/WECONF.2019.8840139.

7. A.S. Vasilchenko (2020). Unmanned aerial vehicle route control stability increasing methods under conditions of fire damage means and radioelectronic weapons application. Vozdushno-Kosmicheskie sili. No. 13, pp. 89-98. (In Russian)

8. A.G. Madera (2017). Modeling and optimization of business processes and process systems under conditions of uncertainty. Business Informatics. Vol. 42. No. 4, pp. 74-82. DOI: 10.17323/1998-0663.2017.4.74.82.

9. A.G. Zuko (1963). Noise immunity and efficiency of communication systems. Moscow: Svjazizdat. 320 p. https://search.rsl.ru/ru/record/01006199520. (In Russian)

10. A.V Selivanov, I.I. Vashlaev, A.G. Mikhaylov (2022). Management of transport logistics parameters in the structure of the logistics consulting center. Modern Transportation Systems and Technologies. Vol. 8. No. 2, pp. 70-91. DOI: 10.17816/transsyst20228270-91. (In Russian)

11. The Concept of integration of unmanned aircraft into the unified airspace of the Russian Federation. Decree of the Government of the Russian Federation No. 2806-r of October 5, 2021. Official Internet portal of legal information [Electronic resource]. 2021. http://publication.pravo.gov.ru/Document/View/0001202110110022. (In Russian).

12. A.N. Lyashenko (2022). Mathematical Model of Decision-Making on Data Fuzzy Set in Logistics Field. Transport Automation Research. Vol. 8. No. 2, Pp. 188-197. DOI: 10.20295/2412-9186-2022-8-02-188-197. (In Russian)

13. M.L. Mil, N.I. Kamov (2023). Russian Helicopters – National Helicopter Building Center. Official Internet portal of legal information [Electronic resource]. https://rhc.aero/structure/nhc. (In Russian)

14. United Aircraft Corporation (UAC). Official Internet portal of legal information [Electronic resource]. 2023. https://www.uacrussia.ru/ru/. (In Russian)

15. Yu.I . Palagin, A.S. Zvereva (2022). Planning of cargo delivery routes by unmanned aerial vehicles. Transport: Science, Equipment, Management. Scientific Information Collection. No. 8, pp. 26-31. DOI:

10.36535/0236-1914-2022-08-4. (In Russian)

16. A.A. Gorelova, A.S. Kostin (2021). Research of the legislative base for the use of unmanned aircraft systems. System Analysis and Logistics. Vol. 30. No. 4, pp. 122-129. DOI: 10.31799/2077-5687-2021-4-122-129. (In Russian)

17. V.A. Vishnyakov (2017). Technology (variant) of using UAVs to improve postal services in the Republic of Belarus. Problems of Infocommunications. Vol. 6. No. 2, pp. 22-28. (In Russian)

18. A.M. Ageev, V.G. Bondarev, V.V. Protsenko (2022). Justification of the choice of radiation sources for a computer vision system in the problem of automatic landing of unmanned aerial vehicles. Computer Optics. Vol. 2. No. 46, pp. 239-245. DOI: 10.18287/2412-6179-CO-875. (In Russian)

19. G.M.Israelyan, A.A. Nazarov, E.O. Garanin (2022). Synthesis and application of multilevel architecture of the control system of unmanned vehicle nodes. Extreme robotics. Vol. 1. No. 1, pp. 98-108. (In Russian)

20. N.A. Pervushina, A.D. Frolova (2022). Designing an adaptive stabilizing system for an unmanned aerial vehicle. Problemy Upravlenia. No. 5, pp. 3-15. DOI: 10.25728/pu.2022.5.1. (In Russian)

21. E.A. Vinogradov (2021). Key wireless communication technologies to support traffic management systems of unmanned aerial vehicles for civil application (review of foreign literature). Scientific Bulletin of the Moscow State Technical University of Civil Aviation. Vol. 24. No. 2, pp. 70-92. DOI: 10.26467/2079-0619-2021-24-2-70-92. (In Russian)

22. G. Shao, H. Latif, C. Martin, P. Denno (2018). Standards-based integration of advanced process control and optimization. Journal of Industrial Information Integration. Vol. 13, pp. 1-12. https://doi.org/10.1016/j.jii.2018.11.006.

23. V. Semenov, D. Ilyin, S. Morozov, O. Tarlapan (2019). Effective consistency management for large-scale product data. Journal of Industrial Information Integration. Vol. 13, pp. 13-21. https://doi.org/10.1016/j.jii.2018.11.006.

24. I. Morshedzadeh, Ng A. H. C., M. Jeusfeld (2021). Managing manufacturing data and information in product lifecycle management systems considering changes and revisions. International Journal of Product Lifecycle Management. Vol. 13. No. 3, pp. 244-264. DOI: 10.1504/IJPLM.2021.118041.

25. A.-L. Asikainen, G. Mangiarotti (2017). Open innovation and growth in IT sector. Service Business. Vol. 11, pp. 45-68. DOI:10.1007/s11628-015-0301-2.

26. J. Auemhammer, R. Bernard (2021). The origin and evolution of Stanford University's design thinking: From product design to design thinking in innovation management. Journal of Product Innovation Management. Vol. 38, pp. 623-644. DOI:10.1111/jpim.12594.

27. C. Lattemann, D. Siemon, D. Dorawa, B. Redlich (2017). Digitization of the design thinking process solving problems with geographically dispersed teams. Proc. Design User Experience and Usability: Theory Methodology and Management. DUXU: Vol. 10288, pp. 71-88. DOI:10.1007/978-3-319-58634-2_6.

28. G.I. Rastegaev (2022). Improving the Quality of Analysis and Evaluation of the Communication Performance of the Command-and-Control Data Link of an Unmanned Aerial Vehicle Based on the Results of Flight Tests. Systems of Control, Communication and Security. No. 4, pp. 103-136. DOI: 10.24412/2410-9916-2022-4-103-136. (In Russian)

29. S.V. Kizima, E.G. Rudenkova (2020). Assessment of the electromagnetic environment of the monitoring of signal propagation and reception conditions. Electrosvyaz Magazine. No. 7, pp. 44-50. DOI: 10.34832/ELSV.2020.8.7.006. (In Russian)

30. S.A. Kudryakov, E.A. Rubtsov, S.A. Belyaev et al. (2019). Analysis of different range data links for command, control and communications with unmanned aircraft. Proceedings of Saint Petersburg Electrotechnical University. No. 1, pp. 31-38. (In Russian)

31. Patent No. 2764389 C1 Russian Federation, MPC G06F 17/15 (2021.08), 2022.

32. Patent No. 2789153 C1 Russian Federation, MPC B60L 15/20 (2006.01), 2022.

33. Patent No. 2780541 C1 Russian Federation, MPC G08G 5/04 (2022.05), 2022.

34. Patent No. 2784884 C1 Russian Federation, MPC G05D 1/08 (2006.01), 2022.

35. Patent No. 2767605 C1 Russian Federation, MPC H04B 7/26 (2006.01), 2022.

36. Certificate of state registration of a computer program No. 2022610460 Russian Federation, 2022.

37. Certificate of state registration of a computer program No. 2022612779 Russian Federation, 2022.

38. Certificate of state registration of the database No. 2022621234 Russian Federation, 2022.

39. Certificate of state registration of the database No. 2022622327 Russian Federation, 2022.

40. Pshenichnikov A. Radio line integral model in a conflict situation. Information and Space. 2016. No. 4, pp. 39-45. (In Russian)

41. Patent No. 2749990 C1 Russian Federation, SPC G05D 1/08 (2020.08), 2021.

42. Patent No. 2751367 C1 Russian Federation, SPC G05D 1/00 (2021.02), 2021.

43. Patent No. 2638732 C1 Russian Federation, MPC G06F 7/76, 2017.

44. Patent No. 2640332 C1 Russian Federation, MPC G05B 19/02, 2017.

INFORMATION ABOUT AUTHORS:

Sergey V. Kozlov, PhD, Head of the Division, Federal Research Center "Computer Science and Control" Russian Academy of Sciences, Moscow, Russia, skozlov@ipiran.ru

Alexander N. Kubankov, PhD, Full Professor, Head of Department, Moscow Technical University of Communication and Informatics, Moscow, Russia, a.n.kubankov@mtuci.ru

Alexander P. Shabanov, PhD, leading researcher, Federal Research Center "Computer Science and Control" Russian Academy of Sciences, Moscow, Russia, apshabanov@mail.ru

For citation: Kozlov S.V., Kubankov A.N., Shabanov A.P. The network model for controlling the movement of an aircraft along logistics routes. H&ES Reserch. 2023. Vol. 15. No. 3. P. 11-19. doi: 10.36724/2409-5419-2023-15-3-11-19 (In Rus)

doi: 10.36724/2409-5419-2023-15-3-20-29

ОБНАРУЖЕНИЕ ДРЕЙФА КОНЦЕПТА ПРИ КЛАССИФИКАЦИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ АВТОКОДИРОВЩИКОВ

ШЕЛУХИН
Олег Иванович[1]

БАРКОВ
Вячеслав Валерьевич[2]

СИМОНЯН
Айрапет Генрикович[3]

АННОТАЦИЯ

Введение: Рассматривается задача обнаружения дрейфа концепта в задачах многоклассовой классификации приложений на примере собранного набора данных сетевого трафика в виде IP-пакетов с мобильных устройств под управлением ОС Android с помощью Android VPN API. **Цель исследования:** разработка и программная реализация алгоритма обнаружения смены концепта в задачах многоклассовой классификации трафика мобильных приложений с использованием ИНС типа автокодировщик (АК). **Новизна работы** заключается в обнаружении дрейфа одного или нескольких мобильных приложений на основе изменения статистических характеристик одного или нескольких атрибутов без использования истинных меток классов с применением ИНС типа автокодировщик. **Результаты:** Разработан алгоритм обнаружения дрейфа концепта приложений, основанный на анализе изменений статистических характеристиках атрибутов или заметного снижения качества классификации анализируемых приложений. В качестве базовой модели детектора дрейфа концепта анализируемых приложений использованы автокодировщики. Приводятся основные теоретические положения создания алгоритма. Показано, что если АК обучен только на доброкачественных экземплярах, то он сможет реконструировать нормальные наблюдения, но не может реконструировать аномальные наблюдения (неизвестные понятия). В результате, когда АК фиксирует существенную ошибку реконструкции, это классифицирует данные наблюдения как аномальные. Наличие дрейфа оценивается с помощью оценок ошибок реконструкции анализируемых приложений и превышения пороговых значений. Представленное решение реализовано в программной среде Python.

Сведения об авторах:

[1] д.т.н., профессор, заведующий кафедрой, Московский технический университет связи и информатики, Москва, Россия, sheluhin@mail.ru

[2] старший преподаватель, Московский технический университет связи и информатики, Москва, Россия, v.v.barkov@mtuci.ru

[3] к.т.н., доцент, доцент, Московский технический университет связи и информатики, Москва, Россия, simonyanag@mail.ru

КЛЮЧЕВЫЕ СЛОВА: *алгоритмы классификации, дрейф концепта, поток данных, атрибуты и приложения, метки класса.*

Для цитирования: Шелухин О.И., Барков В.В., Симонян А.Г. Обнаружение дрейфа концепта при классификации мобильных приложений с использованием автокодировщиков // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 3. С. 20-29. doi: 10.36724/2409-5419-2023-15-3-20-29

Введение

Явление, когда характеристики и распределение данных меняются, приводя к необходимости обновления моделей, лежащих в основе алгоритмов классификации, называется «дрейф концепта», а адаптация модели к новым изменениям – «адаптация дрейфа концепта». Подобная проблема называется «Обнаружение и адаптация дрейфа концепта» [1,2,3].

Термин «дрейф концепта» относится к явлению, когда статистические свойства класса или целевой переменной изменяются со временем случайным образом [4], и впервые был предложен в [5].

Рассмотрим поток данных S_t, наблюдаемый в момент времени t, представленный в виде совокупности пар $(\vec{x}_1, y_1)$, $(\vec{x}_2, y_2)$, $(\vec{x}_{M_1}, y_{M_1})$, где $\vec{x}_m$ вектор атрибутов, а y_m – соответствующая метка. При классификации обычно имеются маркированные прошлые данные, и задача состоит в том, чтобы предсказать метку y_{M_1+1} для вектора $\vec{x}_{M_1+1}$, являющуюся одной точкой, или для коллекции точек данных в виде небольшой группы, $\vec{x}_{M_1+1}, \vec{x}_{M_1+2}, \vec{x}_{M_2}$, наблюдаемых в потоке данных S_{t+1} в момент времени t+1. Для этого на имеющихся помеченных данных $(\vec{x}_1, y_1)$, $(\vec{x}_2, y_2)$, $(\vec{x}_{M_1}, y_{M_1})$ обучается классификатор C_t, чтобы предсказать метку класса для точек данных в S_{t+1}.

Между временем t и t+1 может произойти дрейф концепта. В зависимости от источника дрейфа и его влияния на совместное распределение вероятностей атрибутов и метки класса, дрейф концепта может быть виртуальным или реальным [6,7]. В случае если изменение статистических характеристик атрибутов не влияет на принятие решения, то такой дрейф называется виртуальным. В противном случае дрейф называется реальным [8, 9,14].

В случае реального дрейфа производительность классификатора ухудшится с точки зрения метрики оценки, и потребуется обновление модели. Изменения в распределении данных могут происходить по разным шаблонам, которые могут влиять на границу принятия решения (реальный или виртуальный дрейф концепта) в сценарии контролируемого обучения. Эти изменения могут быть измерены с помощью некоторых статистических показателей, таких как среднее значение, дисперсия и т.д. Исходя из модели изменения, дрейф концепта можно разделить на «внезапный» (резкий), «инкрементный», «постепенный» и «повторяющийся» [1,10].

Одним из современных подходов к обнаружению дрейфа концепта является метод, опирающийся на глубокие автокодировщики (АК), обученные на статистических характеристиках, извлеченных из данных нормального трафика. Показана эффективность технологии глубокого обучения для обнаружения дрейфа [6,7,8,9].

Однако в этих работах, как правило, анализируется бинарная классификации и не рассматривались задачи многоклассовой классификации трафика мобильных приложений, имеющих значительные особенности.

Постановка задачи

Задачу обнаружения дрейфа концепта в задачах многоклассовой классификации мобильных приложений рассмотрим на примере собранного набора данных [10-13]. Сбор необработанных данных сетевого трафика в виде IP-пакетов осуществлялся на мобильных устройствах под управлением ОС Android с помощью Android VPN API. Обработка данных, включающая фильтрация пакетов, содержащих данные протокола TCP, группировку пакетов в TCP сеансы, а также вычисление атрибутов TCP сеансов, характеризующих особенности анализируемых приложений, осуществлялась на сервере всякий раз, когда приходил IP-пакет. Набор вычисляемых атрибутов представлен в таблице 1.

Таблица 1

Описание атрибутов

№	$\vec{x}$	Название
1	$x^{(1)}$	Общий объем полезной нагрузки на сетевом уровне от клиента в байтах. Не включает длину заголовка IP
2	$x^{(2)}$	Общий объем полезной нагрузки на сетевом уровне от сервера в байтах. Не включает длину заголовка IP
3	$x^{(3)}$	Общий объем полезной нагрузки на транспортном уровне от клиента в байтах. Не включает длину заголовка IP и TCP (UDP)
4	$x^{(4)}$	Общий объем полезной нагрузки на транспортном уровне от сервера в байтах. Не включает длину заголовка IP и TCP (UDP)
5	$x^{(5)}$	Средний размер пакета на сетевом уровне со стороны клиента в байтах
6	$x^{(6)}$	Средний размер пакета на сетевом уровне со стороны сервера.
7	$x^{(7)}$	Средний размер полезной нагрузки на транспортном уровне со стороны клиента.
8	$x^{(8)}$	Средний размер полезной нагрузки на транспортном уровне со стороны сервера.
9	$x^{(9)}$	Стандартное отклонение размера пакета на сетевом уровне со стороны клиента
10	$x^{(10)}$	Стандартное отклонение размера пакета на сетевом уровне со стороны сервера
11	$x^{(11)}$	Стандартное отклонение размера полезной нагрузки на транспортном уровне со стороны клиента
12	$x^{(12)}$	Стандартное отклонение размера полезной нагрузки на транспортном уровне со стороны сервера
13	$x^{(13)}$	Среднее число пакетов сетевого уровня для передачи сообщения со стороны клиента
14	$x^{(14)}$	Среднее число пакетов сетевого уровня для передачи сообщения со стороны сервера
15	$x^{(15)}$	КПД клиента – Количество переданной полезной нагрузки транспортного уровня, делённое на общее количество переданной нагрузки транспортного и сетевого уровня со стороны клиента.
16	$x^{(16)}$	КПД сервера – Количество переданной нагрузки сетевого уровня, делённое на общее количество переданной нагрузки транспортного и сетевого уровня со стороны сервера.
17	$x^{(17)}$	Соотношение байт – во сколько раз клиент передал больше пакетов в байтовом представлении, чем сервер.
18	$x^{(18)}$	Соотношение полезной нагрузки транспортного уровня – во сколько раз клиент передал больше байт полезной нагрузки на транспортном уровне, чем сервер.

№	$\vec{x}$	Название
19	$x^{(19)}$	Соотношения общего количества пакетов на сетевом уровне – во сколько раз клиент передал больше пакетов на сетевом уровне, чем сервер.
20	$x^{(20)}$	Общее количество переданных датаграмм на сетевом уровне со стороны клиента
21	$x^{(21)}$	Общее количество переданных датаграмм на сетевом уровне со стороны сервера
22	$x^{(22)}$	IP-адрес источника
23	$x^{(23)}$	IP-адрес назначения

Обработанные данные сетевого трафика формируют **набор данных**, состоящий из **экземпляров.** Каждый экземпляр набора это TCP сеанс $s_m \in S$, представленный в виде вектора вычисленных атрибутов, $\vec{x}_m = \left(x_m^{(n)}; \overline{1,N}\right) \in X$ перечисленных в таблице 1, характеризующих множество приложений $A = \left\{a_k; k = \overline{1,K}\right\}$ Последовательно идущие экземпляры формируют **группы экземпляров** $G^{(r)} \in G$. Каждая группа экземпляров, кроме последней, содержит одинаковое количество экземпляров.

Части набора данных используются для обучения, выбора и проверки модели классификации, а также для обучения и проверки модели обнаружения дрейфа концепта.

В качестве базовой модели детектора дрейфа для каждого анализируемого приложения будем использовать автокодировщики [14,15]. Автокодировщик – это искусственная нейронная сеть (ИНС), которая обучена восстанавливать свои входные данные после некоторого сжатия.

Если АК обучен на экземплярах только одного приложения, он сможет реконструировать экземпляры только этого приложения, но не сможет реконструировать другие приложения, в том числе неизвестные или искажённые. В результате, когда фиксируется существенная ошибка реконструкции восстановленных данных на выходе АК, данный экземпляр классифицируется как не принадлежащий рассматриваемому приложению. Этот эффект будет заложен в алгоритм обнаружения дрейфа концепта [16,17,18].

Новизна работы заключается в обнаружении дрейфа одного или нескольких мобильных приложений на основе изменения статистических характеристик одного или нескольких атрибутов без использования истинных меток классов с применением ИНС типа автокодировщик.

Целью работы является разработка и программная реализация алгоритма обнаружения смены концепта в задачах многоклассовой классификации трафика мобильных приложений с использованием ИНС типа автокодировщик.

Подготовка исходных данных

Пусть имеется множество IP пакетов $P = \{p_j;\ j = \overline{1,J}\}$ мощностью J и множество приложений $A = \{a_k; k = \overline{1,K}\}$ мощностью K, которое их генерирует.

С помощью функции фильтрации $f : \{P' \subset P\} \to \{P'' \subset P'\}$ из множества P выберем только те пакеты, которые содержат в себе TCP сегменты: $P_{TCP} = f(P), P_{TCP} \subset P$.

С помощью функции группировки $\gamma : \left\{P'_{TCP} \subset P_{TCP}\right\} \to \left\{S'\right\}$ преобразуем P_{TCP} в множество TCP сеансов $S = \{s_m; m = \overline{1,M}\}$ мощностью $M : S = \gamma\left(P_{TCP}\right)$.

С помощью функции разметки $\xi : \left\{S' \subset S\right\} \times \left\{A' \subset A\right\} \to \{S'^{(A')}\}$ для каждого TCP сеанса определим приложение-источник и сформируем размеченное множество TCP сеансов: $\xi(S', A') = \left\{\left(s'_m, a'_m\right) \middle| s'_m \in S', a'_m \in A'\right\}$; $S^{(A)} = \xi(S, A)$.

Пусть также имеется множество функций вычисления атрибутов $\Phi = \{\phi_n : S \to \mathbb{R}; n = \overline{1,N}\}$ мощностью N, вычисляющих множество атрибутов TCP сеансов X путём отображения каждого элемента множества TCP сеансов S в элемент множества рациональных чисел $\mathbb{R}$.

Путём отображения каждого элемента множества TCP сеансов S в элемент множества рациональных чисел $\mathbb{R}$ вычислим множество Φ атрибутов TCP сеансов $X : \Phi = \left\{\phi_n : S \to \mathbb{R}; n = \overline{1,N}\right\}$ мощностью N.

Введем в рассмотрение функцию кодирования приложения $\psi : A \to \left\{k; k = \overline{1,K}\right\}$, вычисляющую метку класса $y_k \in Y$ путём отображения элементов множества приложений A в множество целых чисел k.

Представим множество TCP сеансов S в виде множества векторов атрибутов

$$X = \left\{\vec{x}_m = \left(x_m^{(n)}; n = \overline{1,N}\right); m = \overline{1,M} \middle| x_m^{(n)} = \phi_n(s_m), \phi_n \in \Phi, s_m \in S\right\},$$

где n-й элемент вектора $\vec{x}_m$ вычисляется функцией ϕ_n.

Представим множество приложений A в виде множества меток классов $Y = \left\{y_k = \psi(a_k); k = \overline{1,K} \middle| a_k \in A\right\}$. Тогда размеченное множество $S^{(A)}$, полученное с помощью функции разметки ξ, можно представить в виде множества пар векторов атрибутов и метки класса $X^{(Y)}$:

$$X^{(Y)} = \left\{\left(\vec{x}_m, y'_m\right); m = \overline{1,M} \middle| \vec{x}_m = (\phi_n(s_m);\ n = \overline{1,N},\ y'_m = \psi\left(a'_m\right), \left(s_m, a'_m\right) \in S^{(A)})\right\}$$

Разделим полученное множество $X^{(Y)}$ на два непересекающихся подмножества: обучающее $X_{об}^{(Y)}$ и тестовое $X_{тест}^{(Y)}$, с помощью функции разделения $\alpha : \left\{X^{(Y)'} \subset X^{(Y)}\right\} \to \left\{\left(X_{об}^{(Y)'} \subset X^{(Y)'}, X_{тест}^{(Y)'} \subset X^{(Y)'}\right)\right\}$ так, что $X^{(Y)} = X_{об}^{(Y)} \cup X_{тест}^{(Y)}; X_{об}^{(Y)} \cap X_{тест}^{(Y)} = \varnothing$.

Будем считать для определенности, что обучающее подмножество содержит 85% исходного множества $\left|X_{об}^{(Y)}\right| = 0.85\left|X^{(Y)}\right|$, а тестовое $\left|X_{тест}^{(Y)}\right| = 0.15\left|X^{(Y)}\right|$, что

соответствует 15% исходного множества. Так что

$$\alpha\left(X^{(Y)'}\right)=\left(X_{об}^{(Y)'},X_{тест}^{(Y)'}\right)\left|X^{(Y)'}=X_{об}^{(Y)'}\cup X_{тест}^{(Y)'};X_{об}^{(Y)'}\cap X_{тест}^{(Y)'}=\varnothing;\right.$$

$$\left|X_{об}^{(Y)}\right|=0.85\left|X^{(Y)}\right|,\left|X_{тест}^{(Y)}\right|=0.15\left|X^{(Y)}\right|;\left(X_{об}^{(Y)},X_{тест}^{(Y)}\right)=\alpha\left(X^{(Y)}\right);$$

Полученные подмножества будем использовать для обучения алгоритмов классификации трафика и разработки модели обнаружение дрейфа.

Алгоритм обнаружения дрейфа концепта в режиме обучения

Структурная схема алгоритма обнаружения дрейфа концепта в режиме обучения представлена на рисунке 1.

Режим обучения предполагает наличия размеченных данных и заключается в построении АК для каждого приложения, подлежащего идентификации, и настройке порогов обнаружения дрейфа.

Для обучения модели обнаружения дрейфа требуются данные о TCP сеансах приложений. Для обучения поток IP пакетов с метками приложений отфильтровывается с помощью функции фильтрации $f:\{P'\subset P\}\to\{P''\subset P'\}$ таким образом, чтобы в нем остались только IP пакеты с типом протокола TCP $P_{TCP}\subset P$. По четырем полям заголовков IP и TCP – IP адресу источника, IP адресу назначения, порту источника и порту назначения – IP пакеты группируются в TCP сеансы. Меткой TCP сеанса является любая метка IP пакета, принадлежащего этому сеансу.

На основе IP пакетов TCP сеанса с помощью функции группировки $\gamma:\{P'_{TCP}\subset P_{TCP}\}\to\{S'\}$ вычисляется множество TCP сеансов $S=\{s_m;m=\overline{1,M}\}$ из которого формируется размеченное множество TCP сеансов $S^{(A)}=\xi(S,A)$.

Путём отображения каждого элемента множества сеансов $S^{(A)}$ в элемент множества рациональных чисел $\mathbb{R}$ вычисляется множество атрибутов TCP сеансов $\Phi=\{\phi_n:S\to\mathbb{R};n=\overline{1,N}\}$ и функция кодирования приложения $\psi:A\to\{k;k=\overline{1,K}\}$, вычисляющую метку класса $y_k\in Y$.

В результате формируется размеченное множество TCP сеансов, представленных в виде пар векторов атрибутов и меток класса $X^{(Y)}=\{(\vec{x}_m,y'_m)\,|\,\vec{x}_m\in X,y'_m\in Y\}$, которое разбивается на обучающее $X_{об}^{(Y)}$ и тестовое $X_{тест}^{(Y)}$ множества.

Обучающее множество $X_{об}^{(Y)}$ используется как для обучения алгоритмов классификации, так и для обучения модели обнаружения дрейфа. Тестовое множество $X_{тест}^{(Y)}$ используется для оценки качества классификации и модели обнаружения дрейфа.

В отсутствии дрейфа концепта задачей классификации является идентификация конкретного вида приложения $\{a_k;k=\overline{1,K}\}$ из источника TCP сеанса. Задача классификации может быть сформулирована следующим образом:

Пусть имеется конечная множество $X^{(Y)}=\{(\vec{x}_m,y'_m)\,|\,\vec{x}_m\in X,y'_m\in Y\}$.

Требуется построить классификатор C с алгоритмом $a:X_{об}^{(Y)}\to A$, способный классифицировать произвольное приложение $a_k\in A,k=\overline{1,K}$ характеризуемое множеством атрибутов $x\in X$.

Для классификации приложений может использоваться один из известных алгоритмов машинного обучения: Logistic Regression (LR), K-Nearest Neighbors (KNN), Decision Tree (DT), Random Forest (RF) и Gradient Boosting (GB) [12, 13].

В структуре алгоритма представленного на рисунке 1 предусмотрен алгоритм обнаружения дрейфа того или иного приложения TCP сеанса.

Модель обнаружения дрейфа приложения в потоке $D_{прил}$ определяется через модель обнаружения дрейфа атрибута в потоке $D_{атриб}$ обученного на основе алгоритма автокодировщика $AE^{(y_k)}$. Множество реконструированных оценок на выходе автокодировщика $\widehat{X}_{AE}^{(y_k)}$ позволяет принять решение о необходимости перестроить параметры алгоритма классификации $a:X_{об}^{(Y)}\to A$, при фиксации тренда или оставить их неизменными в случае отсутствия драйфа концепта. Структура алгоритма обнаружения дрейфа концепта будет рассмотрена далее.

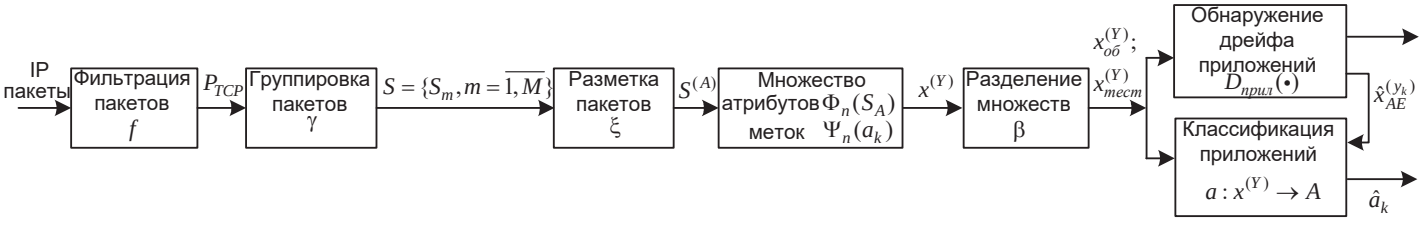

Рис 1. Структурная схема алгоритма в режиме обучения

Обнаружение дрейфа концепта в потоке

Обнаружение дрейфа приложений в потоке представляет собой задачу многозначной классификации, т.к. возможны случаи, когда статистические характеристики изменяются сразу для нескольких приложений.

Обнаружение дрейфа в потоке осуществляется детектором D отдельно для каждой метки класса $y_k = \psi(a_k)$; $k = \overline{1,K} \,|\, a_k \in A$. Для этого строятся модели $D^{(y_k)}$ обнаружения дрейфа потока с заданной меткой класса $y_k \in Y$.

Дрейф считается обнаруженным, если хотя бы одна модель $D^{(y_k)}$ обнаружит дрейф, т.е. обнаружен хотя бы в одном приложении. Разделение размеченного множества $X^{(Y)}$ на подмножества, содержащие только экземпляры с одинаковыми метками классов, осуществляется с помощью разделяющей функции β. Функция β получает на вход некоторое подмножество $X^{(Y)\prime} \subset X^{(Y)}$ и разделяет его на не пересекающиеся подмножества $X^{(Y)\prime\prime}$:

$$\beta : \{X^{(Y)\prime} \subset X^{(Y)}\} \to \{\left\{X^{(y_k)\prime} \subset X^{(Y)\prime}\right\} \Big| X^{(Y)\prime} \subset X^{(Y)}\};$$

$$\beta\left(X^{(Y)\prime}\right) = \{X^{(y_k)\prime} = \{\vec{x}_m; m = \overline{1, \left|X^{(Y)\prime}\right|} \,|\, (\vec{x}_m, y_k) \in X^{(Y)\prime}\}; k = \overline{1,K}\}.$$

При разделении множества на этапах обучения и тестирования в качестве меток классов используются истинные значения, в то время как на этапе предсказания – значения, предсказанные моделью классификации.

Обнаружение дрейфа приложения осуществляется детектором $D^{(y_k)}$ с помощью модели обнаружения дрейфа атрибутов приложения $D^{(y_k)}_{атриб}$.

Модель обнаружения дрейфа атрибутов $D^{(y_k)}_{атриб}$ основана на механизме обнаружения дрейфа в группах экземпляров $G^{(r)}$, которое осуществляется с помощью автокодировщика .

АК использует набор весовых коэффициентов распознавания для отображения входных данных в кодирующий вектор на скрытом слое, а затем использует набор генеративных весовых коэффициентов для восстановления закодированного вектора в исходный входной сигнал на выходном слое. Простой АК состоит из входного слоя, одного или нескольких скрытых слоев и выходного слоя того же размера, что и входной слой [19,20,21].

Если АК обучен только на доброкачественных экземплярах, то он сможет реконструировать нормальные наблюдения, но не может реконструировать аномальные наблюдения (неизвестные понятия). В результате, когда АК фиксирует существенную ошибку реконструкции, это классифицирует данные наблюдения как аномальные**.** Наличие дрейфа оценивается с помощью оценок ошибок реконструкции анализируемых приложений и превышения пороговых значений.

Этот подход заложен в представленном ниже алгоритмом обнаружения дрейфа для задачи многоклассовой классификации мобильных приложений с использованием АК.

Реконструкция приложений

Для каждого из анализируемых приложений $A = \{a_k; k = \overline{1,K}\}$, используя функции расчёта потерь при реконструкции, вычисляются три группы пороговых значений: пороги экземпляра приложения k $T^{(k)}_{экз}$, пороги группы приложения k $T^{(k)}_{гр}$ и пороги подсчета приложения k $T^{(k)}_{n}$. Группы пороговых значений состоят из пороговых значений атрибутов: **порог экземпляра** приложения k атрибута n $T^{(kn)}_{экз}$, **порог группы** приложения k атрибута n $T^{(kn)}_{гр}$ и **порог подсчета** приложения k атрибута n $T^{(kn)}_{n}$. Совокупность порогов атрибутов всех приложений будет выглядеть следующим образом:

$$T_{экз} = \{T^{(k)}_{экз} = \{T^{(kn)}_{экз}; k = \overline{1,K}\}; n = \overline{1,N}\},$$
$$T_{гр} = \{T^{(k)}_{гр} = \{T^{(kn)}_{гр}; k = \overline{1,K}\}; n = \overline{1,N}\},$$
$$T_{n} = \{T^{(k)}_{n} = \{T^{(kn)}_{n}; k = \overline{1,K}\}; n = \overline{1,N}\}.$$

Пороговое значение экземпляра $T_{экз}$ для нормальных (не подготовленных) данных вычисляется как среднее значение +3 (стандартное отклонение) значений ошибки восстановления. Предполагается, что любая точка данных со значениями ошибок восстановления, превышающими пороговое значение экземпляра, будет смещенной точкой данных

Порог группы $T_{гр}$ вычисляется с использованием средних значений потерь при восстановлении пакета. Оно принимается как среднее значение +3 (стандартное отклонение) по сравнению со средними значениями ошибки восстановления пакета по всем данным проверки.

Порог подсчета $T^{(kn)}_{n}$ приложения k атрибута n вычисляется с использованием средних значений потерь при восстановлении пакета. Оно принимается как среднее значение +3 (стандартное отклонение) по сравнению со средними значениями ошибки восстановления партии для всех партий по всем данным проверки.

Качество обученного автокодировщика $AE^{(y_k)}$ оценивается с помощью оценки качества реконструкции экземпляров группы, вычисляемой с помощью функции Q на валидационной выборке $X^{(y_k)}_{AE_в}$. Для этого каждый экземпляр тестирующей выборки $X^{(y_k)}_{AE_в}$ подаётся на вход автокодировщику $AE^{(y_k)}$ и получается множество реконструированных экземпляров $\hat{X}^{(y_k)}_{AE_в} = AE^{(y_k)}(X^{(y_k)}_{AE_в})$.

Метрика качества $Q^{(y_k)}_{в} = Q(X^{(y_k)}_{AE_в}, \hat{X}^{(y_k)}_{AE_в}$ обученного автокодировщика $AE^{(y_k)}$ позволяет оценить качество реконструкции экземпляров АК. При низком качестве хотя бы одного АК требуется его повторное обучение. После достижения достаточного качества реконструкции можно перейти к расчёту пороговых значений.

В качестве функции потерь реконструкции одного атрибута одного **экземпляра** воспользуемся функцией квадрата разности. Пусть $L_{атриб}$ – функция, вычисляющая потери реконструкции *n*-ого атрибута $x_m^{(n)}$ экземпляра $\vec{x}_m$. Функция $L_{атриб}$ получает на вход исходный вектор атрибутов $\vec{x}_m$ из множества *X*, реконструированный вектор атрибутов $\hat{\vec{x}}_m$ из того же множества *X*, номер атрибута *n*, для которого осуществляется вычисление потерь реконструкции, и возвращает квадрат разности *n*-ых элементов исходного $\vec{x}_m$ и реконструированного $\hat{\vec{x}}_m$ векторов:

$$L_{атриб} : \{\vec{x}_m \in X\}^2 \times \{n; n = \overline{1, N}\} \to \mathbb{R}$$
$$L_{атриб}(\vec{x}_m, \hat{\vec{x}}_m, n) = (x_m^{(n)} - \hat{x}_m^{(n)})^2, x_m^{(n)} \in \vec{x}_m, \hat{x}_m^{(n)} \in \hat{\vec{x}}_m$$

Пусть $L_{атриб\ гр} : \{G^{(r)} \subset X\}^2 \times \{n; n = \overline{1, N}\} \to \mathbb{R}$ – функция потерь реконструкции n-ого атрибута в группе экземпляров $G^{(r)}$, вычисляющая потери реконструкции одного атрибута для всех экземпляров группы. Функция $L_{атриб\ гр}$ получает на вход исходную группу векторов атрибутов $G^{(r)} \subset X$, являющуюся подмножеством множества *X*, реконструированную группу векторов атрибутов, $\hat{G}^{(r)} \subset X$, являющуюся подмножеством множества *X*, номер атрибута *n*, для которого осуществляется вычисление потерь, и возвращает множество, содержащее потери реконструкции одного атрибута для всех экземпляров группы:

$$L_{атриб}(G^{(r)}, \hat{G}^{(r)}, n) = \{L_{атриб}(\vec{x}_m, \hat{\vec{x}}_m, n);$$
$$m = \overline{1, \left|G^{(r)}\right|} : \vec{x}_m \in G^{(r)}, \hat{\vec{x}}_m \in \hat{G}^{(r)}\}.$$

Пусть $L_{экз} : \{\vec{x}_m \in X\}^2 \to \mathbb{R}$ – функция вычисления потерь реконструкции одного экземпляра, вычисляющая среднюю потерю реконструкции всех атрибутов этого экземпляра. Функция $L_{экз}$ получает на вход исходный вектор атрибутов $\vec{x}_m$ из множества *X*, реконструированный вектор атрибутов $\hat{\vec{x}}_m$ из того же множества *X* и возвращает среднюю потерю реконструкции всех атрибутов экземпляра (потерю реконструкции экземпляра)

$$L_{экз}(\vec{x}_m, \hat{\vec{x}}_m) = \frac{1}{N} \sum_{n=1}^{N} L_{атриб}(\vec{x}_m, \hat{\vec{x}}_m, n).$$

Функция качества реконструкции <u>*одного атрибута экземпляров*</u> группы можно вычислить с помощью функции $Q_{атриб} : \{G^{(r)} \subset X\}^2 \times \{n; n = \overline{1, N}\} \to \mathbb{R}$ путём усреднения потери реконструкции этого атрибута для всех экземпляров группы. Функция $Q_{атриб}$ получает на вход исходную группу векторов атрибутов $G^{(r)}$, которая является подмножеством множества *X*, реконструированную группу векторов атрибутов $\hat{G}^{(r)}$, являющуюся подмножеством множества *X*, номер атрибута *n*, для которого осуществляется вычисление потерь и возвращает среднюю потерю реконструкции атрибута в группе:

$$Q_{атриб}(G^{(r)}, \hat{G}^{(r)}, n) = \frac{1}{\left|G^{(r)}\right|} \times$$
$$\times \sum_{m=1}^{\left|G^{(r)}\right|} L_{атриб}(G_m^{(r)}, \hat{G}_m^{(r)}, n), G_m^{(r)} \in X, \hat{G}_m^{(r)} \in X.$$

Функция качества реконструкции экземпляров группы можно вычислить с помощью функции $Q : \{G^{(r)} \subset X\}^2 \to \mathbb{R}$ путём усреднения потерь реконструкции одного экземпляра. Функция *Q* получает на вход исходную группу векторов атрибутов $G^{(r)}$, являющуюся подмножеством множества *X*, реконструированную группу векторов атрибутов $\hat{G}^{(r)}$, являющуюся подмножеством множества *X*, возвращает среднее значение потерь реконструкции экземпляров:

$$Q(G^{(r)}, \hat{G}^{(r)}) = \frac{1}{\left|G^{(r)}\right|} \sum_{m=1}^{\left|G^{(r)}\right|} L_{экз}(G_m^{(r)}, \hat{G}^{(r)}), G_m^{(r)} \in X, \hat{G}^{(r)} \in X$$

Пример вычисления ошибок реконструкции экземпляров в группе представлен в табл. 2.

Таблица 2

Вычисление ошибок реконструкции экземпляров в группе

$G^{(r)}$	$\hat{G}^{(r)}$	1	…	*N*	Результат
$\vec{x}_1$	$\hat{\vec{x}}_1$	$L_{атриб}(\vec{x}_1, \hat{\vec{x}}_1, 1)$	…	$L_{атриб}(\vec{x}_1, \hat{\vec{x}}_1, N)$	$L_{экз}(\vec{x}_1, \hat{\vec{x}}_1)$
…	…	…	…	…	…
$\vec{x}_{\left\|G^{(r)}\right\|}$	$\hat{\vec{x}}_{\left\|G^{(r)}\right\|}$	$L_{атриб}(\vec{x}_{\left\|G^{(r)}\right\|}, \hat{\vec{x}}_{\left\|G^{(r)}\right\|}, 1)$	…	$L_{атриб}(\vec{x}_{\left\|G^{(r)}\right\|}, \hat{\vec{x}}_{\left\|G^{(r)}\right\|}, N)$	$L_{экз}(\vec{x}_{\left\|G^{(r)}\right\|}, \hat{\vec{x}}_{\left\|G^{(r)}\right\|})$
		$Q_{атриб}(G^{(r)}, \hat{G}^{(r)}, 1)$	…	$Q_{атриб}(G^{(r)}, \hat{G}^{(r)}, N)$	$Q(G^{(r)}, \hat{G}^{(r)})$

Приведённые функции потерь и функции качества используются для оценки качества обученных АК и вычисления порогов.

Алгоритм обнаружения дрейфа концепта

Процесс обучения модели обнаружения дрейфа атрибутов включает обучение АК, расчёт потерь реконструкции атрибутов и расчёт пороговых значений.

Разделим с помощью описанной выше разделяющей функции β обучающую выборку $X_{об}^{(Y)}$ на *k* компонент $X_{об}^{(Y)} = U_{X_{об}^{(y_k)} \in \beta(X_{об}^{(Y)})} X_{об}^{(y_k)}$.

Каждое полученное множество $X_{об}^{(y_k)}$ содержит только векторы атрибутов, которые помечены меткой класса y_k, то есть представляет собой TCP сеансы, которые принадлежат приложению a_k.

Разобьем каждое множество $X_{об}^{(y_k)}$ на три непересекающихся множества: обучающее $X_{AE_{об}}^{(y_k)}$, валидационное $X_{AE_в}^{(y_k)}$

множества и множество для настройки пороговых значений $X_{AE_n}^{(y_k)}$, так что $X_{об}^{(y_p)} = X_{AE_{об}}^{(y_p)} \cup X_{AE_в}^{(y_p)} \cup X_{AE_n}^{(y_p)}$; $X_{AE_{об}}^{(y_p)} \cap X_{AE_в}^{(y_p)} = \varnothing$; $X_{AE_{об}}^{(y_p)} \cap X_{AE_n}^{(y_p)} = \varnothing$; $X_{AE_в}^{(y_p)} \cap X_{AE_n}^{(y_p)} = \varnothing$.

Будем считать, что обучающая выборка составляет 80% от исходной обучающей выборки $\left|X_{AE_{об}}^{(y_k)}\right| = 0.8\left|X_{об}^{(y_k)}\right|$, валидационная выборка $\left|X_{AE_в}^{(y_k)}\right| = 0.05\left|X_{об}^{(y_k)}\right|$ – 5%, а выборка для настройки пороговых значений $\left|X_{AE_n}^{(y_k)}\right| = 0.15\left|X_{об}^{(y_k)}\right|$ – 5%.

Полученные выборки будут использоваться для обучения, валидации и настройки пороговых значений.

Для обнаружения изменения в данных воспользуемся моделью автокодировщика $AE : \{X_{вх} \subset X\} \to \{X_{вых} \subset X\}$, обучаемой с помощью алгоритма $\lambda : \{X' \mid X' \subset X\} \to AE\}$.

На каждой обучающей выборке $X_{AE_{об}}^{(y_k)}$ автокодировщик $AE^{(y_k)}$ обучается, что может быть описано в виде $AE^{(y_k)} = \lambda(X_{AE_{об}}^{(y_k)})$.

Введём в рассмотрение индикаторную функцию $I(x) = \begin{cases} 1, \textit{ если x истино} \\ 0, \textit{ в противном случае} \end{cases}$.

Тогда модель обнаружения дрейфа атрибута в группе $D_{атриб}^{гр}$ может быть записана в виде:

$$D_{атриб}^{гр}(G^{(r)}, \hat{G}^{(r)}, n, T_{гр}^{(k)}, T_{экз}^{(k)}, T_n^{(k)}) =$$
$$= I(Q_{атриб}(G^{(r)}, \hat{G}^{(r)}, n) > T_{гр}^{(kn)}) I(T_{n\ атриб\ гр}(G^{(r)}, \hat{G}^{(r)}, n, T_{экз}^{(kn)}) > T_n^{(kn)}),$$

где $G^{(r)}$ – группа экземпляров, для которой обнаруживается дрейф атрибута, $\hat{G}^{(r)}$ – группа реконструированных с помощью автокодировщика экземпляров, n – номер атрибута, для которого обнаруживается дрейф, $T_{гр}^{(k)}$ – множество порогов группы для всех атрибутов приложения k, $T_{экз}^{(k)}$ – множество порогов экземпляров для всех атрибутов приложения k, $T_n^{(k)}$ – множество порогов подсчёта для всех атрибутов приложения k, $T_{гр}^{(kn)} \in T_{гр}^{(k)}$ – порог группы для n-ого атрибута приложения k, $T_{экз}^{(kn)} \in T_{экз}^{(k)}$ – порог экземпляра для n-ого атрибута приложения k, $T_n^{(kn)} \in T_n^{(k)}$ – порог подсчёта для n-ого атрибута приложения k, $T_{n\ атриб\ гр}$ – функция вычисления количества экземпляров группы $G^{(r)}$, для которых потеря восстановления превышает порог экземпляров $T_{экз}^{(kn)}$.

Группа экземпляров считается детектором $D_{атриб}^{гр}$ дрейфующей, если средние потери реконструкции группы $G^{(r)}$, вычисленные с помощью функции $Q_{атриб}$, превышают порог группы $T_{гр}^{(kn)}$, а количество экземпляров группы $G^{(r)}$, для которых потеря восстановления превышает порог экземпляров $T_{экз}^{(kn)}$, превышает порог подсчёта $T_n^{(kn)}$.

Модель обнаружения дрейфа атрибута в потоке $D_{атриб}$ определяется через модель обнаружения дрейфа атрибута в группе $D_{атриб}^{гр}$:

$$D_{атриб}(G, \hat{G}, n, T_{гр}^{(k)}, T_{экз}^{(k)}, T_n^{(k)}, w) =$$
$$\begin{cases} r_{дрейф}, \text{ если } \exists r_{дрейф} > 0 : \left[\prod_{r=r_{дрейф}}^{r_{дрейф}+w} D_{атриб}^{гр}(G^{(r)}, \hat{G}^{(r)}, n, T_{гр}^{(k)}, T_{экз}^{(k)}, T_n^{(k)})\right] > 0, \\ 0, \text{ в противном случае} \end{cases}$$

где G – исходное множество групп экземпляров, $\hat{G}$ – множество реконструированных групп экземпляров, n – номер атрибута, для которого обнаруживается дрейф, $T_{гр}^{(k)}$ – множество порогов группы для всех атрибутов, $T_{экз}^{(k)}$ – множество порогов экземпляров для всех атрибутов, $T_n^{(k)}$ – множество порогов подсчёта для всех атрибутов, w – количество подряд идущих групп, в которых должен определиться дрейф.

Атрибут n считается дрейфующим в потоке, если в множестве экземпляров G обнаруживается w подряд идущих групп, для которых модель $D_{атриб}^{гр}$ в атрибуте n обнаруживает дрейф. Модель возвращает номер группы, с которой начался дрейф, либо 0, если дрейф не обнаружен.

Модель обнаружения дрейфа приложения в потоке $D_{прил}$ определяется через модель обнаружения дрейфа атрибута в потоке $D_{атриб}$:

$$D_{прил}(G, \hat{G}, T_{гр}^{(k)}, T_{экз}^{(k)}, T_n^{(k)}, w) = \{(n, r) \mid r =$$
$$= D_{атриб}(G, \hat{G}, n, T_{гр}^{(k)}, T_{экз}^{(k)}, T_n^{(k)}, w), r > 0, n = \overline{1, N}\},$$

где G – исходное множество групп экземпляров, $\hat{G}$ – множество реконструированных групп экземпляров, $T_{гр}^{(k)}$ – множество порогов группы для всех атрибутов, $T_{экз}^{(k)}$ – множество порогов экземпляров для всех атрибутов, $T_n^{(k)}$ – множество порогов подсчёта для всех атрибутов, w – количество подряд идущих групп, в которых должен определиться дрейф.

Для каждого атрибута с помощью модели обнаружения дрейфа атрибута $D_{атриб}$ определяется дрейф атрибута. Если хотя бы в одном атрибуте обнаруживается дрейф, приложение считается дрейфующим. Модель обнаружения дрейфа приложения $D_{прил}$ возвращает множество пар – номер атрибута n, в котором обнаружен дрейф, и номер группы r, с которой этот дрейф начался. Если в атрибуте n дрейф не обнаружен $(r = 0)$, то он не попадает в результирующее множество. В случае если дрейф не обнаружен ни в одном атрибуте, результирующее множество будет пустым.

Итоговую модель обнаружения дрейфа будет иметь вид:

$$D(X^{(Y)'}, w) = \{(y_k, n, r) \mid (n, r) \in D_{прил}(G^{(y_k)}, AE^{(y_k)}(G^{(y_k)}),$$
$$T_{гр}^{(k)}, T_{экз}^{(k)}, T_n^{(k)}, w), G^{(y_k)} \in g(X^{(y_k)}, V), X^{(y_k)} \in \beta(X^{(Y)'})\} \quad (1)$$

где $X^{(Y)\prime}$ – размеченное множество TCP сеансов, представленное в виде множества пары вектора атрибутов $\vec{x}_m \in X$ и метки класса $y'_m \in Y$, w– количество подряд идущих групп, в которых должен определиться дрейф, $X^{(y_k)}$ – размеченное подмножество TCP сеансов, сгенерированное приложением с меткой класса y_k.

Режим обнаружения дрейфа не предполагает наличия истинных меток и заключается в попытке реконструкции данных с использованием всех АК, подсчёте ошибок реконструкции и на основе порогов принятии решения о наличие или отсутствии дрейфа.

Предлагаемая модель для обнаружения дрейфа основана на механизме обнаружения дрейфа в группах экземпляров. На рисунке 2 приведена структурная схема алгоритма обнаружения дрейфа приложения.

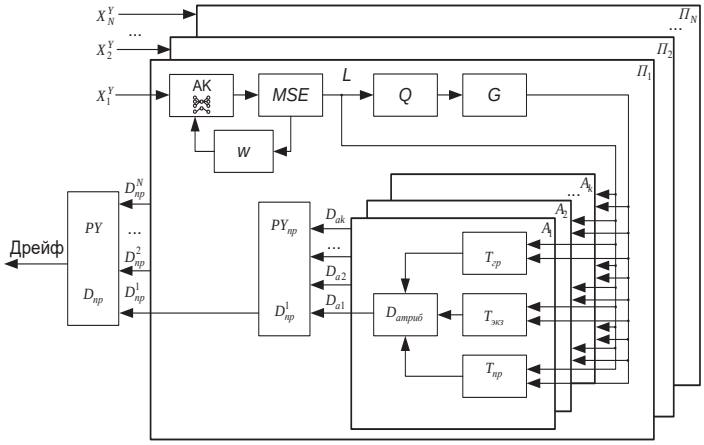

Рис. 2. Структура алгоритма обнаружения дрейфа

На этапе обучения множество АК обучаются на обычных (не дрейфующих) помеченных данных.

Задача обнаружения дрейфа концепции заключается в определении приложений, статистические характеристики признаков которых значительно изменились и качество классификации которых заметно снизилось.

Автокодировщик может быть использован как часть бинарного классификатора. В процессе обучения АК обучается восстанавливать данные, т.е. изучать их структуру. В режиме предсказания АК будет восстанавливать признаки приложения, на котором он обучался с минимальной ошибкой, в то время как при восстановлении признаков других приложений ошибка будет значительно больше.

Обучающее множество $X^{(Y)}_{об}$ разделяется на k подмножеств, равное количеству идентифицируемых приложений. Каждое подмножество $X^{(y_k)}_{об}$ в свою очередь разделяется на обучающее $X^{(y_k)}_{AE_{об}}$, валидационное $X^{(y_k)}_{AE_в}$ множества и множество для настройки порогов приложения $X^{(y_k)}_{AE_n}$. Обучающее множество приложения $X^{(y_k)}_{AE_{об}}$ используется для обучения автокодировщика, а валидационное $X^{(y_k)}_{AE_в}$ – для его оценки.

Множество для настройки порогов $X^{(y_k)}_{AE_n}$ приложения разделяется на группы экземпляров одинакового размера и используется для вычисления порогов экземпляра $T^{(k)}_{экз}$, группы $T^{(k)}_{гр}$ и подсчета $T^{(k)}_n$.

Каждый экземпляр в группе реконструируется (восстанавливается) с помощью обученного АК. Для каждого экземпляра в группах рассчитывается функция потерь. В качестве функции потерь была выбрана среднеквадратичная ошибка $MSE = \frac{1}{N-1}\sum_{i=0}^{N-1}(x_i - \hat{x}_i)^2$. Потери атрибутов в каждой группе усредняются и получаются средние потери атрибута в группе. Усреднив потери атрибутов по группам, получим пороги группы для каждого атрибута $T^{(k)}_{гр} = \{T^{(kn)}_{гр}; n = \overline{1,N}\}$. В каждой группе для каждого атрибута также вычисляется 0,99-квантиль ошибки (значение, которое заданная случайная величина атрибута не превышает с фиксированной вероятностью 0,99). Усреднив по первым нескольким группам $(G^{(r)}; r = \overline{1, R_{уср}}, R_{уср} < R)$, получим пороги экземпляра атрибутов $T^{(k)}_{экз} = \{T^{(kn)}_{экз}; n = \overline{1,N}\}$. В каждой группе вычисляется количество экземпляров, превышающее порог экземпляра. Максимальное значение среди групп будут являться порогами подсчёта атрибутов $T^{(k)}_n = \{T^{(kn)}_n; n = \overline{1,N}\}$.

Если при восстановлении текущего вектора признаков среднеквадратическая ошибка превышает порог экземпляра, значит экземпляр не относится к данному классу. В противном случае считается, что экземпляр относится к данному классу.

В процессе обучения такой модели для каждого класса в обучающей выборке обучается отдельный АК и подбирается порог экземпляра. В процессе предсказания признаки экземпляра подаются на вход всех АК, вычисляется ошибка восстановления экземпляра и сравнивается с порогом экземпляра.

Предсказываемый класс выбирается среди тех АК чья ошибка не превысила порог путем выбора минимальное ошибки. В случае, если пороги превышены для всех АК, приложение считается фоновым или неизвестным.

Реализация разработанного алгоритма обнаружения дрейфа на примере описанного выше набора данных была реализована в рамках программной среды Python. Значения параметров анализируемого трафика приведены в таблице 3.

Таблица 3

Значения параметров потока анализируемого трафика

Параметр	Описание параметра	Значение
M	Общее количество TCP сеансов	30 000
K	Общее количество приложений	6
N	Общее количество атрибутов	21

Для каждого приложения обучаются автокодировщики количество которых равно количеству анализируемых приложений.

Параметры автокодировщиков, реализованных в рамках разработанного алгоритма обнаружения дрейфа концепта представлены в таблица 4.

Таблица 4

Параметры автокодировщика

Тип автокодировщика	Vanilla Autoencoder
Количество слоёв	3 (Input, Bottleneck, Output)
Размерность входного слоя	Количество атрибутов в наборе данных за исключением метки класса (22)
Размерность скрытого слоя	Одна третья от размерности входного слоя (7)
Функция активации	Sigmoid
Оптимизатор	Adam
Функция потерь	MSE
Размер группы (q)	32

Заключение

Разработан алгоритм обнаружения дрейфа концепта приложений, основанный на анализе изменений статистических характеристиках атрибутов или заметного снижения качества классификации анализируемых приложений. В качестве базовой модели детектора дрейфа концепта анализируемых приложений использованы ИНС типа автокодировщик.

Предлагаемый метод использует несколько АК, каждый из которых обучен на соответствующем классе, без дрейфа.

Показано, что если АК обучен только на доброкачественных экземплярах, то он сможет реконструировать нормальные наблюдения, но не может реконструировать аномальные наблюдения (неизвестные понятия). В результате, когда АК фиксирует существенную ошибку реконструкции, это классифицирует данные наблюдения как аномальные**.** Наличие дрейфа оценивается с помощью оценок ошибок реконструкции анализируемых приложений и превышения пороговых значений.

Входящий пакетный поток передается АК на выходе которого вычисляются потери при восстановлении. вычисляются ошибки реконструкции и превышения и сравниваются с соответствующими порогами экземпляра, группы и подсчета. Если два пакет превышает два порога, генерируется предупреждение, а если три последовательных пакета превышают оба порога, то подтверждается дрейф.

Литература

1. *Gama J., Zliobaite I., Bifet A., Pechenizkiy M., Bouchachia A.* A survey on concept drift adaptation // ACMComputing Surveys. 46(4). 2014. DOI: https://doi.org/10.1145/2523813

2. *Schröder T., Schulz M*. Monitoring machine learning models: A categorization of challenges and methods. In Data Science and Management. 2022. DOI: https://doi.org/10.1016/j.dsm.2022.07.004

3. *Oladele S*. A Comprehensive Guide on How to Monitor Your Models in Production – neptune.ai // Página Oficial Neptune AI. 2021. https://neptune.ai/blog/how-to-monitor-your-models-in-production-guide.

4. *Lu N., Zhang G., Lu J*. Concept drift detection via competence models // Artificial Intelligence. No. 209(1), pp. 11-28. 2014. DOI: https://doi.org/10.1016/j.artint.2014.01.001

5. *Schlimmer J. C., Granger R.H*. Incremental Learning from Noisy Data // Machine Learning. 1(3), pp. 317-354. 1986. https://doi.org/10.1023/A:1022810614389

6. *Jaworski M., Rutkowski L., Angelov P*. Concept Drift Detection Using Autoencoders in Data StreamsProcessing. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2020. LNAI vol.12415, pp. 124-133. DOI: https://doi.org/10.1007/978-3-030-61401-0_12

7. *Yong B.X., Fathy Y., Brintrup A*. Bayesian Autoencoders for Drift Detection in Industrial Environments //2020 IEEE International Workshop on Metrology for Industry 4.0 and IoT. 2020, pp. 627-631. https://doi.org/10.1109/MetroInd4.0IoT48571.2020.9138306

8. *Menon A.G., Gressel G*. Concept Drift Detection in Phishing Using Autoencoders// Communications in Computer and Information Science. 2021. Vol. 1366, pp. 208-220. https://doi.org/10.1007/978-981-16-0419-5_17

9. *Шелухин О.И., Барков В.В., Секретарев С.А*. Алгоритмы обнаружения дрейфа концепта при потоковой классификации трафика мобильных приложений // REDS: Телекоммуникационные устройства и системы. 2020. №3. С.19-27.

10. *Sheluhin O.I., Erokhin S.D., Osin A.V., Barkov V.V*. Experimental Studies of Network Traffic of Mobile Devices with Android OS // Systems of Signals Generating and Processing in the Field of on Board Communications. 2019.

11. *Sheluhin O.I., Barkov V.V*. Influence of Background Traffic on the Effectiveness of Mobile Applications Traffic Classification Using Data Mining Techniques // T-Comm: Телекоммуникации и транспорт. 2018. Vol.12. No.10, pp. 52-57.

12. *Шелухин О.И., Ерохин С.Д., Барков В.В*. Создание базы данных сетевого трафика для автоматизации классификации мобильных приложений под управлением операционной системы Android // Нейрокомпьютеры: разработка, применение. 2019. №1. С. 40-51.

13. *Шелухин О.И., Барков В.В*. Экспериментальные исследования и создание базы данных сетевого трафика мобильных устройств под управлением операционной системы Android // Фундаментальные проблемы радиоэлектронного приборостроения: «INTERMATIC-2018». М.: МИРЭА. 2018. Т. 18. №4. С. 1011-1017.

14. *Usman Ali, Tariq Mahmood*. A Novel Framework for Concept Drift Detection using Autoencoders for Classification Problems in Data Streams. 2022. DOI: https://doi.org/10.32388/ZU17S4

15. *Mahmood Yousefi-Azar, Vijay Varadharajan, Len Hamey, Uday Tupakula*. Autoencoder-based feature learning for cyber security applications. In Neural Networks (IJCNN) // 2017 International Joint Conference on. 2017, pp. 3854-3861. IEEE.

16. *Kim Y., Park C.H*. An efficient concept drift detection method for streaming data under limited labeling // IEICE Transactions on Information and Systems, Vol. E100D(10). 2017, pp. 2537-2546. https://doi.org/10.1587/transinf.2017EDP7091

17. *Lu J., Liu A., Dong F., Gu F., Gama J., Zhang G*. Learning under Concept Drift: A Review // IEEE Transactions on Knowledge and Data Engineering. 2019. Vol.31(12), pp. 2346-2363. https://doi.org/10.1109/TKDE.2018.2876857

18. *Pinagé F., dos Santos E.M., Gama J*. A drift detection method based on dynamic classifier selection // Data Mining and Knowledge Discovery. 2020. Vol. 34(1), pp. 50-74. https://doi.org/10.1007/s10618-019-00656-w

19. *Soppin S., Ramachandra M., Chandrashekar B.N*. Essentials of Deep Learning and AI: Experience Unsupervised Learning, Autoencoders, Feature Engineering, and Time Series Analysis with TensorFlow, Keras, and scikit-learn (English Edition). 2021.

20. *Wares S., Isaacs J., Elyan E*. Data stream mining: methods and challenges for handling concept drift // SN Applied Sciences. 2019. No. 1(11). https://doi.org/10.1007/s42452-019-1433-0.

CONCEPT DRIFT DETECTION IN MOBILE APPLICATIONS CLASSIFICATION USING AUTOENCODERS

OLEG I. SHELUHIN,
Moscow, Russia

VYACHESLAV V. BARKOV,
Moscow, Russia

AIRAPET G. SIMONYAN,
Moscow, Russia

KEYWORDS: *classification algorithms, concept drift, data stream, attributes and applications, class labels.*

ABSTRACT

Intoduction: The study observes the task of concept drift detection in multiclass applications classification tasks on the example of collected data set of network traffic in the form of IP packets from **Purpose of the study:** development and software implementation of an algorithm for a concept change detection in tasks of multiclass mobile application traffic classification using ANNs of the autoencoder type (AC). Novelty of the study consists in drift detection of one or several mobile applications based on changes in the statistical characteristics of one or several attributes without usage of true class labels implying ANNs of the autoencoder type. **Results:** The study developed an algorithm for concepts drift of application detection based on the analysis of changes in the statistical characteristics of attributes or a noticeable decrease in the quality of the analyzed applications classification. As for fundamental model of concept drift detector of analyzed applications, the study used autoencoders. The research contains basic theoretical positions of the algorithm creation. The study shows that in case of trained AC only on high-quality prototypes, it will be able to reconstruct normal observations but not abnormal observations (unknown concepts). As a result, when the autoencoder detects a significant reconstruction error, it classifies the observation data as abnormal. Estimation of reconstruction errors of the analyzed applications and excess of threshold value assess the presence of drift. The Python software environment provides the implementation of the presented solution.

REFERENCES

1. J. Gama, I. Zliobaite, A. Bifet, M. Pechenizkiy, A. Bouchachia (2014). A survey on concept drift adaptation. *ACMComputing Surveys*. No. 46(4). DOI: https://doi.org/10.1145/2523813
2. T. Schroder, M. Schulz (2022). Monitoring machine learning models: A categorization of challenges and methods. *Data Science and Management*. DOI: https://doi.org/10.1016/j.dsm.2022.07.004
3. S. ladele (2021). A Comprehensive Guide on How to Monitor Your Models in Production – neptune.ai. *Pagina Oficial Neptune AI*. https://neptune.ai/blog/how-to-monitor-your-models-in-production-guide
4. N.Lu, G. Zhang, J. Lu (2014). Concept drift detection via competence models. *Artificial Intelligence*. No. 209(1), pp. 11-28. DOI: https://doi.org/10.1016/j.artint.2014.01.001
5. J.C. Schlimmer, R.H. Granger (1986). Incremental Learning from Noisy Data. *Machine Learning*. No. 1(3), pp. 317-354. https://doi.org/10.1023/A:1022810614389
6. M. Jaworski, L. Rutkowski, P. Angelov (2020). Concept Drift Detection Using Autoencoders in Data StreamsProcessing. *Lecture Notes in Computer Science* (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). LNAI Vol.12415, pp. 124-133. DOI: https://doi.org/10.1007/978-3-030-61401-0_12
7. B.X. Yong, Y. Fathy, A. Brintrup (2020). Bayesian Autoencoders for Drift Detection in Industrial Environments. *2020 IEEE International Workshop on Metrology for Industry 4.0 and IoT*, pp. 627-631. https://doi.org/10.1109/MetroInd4.0IoT48571.2020.9138306
8. A.G. Menon, G. Gressel (2021). Concept Drift Detection in Phishing Using Autoencoders. *Communications in Computer and Information Science*. Vol. 1366, pp. 208-220. https://doi.org/10.1007/978-981-16-0419-5_17
9. O.I.Sheluhin, V.V. Barkov, S.A. Sekretarev (2020). Concept drift detection algorithms in streaming classification of mobile application traffic. *REDS: Telecommunication devices and systems*. No.3, pp.19-27. (In Rus)
10. O.I. Sheluhin, S.D. Erokhin, A.V. Osin, V.V. Barkov Experimental Studies of Network Traffic of Mobile Devices with Android OS (2019). *Systems of Signals Generating and Processing in the Field of on Board Communications*.
11. O.I. Sheluhin, V.V. Barkov (2018). Influence of Background Traffic on the Effectiveness of Mobile Applications Traffic Classification Using Data Mining Techniques. *T-Comm*. Vol.12. No.10, pp. 52-57.
12. O.I. Sheluhin, S.D. Erokhin, V.V. Network (2019). Barkov traffic database creation for automation of android mobile applications classification. *Neurocomputers*. No.1, pp. 40-51. (In Rus)
13. O.I. Sheluhin, V.V. Barkov (2018). Experimental studies and network traffic database creation of mobile devices with Android OS. *Fundamental'nyye problemy radioelektronnogo priborostroyeniya: "INTERMATIC-2018"* [Fundamental problems of radio-electronic instrumentation: "INTERMATIC-2018"]. Vol. 18. No.4, pp. 1011-1017. (In Rus)
14. Ali Usman, Mahmood Tariq (2022). A Novel Framework for Concept Drift Detection using Autoencoders for Classification Problems in Data Streams. DOI: https://doi.org/10.32388/ZU17S4
15. Mahmood Yousefi-Azar, Vijay Varadharajan, Len Hamey and Uday Tupakula (2017). Autoencoder-based feature learning for cyber security applications. *Neural Networks (IJCNN). 2017 International Joint Conference*, pp. 3854-3861. IEEE.
16. Y. Kim, C.H.Park (2017). An efficient concept drift detection method for streaming data under limited labeling. *IEICE Transactions on Information and Systems*. Vol. E100D(10), pp. 2537-2546. https://doi.org/10.1587/transinf.2017EDP7091
17. J. Lu, A Liu, F. Dong, F. Gu, J.Gama, G. Zhang (2019). Learning under Concept Drift: A Review. *IEEE Transactions on Knowledge and Data Engineering*. Vol. 31(12), pp. 2346-2363. https://doi.org/10.1109/TKDE.2018.2876857
18. F. Pinage, E.M. dos Santos, J. Gama (2020). A drift detection method based on dynamic classifier selection. *Data Mining and Knowledge Discovery*. Vol. 34(1), pp. 50-74. https://doi.org/10.1007/s10618-019-00656-w
19. S. Soppin, M. Ramachandra, B.N. Chandrashekar (2021). Essentials of Deep Learning and AI: Experience Unsupervised Learning, Autoencoders, Feature Engineering, and Time Series Analysis with TensorFlow, Keras, and scikit-learn (English Edition).
20. S. Wares, J. Isaacs, E. Elyan (2019). Data stream mining: methods and challenges for handling concept drift. SN Applied Sciences. No. 1(11). https://doi.org/10.1007/s42452-019-1433-0.

INFORMATION ABOUT AUTHORS:

Oleg I. Sheluhin, PhD, Full Professor, Professor Moscow Technical University of Communications and Informatics, Moscow, Russia
Vyacheslav V. Barkov, Senior lecturer Moscow Technical University of Communications and Informatics, Moscow, Russia
Airapet G. Simonyan, PhD, Docent, Assistant Professor Moscow Technical University of Communications and Informatics, Moscow, Russia

For citation: Sheluhin O. I., Barkov V.V., Simonyan A.G. Concept drift detection in mobile applications classification using autoencoders. *H&ES Reserch*. 2023. Vol. 15. No. 3. P. 20-29. doi: 10.36724/2409-5419-2023-15-3-20-29 (In Rus)

doi: 10.36724/2409-5419-2023-15-3-30-37

ПОДХОД К ФОРМАЛИЗАЦИИ ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕТОДОМ НЕЧЕТКОГО МОДЕЛИРОВАНИЯ

ВОВИК
Андрей Геннадьевич[1]

ЛАРИН
Александр Иванович [2]

АННОТАЦИЯ

Введение: Уровень угроз информационной безопасности в защищаемой системе может быть рассмотрен в качестве входной переменной модели управления информационной безопасностью наряду с другими факторами, характеризующими дестабилизирующие воздействия на систему. Существующие методики оценки угроз представляют собой совокупность неформализованных вербальных моделей, содержащих рекомендации и последовательность действий специалиста. Такие модели позволяют определять комплекс мероприятий, но лишены возможности проводить численные оценки, главным образом численно определять изменения в составе и качестве актуального перечня угроз. В нормативных документах рекомендовано использование исключительно экспертных методов, однако использование экспертных оценок в качестве "точного измерителя" исключает проведение численных оценок в непрерывном режиме, кроме того, рекомендации ФСТЭК по формированию экспертной группы из числа сотрудников защищаемой системы ставит под сомнение объективность такой оценки. **Цель исследования:** Целью исследования является обоснование возможности использования комбинации методов экспертных оценок и методов нечеткого моделирования для проведения численных оценок уровня актуальных угроз информационной безопасности в защищаемой системе. **Методы:** Объект моделирования – процесс оценки уровня актуальных угроз – рассматривается как сложная система с неустранимой неопределенностью. В качестве используемого метода моделирования выбрано сочетание метода экспертных оценок для начального определения численных значений уровня угроз по предложенной экспертам вещественной относительной шкале и метода нечеткого моделирования на основе алгоритма вывода на правилах Мамдани, а также метод структуризации типа "дерево угроз". **Результаты:** Обоснована качественная адекватность предложенной модели, показана возможность оперативного изменения численной оценки общего уровня угроз при идентификации новых угроз, о наличии которых не было известно ранее. **Практическая значимость:** Использование описанного подхода к численной оценке уровня угроз в защищаемой системе позволяет формализовать одну из входных переменных общей модели управления информационной безопасностью.

Сведения об авторах:

[1] ассистент каф. ИСУиА, Московский технический университет связи и информатики, Москва, Россия, a.g.vovik@mtuci.ru

[2] к.т.н., доцент каф. ИСУиА, Московский технический университет связи и информатики, Москва, Россия, a.i.larin@mtuci.ru

КЛЮЧЕВЫЕ СЛОВА: *Управление информационной безопасностью, оценка угроз, нечеткая логика, алгоритм Мамдани.*

Для цитирования: *Вовик А.Г., Ларин А.И.* Подход к формализации оценки угроз информационной безопасности методом нечеткого моделирования // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 3. С. 30-37. doi: 10.36724/2409-5419-2023-15-3-30-37

Введение

Управление информационной безопасностью (УИБ) - процесс, который обеспечивает конфиденциальность, целостность и доступность информационных активов, данных и услуг организации.

Управление информационной безопасностью может быть рассмотрено как часть организационного подхода к управлению безопасностью, который имеет более широкую область охвата, чем компьютерная или сетевая безопасность, и включает обработку бумажных документов, доступ в здания, телефонные звонки и т.п., для всей организации.

В современной терминологии чаще используется понятие «Менеджмент информационной безопасности» [1-3], которое включает в себя действия по управлению организацией, ее контролю и непрерывному совершенствованию в рамках соответствующих структур. Менеджмент охватывает действия, методы или практики формирования и обработки ресурсов, обращения с ресурсами, наблюдения за ними, а также управления ими. Масштаб управленческой структуры варьируется от одного человека в небольших организациях до управленческой иерархии, состоящей из многих людей, в крупных организациях.

В работе учтены требования и рекомендации к управлению ИБ, содержащиеся в следующих нормативных документах:

- ГОСТ Р ИСО/МЭК 27000-27004-2021 Информационная технология. Методы и средства обеспечения безопасности.
- ГОСТ Р ИСО/МЭК15408- 1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1 Введение и общая модель (Общие критерии).
- РД ФСТЭК. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации
- Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.
- Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.
- Банк данных угроз безопасности информации. ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Существующие государственные и ведомственные нормативные акты, регламентирующие вопросы управления информационной безопасностью, содержат вербальные (неформальные) модели, описывающие содержание таких составляющих УИБ как:

- оценка дестабилизирующих факторов (оценка угроз информационной безопасности, оценка информационных рисков);
- оценка актуальности угроз безопасности информации;
- определение информационных активов (информационных ресурсов) системы, на которые может быть направлены угрозы;
- определение негативных последствий от реализации (возникновения) угроз безопасности информации;
- определение управляющих воздействий, т.е. возможных контрмер, которые необходимо применять для снижения возможности реализации тех или иных угроз.

При этом содержание понятия «оценка» используется в качественном аспекте и ограничивается идентификацией и актуализацией угроз, выявлением уязвимостей системы и установлением наличия информационных рисков.

Созданная ФСТЭК система вербальных моделей безусловно полезна и позволяет упорядочить процесс управления информационной безопасностью, однако отсутствие формальных моделей позволяет говорить только о «ручном» управлении информационной безопасностью, основанном на активизации интуиции и опыте специалистов, то есть привлечения экспертов для определения вероятностных характеристик, например реализации угрозы через известную уязвимость.

Такой подход вносит излишнюю субъективность и подверженность ошибкам, обусловленных в том числе и человеческим фактором. Организация сложных экспертиз и получение с их помощью достоверных результатов, вообще говоря, представляет собой достаточно трудно реализуемое мероприятие [4]. Нормативные акты в области УИБ содержат требование проводить оценки угроз и рисков в системе периодически. Так, например, в п.2.4. МД ФСТЭК «Методика оценки угроз безопасности информации» указано, что «оценка угроз безопасности информации должна носить систематический характер и осуществляться как на этапе создания систем и сетей, так и в ходе их эксплуатации, в том числе при развитии (модернизации) систем и сетей. Систематический подход к оценке угроз безопасности информации позволит поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных ресурсов и компонентов систем и сетей».

Отсюда следует, что экспертную группу для проведения такой оценки необходимо создавать достаточно часто (по оценкам авторов на практике периодичность может составлять от 3-х до 6-ти месяцев). Что также усложняет как оперативность таких оценок, так и их реализуемость вообще: с одной стороны, частое привлечение компетентной экспертной группы может создавать организационные трудности, а с другой стороны стремительные развитие информационных технологий и связанное с этим достаточно быстрое качественное и количественное изменение множества актуальных угроз объективно требует как можно более частое проведение оценки угроз, практически в режиме реального времени.

Эффективность управления, основанного на вербальных (описательных) моделях с периодическим привлечением экспертов в качестве измерительного инструмента для численной оценки отдельных вероятностных характеристик, будет достаточно сильно зависеть от многих, не всегда контролируемых факторов. Косвенное подтверждение данного утверждения вытекает из наличия положительной динамики ежегодного роста количества информационных инцидентов [5], а также ежегодного роста размеров причиняемого ущерба различным информационным системам [6]. При этом положительная динамика роста характерна как для Российской Федерации, так и в мировом аспекте.

Под эффективностью управления информационной безопасностью в данном случае понимается постоянный мониторинг уровня защищенности информации в системе (в некоторой численной метрике) и своевременное применение управляющих воздействий (контрмер) для исключения его снижения ниже заранее заданного уровня.

Отсутствие на сегодняшний день формальных моделей является причиной отсутствия обобщенных численных метрик, что в свою очередь не позволяет говорить на современном этапе об автоматических (или хотя бы автоматизированных) системах управления информационной безопасностью. Более того, анализ направленности нормативных документов по управлению информационной безопасностью показывает, что, вообще говоря, даже не ставится задача создания таких систем.

Общая структура модели УИБ

С точки зрения теории автоматического управления на основе обратной связи процесс управления информационной безопасностью может быть представлен в виде сетевой структуры [7] (рис. 1).

Рис. 1. Структурная модель процесса управления информационной безопасностью информационной системы

В представленной модели угрозы информационной безопасности рассматриваются как дестабилизирующее воздействие на защищаемую систему, которое влияет на уровень защищенности информации, определяемый как текущее значение обобщенного показателя эффективности

$$П = F(D_1, D_2, R) \quad (1)$$

где D_1 – уровень актуальных угроз в системе;

D_2 – уровень изменения внутреннего состояния защищаемой системы;

R – конфигурация СЗИ (совокупность применяемых методов и способов защиты информации в системе).

Предполагается, что в системе происходит постоянное численное оценивание текущего значения показателя **П**, который сравнивается в заранее заданным требуемым уровнем защищенности информации в системе $\mathbf{П_0}$ (обобщенный показатель эффективности защиты информации в системе). При выполнении неравенства

$$П \geq П_0 \quad (2)$$

будем считать, что система находится в состоянии заданного уровня защищенности информации и дополнительных регулирующих воздействий на систему не требуется.

В случае, если равенство (1) не выполняется, необходимо формировать управляющее воздействие, которое в модели (рис. 1) представляет собой изменение конфигурации системы защиты информации (СЗИ): добавление нового метода защиты, изменение применяемых способов защиты и т.д.

Для реализации представленной модели необходимо, чтобы все переменные модели могли быть выражены в какой-либо численной метрике. В предыдущей статье «О возможности численных метрик в управлении информационной безопасностью» [7] показан один из возможных способов реализации обобщенной модели управления информационной безопасностью в защищаемой системе. Настоящий материал посвящен проблеме численного оценивания одной из входных переменных модели – оценке уровня угроз информационной безопасности.

Методический документ ФСТЭК «Методика оценки угроз безопасности информации» содержит ряд рекомендаций и определяет последовательность действий для того, чтобы составить множество актуальных угроз информационной безопасности и детализировать их по схеме «источник угрозы – атакуемый информационный актив», при этом для детализации угрозы используется понятие «сценарий реализации угрозы», который включает в себя определение тактики действия нарушителя и используемых им техник.

Вместе с тем, подход к оценке угроз через понятия «сценарии – тактики – техники» с одной стороны позволяет детализировать угрозы и уточнить наличие и характер уязвимостей защищаемой системы, с другой стороны усложняет процедуру и ограничивает поле принятия решений известными сценариями. Если же ограничиться оценкой возможности реализации угрозы через известную уязвимость, это возможно позволит учитывать в конечном счете даже такие сценарии, которые не известны на момент принятия решения.

Кроме того, охватываемая предметная область оценок в указанном документе ограничена рассмотрением только антропогенных угроз и имеет отношение в основном к компьютерной безопасности (сетевые угрозы, угрозы программному обеспечению и проч.).

Практическая реализация представленной на рис.1 модели предполагает численные оценки текущего значения обобщенного показателя эффективности **П** (уровень защищенности информации в системе), а значит необходимо иметь инструментарий для численного определения и других переменных модели, например уровень угроз информационной безопасности (ИБ). При чем в большей степени будет иметь значение возможность оценки изменений этого уровня, а не определение абсолютных значений.

Для определения множества угроз, влияющих на защищаемую информационную систему, и выделения из него подмножества актуальных угроз необходимо руководствоваться

положениями РД ФСТЭК, при этом для формализации результата возможно использовать как классификацию угроз, содержащихся в базе угроз ФСТЕК (bdu.fstec.ru), так и метод «дерева угроз», который является приложением метода «дерева целей» Черчмена [8].

Первый уровень декомпозиции такого «дерева угроз» можно представить в виде – «угрозы доступности», «угрозы конфиденциальности» и «угрозы целостности» и в дальнейшем проводить последовательную декомпозицию актуальных угроз до уровня так называемых элементарных угроз, которые уже не могут быть разложены на составляющие (то есть представлены совокупностью угроз на нижележащем уровне структуризации).

Экспертная оценка может быть использована для определения начальных значений по предложенной экспертам шкале (удобной представляется 10-ти бальная шкала, где «0» означает отсутствие угрозы и «10» – максимально критический уровень угрозы).

Для повышения точности экспертной оценки необходимо произвести декомпозицию угроз до уровня, когда оценка по предложенной экспертам шкале не будет вызывать затруднений. Кроме того, представляется важным выполнение всех известных рекомендаций для формирования экспертной группы и обеспечения необходимого уровня согласованности получаемой экспертной оценки [4].

Общая структура модели оценки общего уровня угроз представлена на рисунке 2.

Рис. 2. Структура модели угроз ИБ в защищаемой системе

Численные значения входных переменных модели Level A, Level I, Level C могут определяться на основании последовательности экспертных оценок, либо быть определяемыми из моделей нижнего уровня.

Выходная переменная модели угроз ИБ – «Общий уровень актуальных угроз» (Threat Level) - в свою очередь является входной переменной в модели управления информационной безопасностью наряду с переменными, численно отражающими внутреннее состояние защищаемой системы, уровень защиты информации в системе (рис. 1). Кроме того, в качестве входной переменной также могут использоваться и другие величины, например коэффициент готовности средств защиты СЗИ.

В различных публикациях последних лет все чаще встречаются обоснования необходимость численных метрик при управлении информационной безопасностью в информационной системе. В том числе, рассматривается возможность применения нечетких методов моделирования для создания моделей управления информационной безопасностью [9-13].

При наличии заранее составленного «дерева угроз» (в данном случае целесообразно говорить об актуальных угрозах), имеющего от четырех до шести уровней декомпозиции, необходимо экспертным путем определить численные веса (k_i) для угроз, которые необходимо считать одинаковыми для i-го уровня декомпозиции. Таким образом, идентификация и актуализация «новой» угрозы, не учтенной ранее в имеющемся «дереве угроз», и последующее определение для этой угрозы соответствующего ей уровня декомпозиции даст численное значение $\Delta(\text{Level X}) = k_i$ (рис. 3).

Новое значение общего уровня угроз, таким образом, будет определяться как

$$(\text{Threat}\_\text{Level})' = \text{F}((\text{Threat}\_\text{Level}), (\Delta(\text{Level}\_\text{X})) \qquad (3)$$

Под **F** в данном случае понимается оператор модели оценки угроз.

Рис. 3. Алгоритм анализа угрозы ИБ в защищаемой системе

Результаты работы приведенного на рисунке 3 алгоритма в последующем учитываются в нечеткой модели оценки уровня угроз ИБ на основе алгоритма Мамдани [14].

Нечеткая модель оценки уровня угроз ИБ

Разработка нечеткой модели осуществлена в MATLAB [15] с использованием пакета Fuzzy Logic Toolbox [16].

Входные переменные модели процесса управления информационной безопасностью (рис. 2) в виде лингвистических переменных на вещественной области определения представлены на рисунках 4,5 и 6, выходная переменная – рисунок 7 (варианты). В качестве вещественной области определения использована условная 10-ти балльная шкала.

Такая размерность обусловлена использованием 10-ти балльной шкалы для экспертной оценки первоначального уровня угроз в системе. Однако следует учитывать, что в случае экспертной оценки такая вещественная область значений будет предположительно дискретной. Для представления же лингвистических переменных целесообразно использовать непрерывную область определения, в том числе для обеспечения непрерывности и относительной точности получаемого результата.

Для задания каждой лингвистической переменной использовано четыре нечетких множества (терма) и кусочно-линейной функции принадлежности нечетким множествам в виде трапеции. По мнению авторов, именно такая форма функции принадлежности наиболее близка интуитивному способу оценивания уровня угроз специалистами.

1. Уровень угроз нарушения конфиденциальности Level C = {низкий, средний, высокий, критический}.

2.

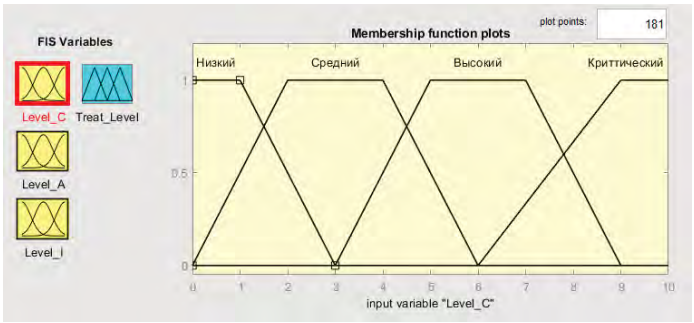

Рис. 4. Лингвистическая переменная модели «Уровень угроз конфиденциальности информации» (Level C)

3. Уровень угроз нарушения доступности Level A = {низкий, средний, высокий, критический}.

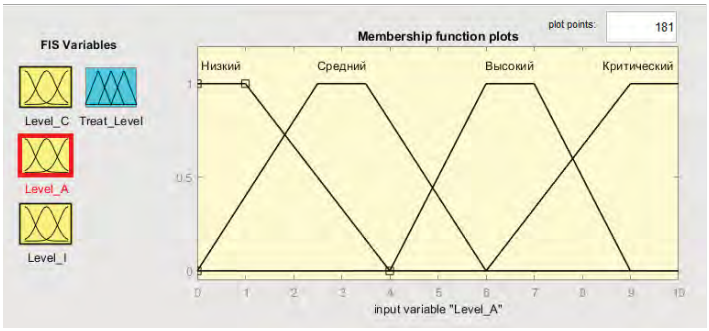

Рис. 5. Входная переменная модели «Уровень угроз доступности информации» (Level A)

4. Уровень угроз нарушения целостности Level I = {низкий, средний, высокий, критический}.

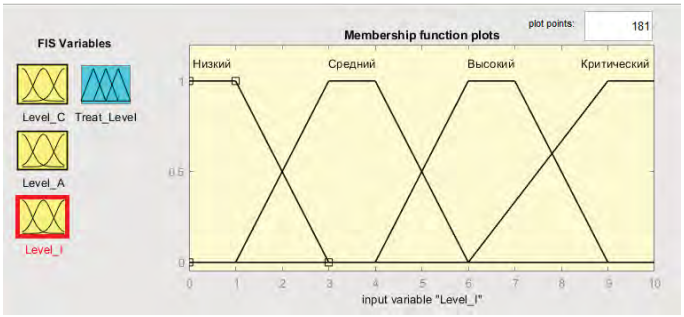

Рис. 6. Входная переменная модели «Уровень угроз целостности информации» (Level I)

Такие лингвистические значения чаще всего используют специалистами при качественных оценках уровня угроз.

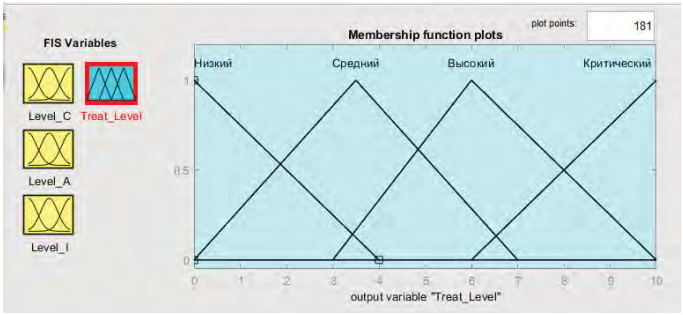

Рис. 7. Выходная переменная модели «Общий уровень актуальных угроз в системе» (Treat Level)

В таблице 1 приведены использованные параметры нечеткой модели Мамдани MISO (вариант).

Таблица 1

Параметры модели

№ пп.	Наименование	Значение
1	OR method	MAX
2	Implication	MIN
3	Agregation	MAX
4	Defuzzification	Centroid
5	Кол-во правил	64
6	Кол-во входных и выходных состояний	50

Прямая графическая интерпретация 4-х мерной модели не представляется возможной, поэтому на рисунке 8 приводится трехмерная проекция модели (Level C – Level A).

В представленной проекции поверхности решения модели, отражающей зависимость общего уровня от угроз (Threat Level) от уровней угроз доступности (Level A) и конфиденциальности (Level C), в качестве метода дефаззификации использован метод Center Of Gravity (CG). Такой метод обеспечивает хорошие чувствительность и неразрывность модели, однако ему присуще и некоторое сужение области дефаззификации.

В приведенном случае проявление такого сужения выражается в том, что изменения выходной переменной (Threat Level) происходят не в ожидаемом диапазоне [0, 10], а в диапазоне [2,66, 8,7]. Однако, учитывая относительность вещественной области определения, а также важность именно изменения текущего состояния выходной переменной модели, а не ее абсолютного значения, с таким «недостатком» модели можно примириться.

Альтернативным решением может быть использование «расширенного метода дефаззификации Extended Center of Gravity, ECG [14]. Метод ECG при изменении параметров модели способен обеспечить изменение значений выходной переменной в ожидаемом диапазоне [0, 10], однако при этом требуется искусственное расширение вещественной области определения входных лингвистических переменных модели в отрицательную область слева, что вряд ли оправдано с точки зрения стремления соответствовать интуитивным представлениям специалистов.

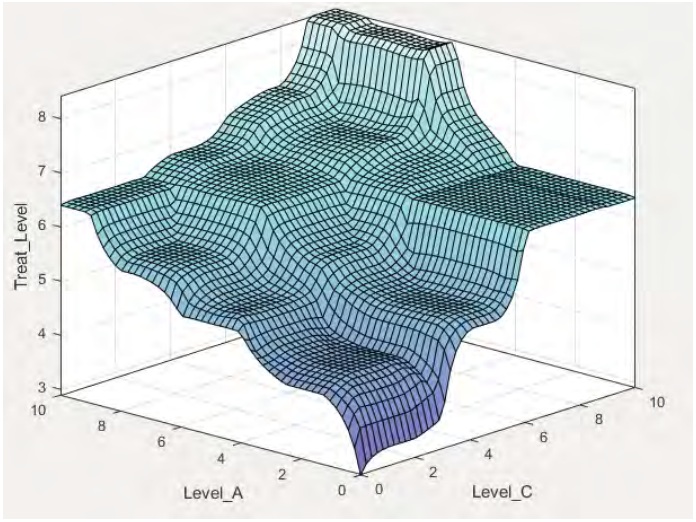

Рис. 8а. Зависимость общего уровня угроз в защищаемой системе (Threat Level) от уровня угроз конфиденциальности (Level C) и доступности (Level A) информации (дефаззификация по методу CG)

С другой стороны, излишнее стремление к максимально чувствительной и неразрывной поверхности решения модели в данном контексте может быть подвергнуто сомнению. В конечном счете специалиста по безопасности может интересовать состояние уровня угроз в защищаемой системе именно в рамках категорий «Низкий уровень – Средний уровень – Высокий уровень – Критический уровень». В таком случае наличие промежуточных значений в численной оценке (рис. 8а) может, в известной степени, создать дополнительную неопределенность с случае «ручного» управления или усложнить структуру системы автоматического управления информационной безопасностью.

Тогда в качестве метода дефаззификации может быть использован метод First of Maxima (FM) [14]. Трехмерная проекция поверхности решения модели представлена на рисунке 8б.

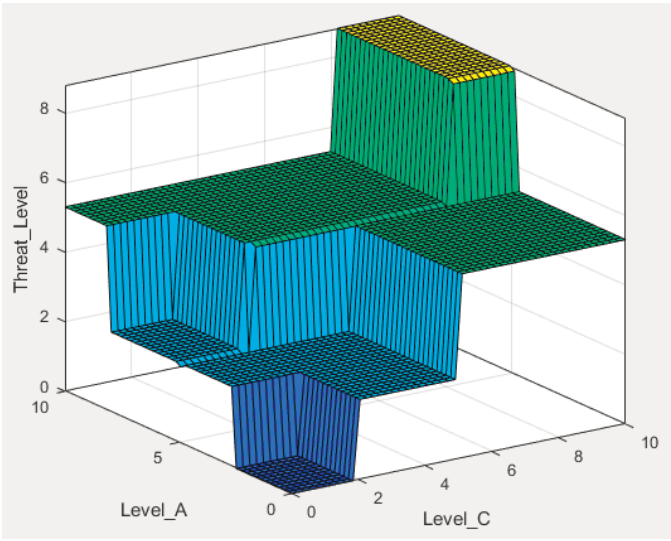

Рис. 8б. Зависимость общего уровня угроз в защищаемой системе (Threat Level) от уровня угроз конфиденциальности (Level C) и доступности (Level A) информации (дефаззификация по методу FM)

Кроме того, метод FM не обладает свойством сужения диапазона выходной переменной, поэтому изменения численных значений на выходе модели (Общий уровень угроз) будут попадать в интервал [0, 10].

Заключение

В результате анализа поверхности проекций модели обоснована качественная адекватность моделируемой системы. На поверхностях всех трех проекций отмечаются локальные области нечувствительности модели. Наибольшие области нечувствительности отмечаются при использовании метода деффаззификации FM.

Наличие областей нечувствительности для обоих методов дефаззификации также объясняется применением при задании входных лингвистических переменных функций принадлежности нечетких множеств в виде трапеций. Вместе с тем, такая форма функций принадлежности, по мнению авторов, вполне соответствует интуитивным представлениям специалистов об использованных лингвистических значениях – низкий, средний, высокий и критический уровни угроз.

В качестве заключения можно отметить, что предложенный в статье подход может быть рассмотрен как попытка авторов перейти от неформальных (вербальных) моделей в управлении информационной безопасностью к формализации с помощью нечетких методов моделирования.

Показано, что такой подход в комбинации с экспертными методами, главным образом, дает возможность численно оценивать изменения дестабилизирующих факторов (например, общего показателя угроз информационной безопасности). И, как видно из предложенной общей структуры модели, в конечном счете позволяет в режиме реального времени контролировать значение общего показателя эффективности – показателя защищенности информации в системе. Экспертная группа в предложенном контексте может быть использована в качестве «точного измерителя» начальных значений

входных переменных модели, а в дальнейшем все изменения входных переменных модели и соответствующие изменения выходной переменной – показателя защищенности информации в системе могут отслеживаться автоматически.

Вместе с тем следует отметить, что альтернативой разработки достаточно сложной структуры нечеткой модели, представляющей собой последовательность двух- или трех- входовых подмоделей может стать искусственная нейронечеткая сеть. Разработка такой сети является следующим этапом исследования.

Литература

1. *Чапрыгина А.Д.* Система менеджмента информационной безопасности. Защита компании от киберугроз. 2021.

2. *Филатов В.В.* и др. Организационно-экономическое риски внедрения систем информационной безопасности предприятия // Известия высших учебных заведений. Технология текстильной промышленности. 2020. №. 2. С. 60-68.

3. *Виноградов В.В., Зелинская М.В.* Менеджмент информационной безопасности в системе предотвращения утечек в государственных учреждениях. 2021.

4. *Волков В.Н., Горелова Г.В., Козлов В.Н.* и др.: под ред. В.Н. Волковой, В.Н. Козлова Математическое моделирование систем и процессов: учебник для академического бакалавриата. М.: Издательство Юрайт, 2018. 450 с. Серия: Баклавр. Академический курс. ISBN 978-5-534-02422-7.

5. *Семеко Г.В.* Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. 2020. №. 1 (1). С. 77-96.

6. *Листопад М.Е., Нагуманов А.З.* Инструменты обеспечения информационной безопасности в экономике России //Экономика: теория и практика. 2020. №. 2. С. 81-86.

7. *Вовик А.Г., Ларин А.И.* О возможности численных метрик в управлении информационной безопасностью // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14, № 6. С. 12-19. DOI 10.36724/2409-5419-2022-14-6-12-19. EDN BRHJMS.

8. *Потапов А.В.* Использование методов системного анализа в системном инжиниринге и бизнесе // Бизнес-инжиниринг сложных систем: модели, технологии, инновации. 2016. С. 207-210.

9. *Ермаков С.А.* и др. Оценка и регулирование рисков нарушения информационной безопасности телекоммуникационных сетей связи и управления промышленного интернета вещей // Информация и безопасность. 2020. Т. 23. №. 1. С. 107-114.

10. *Мельников А.В., Чирков В.Е.* Алгоритм оценки относительного уровня опасности совместной эксплуатации уязвимостей информационной безопасности на основе CVSS // Вестник Воронежского института МВД России. 2019. №. 1. С. 37-44.

11. *Заколдаев Д.А., Гришенцев А.Ю.* Формальная модель обеспечения информационной безопасности при управлении ресурсами на производствах // Системы управления, связи и безопасности. 2021. №. 1. С. 33-61.

12. *Зима В.М., Крюков Р.О., Кравчук А.В.* Методика оценивания информационных рисков на основе анализа уязвимостей // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. №. 11-12. С. 36-46.

13. *Жукова М.Н., Коромыслов Н.А.* Модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики // Известия ЮФУ. Технические науки. 2013. № 12 (149).

14. *Пегат А.* Нечеткое моделирование и управление: пер. с англ. 2-е изд. М.: БИНОМ. Лаборатория знаний, 2017. 798 с.: ил. (Адаптивные и интеллектуальные системы). ISBN 978-5-9963-1495-9.

15. *Buldakova T.I., Mikov D.A.* Matlab application for information security risk analysis // AIP Conference Proceedings. AIP Publishing LLC, 2019. Т. 2195. №. 1. С. 020004.

16. *Goztepe K.* Designing fuzzy rule based expert system for cyber security // International Journal of Information Security Science. 2012. Т. 1. №. 1. С. 13-19.

APPROACH TO FORMALIZING THE ASSESSMENT OF INFORMATION SECURITY THREATS BY THE METHOD OF FUZZY MODELING

ANDREY G. VOVIK,
Moscow, Russia, a.g.vovik@mtuci.ru

ALEXANDER I. LARIN,
Moscow, Russia, a.i.larin@mtuci.ru

KEYWORDS: *Information security management, ehreat assessment, auzzy logic, ьamdani's algorithm.*

ABSTRACT

Introduction: The level of information security threats in the protected system can be considered as an input variable of the information security management model as a destabilizing effect. The existing methods of threat assessment are a set of informal verbal models having recommendations and a sequence of a specialist actions. Such models make it possible to determine a set of measures, but lack the ability to conduct numerical assessments, mainly to numerically determine changes in the composition and quality of the current threats list. The regulatory documents recommend the use of exclusively expert methods. However, the use of expert assessments as an "accurate meter" excludes continuous numerical assessments. Besides, the FSTEC of Russia recommendations on the formation of an expert group from among the employees of the protected system cast doubt on the objectivity of such an assessment. **Research objective:** The research objective is to substantiate the possibility of using a combination of expert assessment methods and fuzzy modeling methods to conduct numerical assessments of the actual information security threats level in a protected system. **Methods:** The object of modeling – the process of assessing the actual threats level – is considered as a complex system with unavoidable uncertainty. The applied modeling method is a combination of the expert assessment method, the fuzzy modeling method and the "threat tree" structuring method. The expert assessment method is used to initially determine the numerical values of the threats level. As a fuzzy algorithm, the basic algorithm of Mamdani inference on the rules is used. **Results:** The qualitative adequacy of the proposed model is substantiated. The possibility of promptly changing the numerical assessment of the overall threats level when identifying new threats, not known before, is shown. **Practical significance:** Using the described approach to the numerical assessment of the threats level in the protected system allows to formalize one of the input variables of the general information security management model.

REFERENCES

1. A.D. Chaprygina (2021). Information security management system. *Protecting the company from cyber threats*. (In Rus)

2. V.V. Filatov et al. (2020). Organizational and economic risks of introduction of information security systems of the enterprise. I*zvestija vysshih uchebnyh zavedenij. Tehnologija tekstil'noj promyshlennosti*. No.. 2, pp. 60-68. (In Rus)

3. V.V. Vinogradov, M.V. Zelinskaya (2021). Information security management in the system of prevention of leaks in public institutions. Economics and management: topical issues of theory and practice: Materialy XVI mezhdunarodnoj nauchno-prakticheskoj konferencii, Krasnodar, 2021, pp. 64-68. (In Rus)

4. A.V. Surin, O.P. Molchanova (2009). Innovation management. Moscow: Infra-M. (In Rus)

5. G.V. Semeko (2020). Information Security in the Financial Sector: Cybercrime and Countermeasures Strategy. *Social'nye novacii i social'nye nauki*. No. 1(1), pp. 77-96. (In Rus)

6. M.E. Listopad, A.Z. Nagumanov (2020). Information security instruments in the russian economy. *Jekonomika: teorija i praktika*. No. 2(58), pp. 81-86. (In Rus)

7. A.G. Vovik, A.I. (2022). Larin Exploring possibility of using numerical metrics in information security management. *H&ES Reserch*. Vol. 14. No. 6, pp. 12-19. doi: 10.36724/2409-5419-2022-14-6-12-19 (In Rus)

8. A.V. Potapov (2016). Using systems analysis methods in systems engineering and business. *Biznes-inzhiniring slozhnyh sistem: modeli, tehnologii, innovacii*, pp. 207-210. (In Rus)

9. S.A. Ermakov et al. (2020). Assessment and risk management of information security breaches of telecommunication communication networks and the management of the industrial internet of things. *Informacija i bezopasnost*. Vol. 23. No. 1, pp. 107-114. (In Rus)

10. A.V. Mel'nikov, V.E. Chirkov (2019). Algorithm for assessing the relative level of danger of joint exploitation of information security vulnerabilities based on CVSS. *Vestnik Voronezhskogo instituta MVD Rossii*. No. 1, pp. 37-44. (In Rus)

11. D.A. Zakoldaev, A.Ju. Grishencev (2021). A formal model for ensuring information security in resource management in production. *Sistemy upravlenija, svjazi i bezopasnosti*. No. 1, pp. 33-61. (In Rus)

12. V.M. Zima, R.O. Krjukov, A.V. Kravchuk (2019). Methodology for information risk assessment based on analysis of vu. *Voprosy oboronnoj tehniki. Serija 16: Tehnicheskie sredstva protivodejstvija terrorizmu*. No. 11-12, p p. 36-46.

13. M.N. Zhukova, N.A. Koromy'slov (2013). A model for assessing the security of an automated system using the apparatus of fuzzy logic. *Izvestiya YuFU. Texnicheskie nauki*. No. 12(149), pp. 63-69.

14. A. Pegat (2012). Nechetkoe modelirovanie i upravlenie (Fuzzy Simulation and Control), Moscow: BINOM. Laboratoriya Znanii. (In Rus)

15. T. I. Buldakova, D.A. Mikov (2019). Matlab application for information security risk analysis. *AIP Conference Proceedings*. AIP Publishing LLC, 2019. Vol. 2195. No. 1. P. 020004.

16. K. Goztepe (2012). Designing fuzzy rule based expert system for cyber security. *International Journal of Information Security Science*. Vol. 1. No. 1, pp. 13-19.

INFORMATION ABOUT AUTHORS:

Andrey G. Vovik, Lecturer at the Department ISUiA, Moscow Technical University of Communications and Informatics, Moscow, Russia
Alexander I. Larin, PhD, Associate Professor at the Department ISUiA, Moscow Technical University of Communications and Informatics, Moscow, Russia

For citation: Vovik A.G., Larin A.I. Approach to formalizing the assessment of information security threats by the method of fuzzy modeling. H&ES Reserch. 2023. Vol. 15. No 3. P. 30-37. doi: 10.36724/2409-5419-2023-15-3-30-37 (In Rus)

doi: 10.36724/2409-5419-2023-15-3-38-46

РАЗРАБОТКА МОДЕЛЕЙ СКРЫТНОГО ВОЗДЕЙСТВИЯ НА ИНФРАСТРУКТУРУ БЕСПРОВОДНЫХ СЕТЕЙ С ПОМОЩЬЮ СИГНАЛОПОДОБНЫХ ПОМЕХ И ОЦЕНКА ИХ УСТОЙЧИВОСТИ К ОБНАРУЖЕНИЮ

МИХАЙЛОВ
Владимир Юрьевич[1]

АБРАМОВ
Артем Андреевич[2]

МАЗЕПА
Роман Богданович[3]

ЯКУШ
Никита Александрович[4]

АННОТАЦИЯ

Введение: В статье анализируются сценарии, при которых, согласно стандарту 802.11, сеансы информационного взаимодействия разрушаются путем отправления фреймов деаутентификации. Объект исследования: беспроводные сети стандарта IEEE 802.11, физическая среда информационного взаимодействия. Предмет исследования: эффективность скрытного воздействия на инфраструктуру беспроводных сетей с помощью сигналоподобных помех. **Цель исследования:** разработка моделей сигналоподобных помех; методов и средств их создания, сценариев применения; оценка устойчивости формируемых сигналоподобных помех и методов их применения к обнаружению. Разработанный программно-аппаратный комплекс производит запись подобного взаимодействия, которая впоследствии используется в качестве сигналоподобной помехи. В качестве аппаратной основы, обеспечивающей запись и трансляцию выборок сигнала выступает USRP NI 2901, а в качестве программной основы – NI LabVIEW 2018, с помощью которой происходит настройка и управление оборудованием USRP. На основе анализа многочисленных источников и результатов собственных экспериментальных исследований сформирована система признаков, используемая в работе для оценки устойчивости сигналоподобной помехи к обнаружению. **Результаты исследования** могут быть применены при настройке автоматических систем администрирования сети (IDS/IPS-систем), что позволит своевременно обнаруживать воздействие, повышая безопасности сетей беспроводной связи.

Сведения об авторах:

[1] Московский авиационный институт (национальный исследовательский университет), Москва, Россия, mihvj@yandex.ru

[2] Московский авиационный институт (национальный исследовательский университет), Москва, Россия, artyom.abramov662@yandex.ru

[3] Московский авиационный институт (национальный исследовательский университет), Москва, Россия, mrb402@mail.ru

[4] Московский авиационный институт (национальный исследовательский университет), Москва, Россия, yachkuch@gmail.com

КЛЮЧЕВЫЕ СЛОВА: *IEEE 802.11, USRP, LabVIEW, сигналоподобная помеха, EAPOL, DoS-воздействие, IDS/IPS-системы.*

Для цитирования: Михайлов В.Ю., Абрамов А.А., Мазепа Р.Б., Якуш Н.А. Разработка моделей скрытного воздействия на инфраструктуру беспроводных сетей с помощью сигналоподобных помех и оценка их устойчивости к обнаружению // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 3. С. 38-46. doi: 10.36724/2409-5419-2023-15-3-38-46

Введение

В настоящее время DDoS-атаки на информационные ресурсы различного уровня и типа наиболее популярны вследствие относительной легкости их создания и высокой эффективности применения. Между тем, существующих механизмов недостаточно для их обнаружения [1]. Потому проблема защиты от подобного рода атак является все более актуальной, в том числе при реализации воздействия на беспроводную сеть стандарта IEEE 802.11.

Одной из причин опасности подобного вмешательства является не только возможность лишить пользователя доступа к информационному ресурсу, но, обладая хорошими вычислительными мощностями, злоумышленник может искусственно инициировать процедуру EAPOL и перехватить хендшейк между легальной точкой доступа (ТД) и легальным пользователем, после чего выделить передаваемый секретный ключ и получить несанкционированный доступ к сети и дешифрованию передаваемого трафика [2, 3].

Одним из основных способов автоматизированной защиты от таких атак является использования IDS/IPS-систем.

Формулировка задачи

Некоторые современные IDS/IPS способны обнаруживать DoS-воздействия фреймами деаутентификации или деассоциации на основе формулируемых правил. В этих правилах указываются признаки, по которым можно в трафике обнаружить воздействие, например, утилитами Kali Linux и др. (aireplay-ng, file2air, Airjack).

Так, самым распространенным протоколом аутентификации ТД пользователя пока является WPA2, который не отвечает современным требованиям безопасности, так как существуют уязвимости процедуры EAPOL, эксплуатация которой может проводится уже упомянутым инструментарием Kali Linux. Однако пришедший на смену более безопасный WPA3 также подвержен подобным воздействиям [4].

В современной научной литературе во многих статьях есть упоминания маркеров (признаков) атакующего воздействия путем инжекции фреймов деаутентификации и деассоциации пользователя и точки доступа (ТД). В статьях [4-12] рассмотрено пять основных признаков DoS-воздействия. Именно на основе этих признаков и формируются правила для IDS/IPS-систем. Однако они направлены на обнаружение нарушения логики работы сетей стандарта IEEE 802.11, возникающей при инжекции фреймов деаутентификации инструментарием Kali Linux.

Очевидно, что само наличие активного сетевого адаптера злоумышленника и искусственная инжекция пакетов на логическом уровне не обеспечивает скрытность атакующего воздействия. Только переход на нижний (физический) уровень модели OSI должен решить проблему скрытности [13, 14]. То есть необходимо разработать такие модели сигналоподобных помех, которые бы оказывали воздействие не на логическом, а на физическом уровне, не нарушая логику работы стандарта 802.11 при отсутствии работы какого-либо сетевого адаптера. разработка моделей сигналоподобных помех; методов и средств их создания, сценариев применения; оценка устойчивости формируемых сигналоподобных помех и методов их применения к обнаружению.

Целью исследования является разработка и апробация моделей сигналоподобных помех для нарушения доступности ТД или для компрометации соединения клиента с ТД при перехвате процедуры EAPOL. Необходимо спроектировать методы и средства формирования помех, а также сценарии их применения. Кроме того, важно оценить устойчивость формируемых сигналоподобных помех на физическом уровне и методов их применения к обнаружению с помощью выбранных признаков.

Обоснование выбора оборудования программно-аппаратного комплекса

В качестве аппаратной основы выступает оборудование компании National Instruments USRP NI 2901, а программной – NI LabVIEW 2018, с помощью которой происходит настройка и управление оборудования USRP. Прототипом виртуальных инструментов (VI), выполняющих запись и воспроизведение радиосигнала, выбран проект «NI USRP Record and Playback – I16». Его особенностью является то, что запись и воспроизведение выполняются одним виртуальным прибором с удобным интерфейсом из нескольких вкладок [15]. Во вкладке «Record» и «Payback» необходимо выставить настройки конфигурации приемника и передатчика: имя USRP, несущая частота записи, частота I/Q выборок, усиление записанного сигнала, выбор активной антенны и размер буфера (рис. 1).

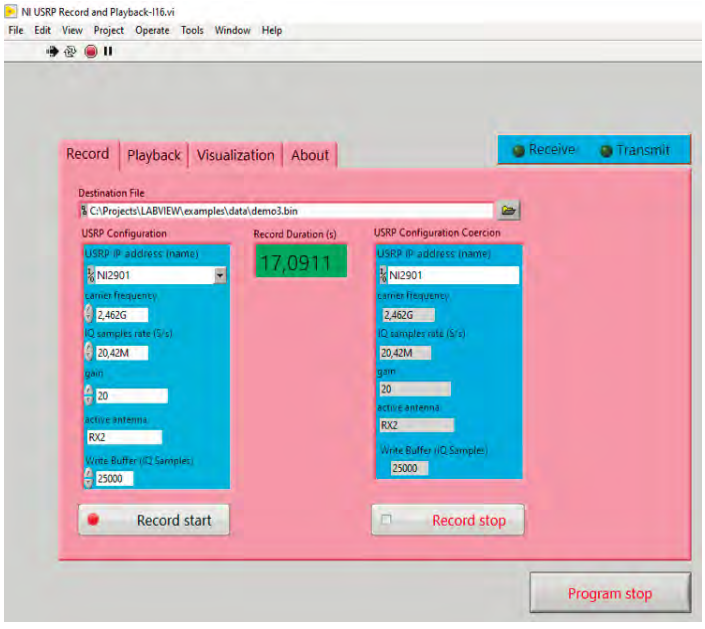

Рис. 1. Настройка конфигурации USRP 2901

Для обнаружения в информационном канале интересующих нас пакетов и последующего анализа передаваемого трафика использовалось средство сетевого анализатора Wireshark [16].

A. Отключение пользователя от точки доступа

Один из наиболее часто встречающихся штатных состояний протокольной машины стандарта 802.11, при которой отправляется служебный пакет деаутентификации, – это отключение пользователя от точки доступа (ТД), например, путем выключения модуля Wi-Fi на устройстве пользователя или переподключение к другой ТД. На рисунке 2 изображена схема эксперимента.

Пользователь (XiaomiCo_b5:cf:87) отключает модуль Wi-Fi на телефоне, отправляя пакет деаутентификации к ТД (ComplexPt_24:25:26). USRP 2901 записывает этого взаимодействие. Далее USRP 2901 транслирует записанную помеху и отключает пользователя от ТД.

Рис. 2. Схема эксперимента «А»

На рисунке 3 видно, как в записи зафиксирована отправка фрейма деаутентификации.

166	3.598370328	XiaomiCo_b5:cf:87	IPv4mcast_02	802.11	140 Data, SN=608, FN=0, Flags=
167	3.605869618	XiaomiCo_b5:cf:87	IPv4mcast_fb	802.11	142 QoS Data, SN=2631, FN=0, F
168	3.605892870		XiaomiCo_b5:cf:87 (7c:d6:…	802.11	70 Acknowledgement, Flags=...
169	3.605894971	XiaomiCo_b5:cf:87	IPv6mcast_16	802.11	246 QoS Data, SN=73, FN=0, Fla
170	3.605896863		XiaomiCo_b5:cf:87 (7c:d6:…	802.11	70 Acknowledgement, Flags=...
171	3.607322966	XiaomiCo_b5:cf:87	IPv6mcast_16	802.11	244 Data, SN=609, FN=0, Flags=
172	3.607823038	XiaomiCo_b5:cf:87	ComplexPt_24:25:46	802.11	86 Deauthentication, SN=3368,
173	3.608085406		XiaomiCo_b5:cf:87 (7c:d6:…	802.11	70 Acknowledgement, Flags=...
174	3.686911791	ComplexPt_24:25:46	Broadcast	802.11	202 Beacon frame, SN=2322, FN=
175	3.710614627	c6:33:96:5d:fc:20	Broadcast	802.11	267 Beacon frame, SN=1183, FN=
176	3.789232374	ComplexPt_24:25:46	Broadcast	802.11	202 Beacon frame, SN=2323, FN=
177	3.891334083	ComplexPt_24:25:46	Broadcast	802.11	202 Beacon frame, SN=2324, FN=

Рис. 3. Интерпретация записи первой модели сигналоподобной помехи

На рисунке 4 представлена трансляция записанной помехи. Пользователь получил фрейм деаутентификации и, следуя логике стандарта отключается от точки доступа, хотя не инициировал разрыв соединения. Порядковый номер SN=3368 доказывает, что это именно записанный ранее фрейм деаутентификации. Этот маркер также понадобится в дальнейшем для обнаружения подобных помех.

1351	12.545950657	ComplexPt_24:25:46	Shenzhen_86:b3:5d	802.11	196 Probe Response, SN=358, FN
1352	12.547832438	ComplexPt_24:25:46	Shenzhen_86:b3:5d	802.11	196 Probe Response, SN=358, FN
1353	12.572325828	ComplexPt_24:25:46	Broadcast	802.11	202 Beacon frame, SN=359, FN=0
1354	12.613478304	ComplexPt_24:25:46	Broadcast	802.11	202 Beacon frame, SN=2319, FN=
1355	12.626236498	XiaomiCo_b5:cf:87	ComplexPt_24:25:46	802.11	86 QoS Null function (No data
1356	12.626486269		XiaomiCo_b5:cf:87 (7c:d6:…	802.11	70 Acknowledgement, Flags=...
1357	12.627465547	XiaomiCo_b5:cf:87	IPv4mcast_02	802.11	140 Data, SN=608, FN=0, Flags=
1358	12.634874963		XiaomiCo_b5:cf:87 (7c:d6:…	802.11	70 Acknowledgement, Flags=...
1359	12.634887126		XiaomiCo_b5:cf:87 (7c:d6:…	802.11	70 Acknowledgement, Flags=...
1360	12.636893133	XiaomiCo_b5:cf:87	ComplexPt_24:25:46	802.11	86 Deauthentication, SN=3368,
1361	12.637147097		XiaomiCo_b5:cf:87 (7c:d6:…	802.11	70 Acknowledgement, Flags=...
1362	12.644979664	HuaweiDe_a4:91:79	c6:33:96:5d:fc:20	802.11	84 Null function (No data), S
1363	12.646618397		c6:33:96:5d:fc:20 (c6:33:…	802.11	70 Acknowledgement, Flags=...
1364	12.674981142	ComplexPt_24:25:46	Broadcast	802.11	202 Beacon frame, SN=360, FN=0
1365	12.715905474	ComplexPt_24:25:46	Broadcast	802.11	202 Beacon frame, SN=2322, FN=
1366	12.733927427	3a:50:b3:46:24:74 (3a:50:…	Broadcast (ff:ff:ff:ff:ff…	802.11	76 CF-End (Control-frame), FI

Рис. 4. Интерпретация трансляции первой модели сигналоподобной помехи

Данная модель помехи опасна тем, что может быть использована не только в качестве DoS-воздействия при итеративной трансляции одной и той же записи, но и для инициации процедуры EAPOL. Если пользователь вручную попытается подключиться к ТД, то злоумышленник может записать с помощью USRP хендшейк и дешифровать пароль, что нарушит конфиденциальность канала связи. Чтобы защититься от повторного хендшейка с ТД, пользователю следует использовать параметр «автоподключение» к ТД. В подобной ситуации большинство устройств не будет инициировать EAPOL при получении одного фрейма деаутентификации. Отметим, однако, что это действие снизит безопасность пользователей по отношению к подменным точкам доступа (спуффинг-атакам).

B. Смена радиоканала точки доступа

Другой причиной отправки фрейма деаутентификации может служить смена радиоканала ТД. На рисунке 5 представлена схема с участниками сценария данного взаимодействия.

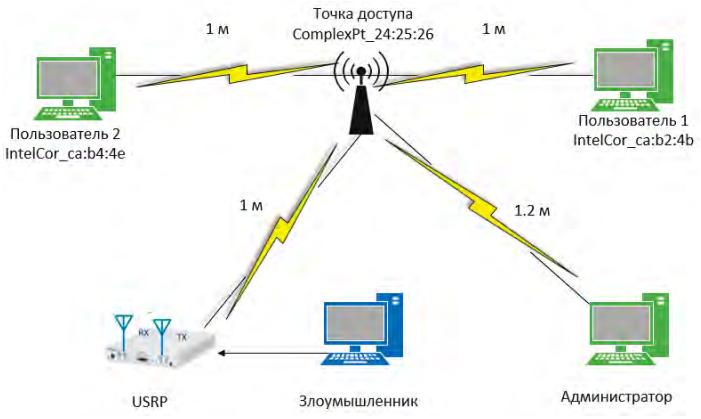

Рис. 5. Схема эксперимента «В»

Два пользователя используют общую сетевую папку по протоколу SMB, скачивая некоторый файл. Однако в данном сценарии в работу локальной сети вмешивается Администратор: он переводит ТД с 11-го радиоканала на пятый, меняя частоту несущей с 2.462 ГГц на 2.432 ГГц. При реализации данного изменения ТД отправляет широковещательный фрейм деаутентификации с кодом 0x03 (рис. 6) – станция покидает или покинула IBSS (Independent Basic Service Set) или ESS (Extended Service Set).

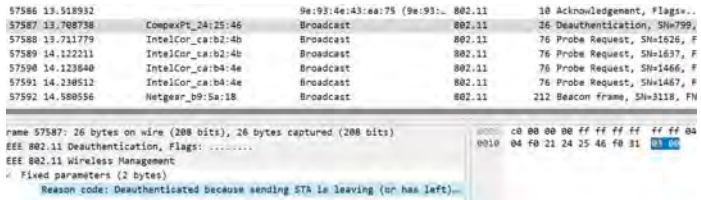

Рис. 6. Интерпретация трансляции второй модели сигналоподобной помехи

После записи данной сигналоподобной помехи администратор возвращает ТД на прежний 11-ый радиоканал.

После того, как пользователи снова подключаются к ТД на прежнем радиоканале, включается трансляция помехи USRP. Интерпретацию воздействия помехи на логическом уровне видно на рисунке 7. USRP транслирует в радиоканал ранее записанный фрейм с номером SN=799, который отключает всех пользователей, хотя ТД не меняет радиоканал вещания. Однако примерно через 0.5 секунды на рисунке 7 ниже видно, что пользователи, обнаруживая присутствие ТД (Beacons) снова пытается к ней подключиться, инициируя процедуру EAPOL, что в свою очередь может перехватить USRP злоумышленника.

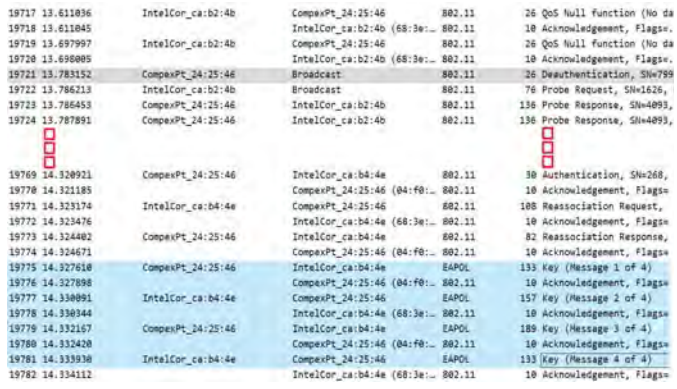

Рис. 7. Обнаружение процедуры EAPOL после воздействия помехи

C. Имитация загруженности радиоканала

Сценарий формирования сигналоподобной помехи, которая упоминается в статье [15], сводится к тому, чтобы записать активное взаимодействие двух и более пользователей, что имитирует передачу трафика пользователями через одну и ту же ТД (рис. 8). Примером такого сценария является обращение пользователей к какому-то видеохостингу для просмотра видео в высоком разрешении. Тем самым имитируется загруженность радиоканала, так как передаются большие объемы данных.

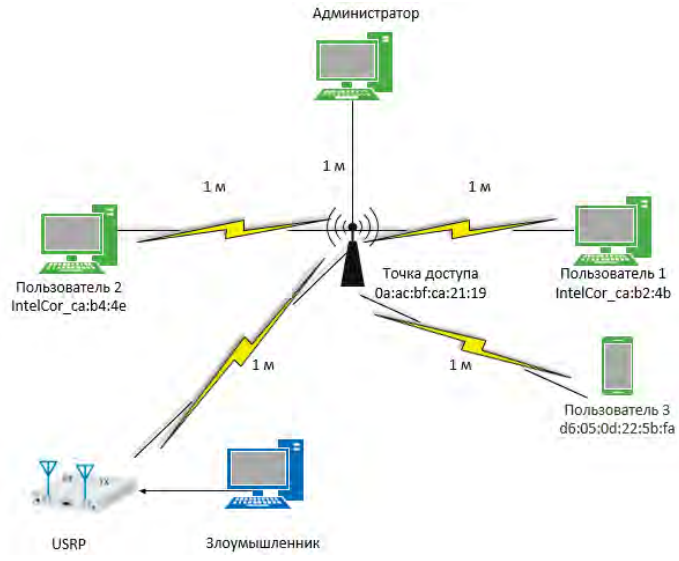

Рис. 8. Схема эксперимента «C»

Трансляция подобной помехи при дальнейшем взаимодействии тех же самых пользователей приводит к падению скорости передачи трафика вплоть до полной остановки.

С одной стороны, DoS-воздействие заключается в том, что срабатывает защитный механизм обхода коллизий протокола RTS/CTS [17, 18], который не позволяет передавать легитимный трафик во время трансляции помехи. С другой стороны, ТД (0a:ac:bf:ca:21:19), интерпретируя помеху (рис. 9), обнаруживает в ней «новые» потоки данных от пользователей, которые на самом деле уже давно были переданы и реагирует на них фреймами деаутентификации с кодом ошибки 0x07 (кадр класса 3, полученный от неассоциированной станции).

Однако в статье [15] утверждается, что ТД в таком случае отправляет фрейм с кодом ошибки 0x06 (кадр класса 2 получен от неаутентифицированной станции). Это вероятно объясняется тем, что особенности реализации протокольных машин стандарта 802.11 у каждого производителя различаются. При формировании универсальных методов обнаружения сигналоподобных помех важно учитывать эти особенности.

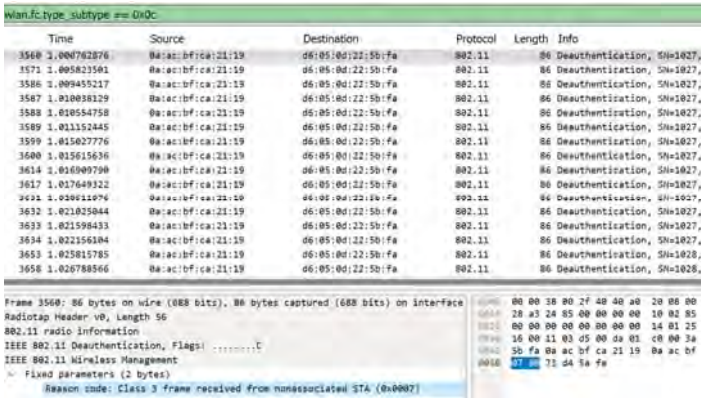

Рис. 9. Интерпретация трансляции третьей модели сигналоподобной помехи

D. Добавление пользователя в черный список

Данный сценарий реализует ситуацию добавления пользователя администратором в черный список ТД в то время, когда пользователь еще подключен (рис. 10).

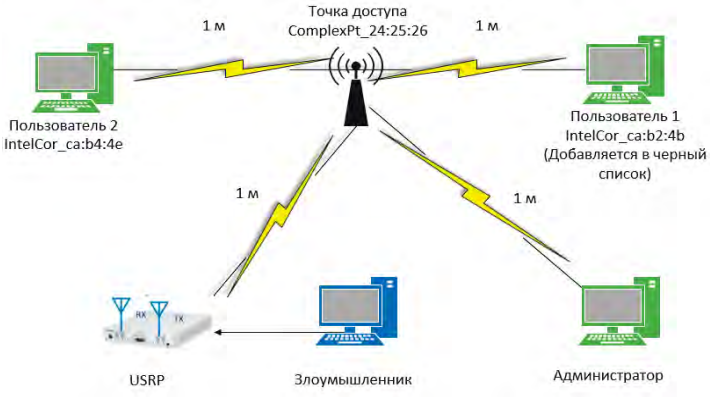

Рис. 10. Схема эксперимента «D»

После сохранения настроек ТД администратором, она отправляет фрейм деаутентификации соответствующему пользователю, разрывая соединение с ним. На рисунке 11 видно, как в результате трансляции пользователь неожиданного получает этот фрейм с кодом ошибки 0x02 (Предыдущая ассоциация больше недействительна).

Рис. 11. Интерпретация трансляции четвертой модели сигналоподобной помехи

Интересная особенность подобного воздействия заключается в том, что администратор не сможет понять, почему пользователь отключился от ТД (рис. 12), т.к. в настройках роутера пользователь отображен как подключенный (его никто не вносил в черный список), потому что ТД не отправляла никаких фреймов деаутентификации: разрыв соединения – это реакция на записанную помеху.

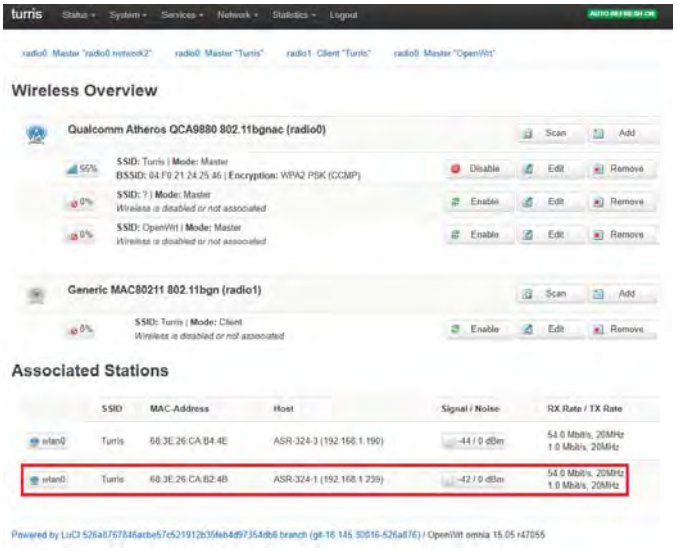

Рис. 12. Интерфейс настройки черного списка ТД

Как и в пункте «В», клиенту придется снова запускать процедуру EAPOL, компрометируя хеш своего пароля (рис. 13).

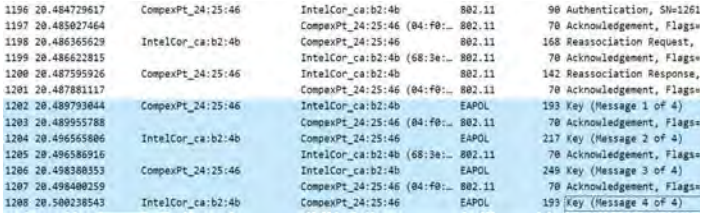

Рис. 13. Инициирование процедуры EAPOL

E. Отключение радиоинтерфейса ТД

Пятым примером сигналоподобной помехи будет реализация сценария, при котором администратор отключает радиоинтерфейс Wi-Fi ТД, по которому пользователи обменивались данными (рис. 14).

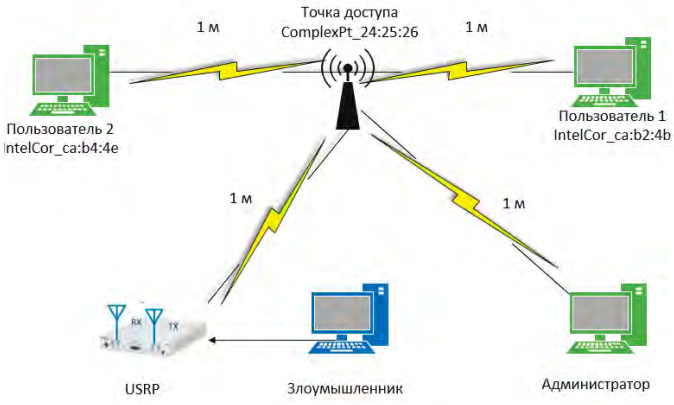

Рис. 14. Схема эксперимента «E»

При отключении радиоинтерфейса ТД также посылает широковещательный фрейм деаутентификации с кодом ошибки 0x03 (рис. 15). Все пользователи, получая подобный фрейм, также отключаются от ТД. Однако уже при повторном подключении снова запускается EAPOL.

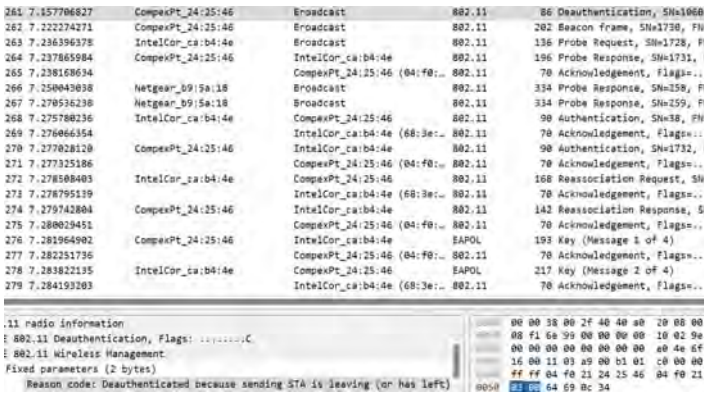

Рис. 15. Интерпретация трансляции пятой модели сигналоподобной помехи

Методы обнаружения воздействия сигналоподобной помехой

Как уже было упомянуто ранее, в научной литературе, посвященной теме обнаружения DoS-атак рассматриваются, в основном, пять основных признаков воздействия:

1. Отправка большого количества фреймов управления.
2. Код причины 0x07.
3. Изменение мощности сигнала.
4. Неверное отображение порядковых номеров фреймов.
5. Незначительное изменение метки времени.

Отправка большого количества фреймов управления. В статьях [4-7] утверждается, что независимо от сценария атаки (широковещательной, направленной от ТД на всех

участников сети, или направленной только на конкретного пользователя сети) происходит инжекция большого количества фреймов деаутентификации за короткий промежуток времени. Например, утилита aireplay-ng отправляет обычно 256 фреймов деаутентификации, что, безусловно, нарушает логику работы стандарта IEEE 802.11. Однако во всех представленных интерпретациях разработанных пяти моделей сигналоподобных помех такие аномалии с подряд идущими фреймами деаутентификации обнаружены не были. Это связано с тем, что USRP не инжектирует искусственно созданные фреймы, а транслирует запись радиосигнала, который интерпретируется Wireshark (а следовательно, и администратором) как естественный диалог между пользователем и ТД. То есть запись содержит как сам нужный злоумышленнику фрейм деаутентификации, так и другое случайное множество фреймов диалога, маскируя тем самым свое воздействие и обеспечивая его скрытность. Исключением является модель «C», которая инициирует отправку большого количества фреймов деаутентификации легальной ТД.

Код причины 0x07.

Согласно статьям [4, 5, 8-10], во время атакующего воздействия все инжектируемые фреймы имеют код ошибки 0x07 (кадр класса 3, полученный от неассоциированной станции). При анализе пяти моделей помех было обнаружено, что практически во всех записанных сценариях ТД отправляла другие коды ошибки: в модели «A», «B», «E» – 0x03, «C» – 0x06 или 0x07, «D» – 0x02. Таким образом, только в одном случае был отправлен код ошибки 0x07. При этом важно отметить, что выбор кода ошибки может различаться в зависимости от прошивки производителя ТД. Однако обнаружить помеху по данному признаку маловероятен.

Изменение мощности сигнала.

Так как изменение средней мощности принимаемого сигнала является функцией расстояния от передающего устройства до приёмного, то в случае, если ТД злоумышленника будет находиться ближе к атакуемому при том, что условия распространения электромагнитной волны будут примерно одинаковы, то принимаемый сигнал от нее будет мощнее, и наоборот. То есть IDS/IPS-система может обнаружить аномальный скачок средней мощности сигнала во время атакующего воздействия.

Преимуществом применения USRP является то, что устройство обладает возможностью гибкой настройки средней мощности сигнала. Так, в проекте «NI USRP Record and Playback – I16» есть настройка параметра усиления сигнала «gain» (рис. 16). Таким образом, разницу расстояния от легальной ТД до пользователя и от USRP до пользователя можно нивилировать регулировкой этого параметра. Поэтому с помощью USRP можно обойти данный признак обнаружения.

Неверное отображение порядковых номеров фреймов.

Безусловно, нарушение последовательности порядковых номеров – важный признак обнаружения воздействия, причем неважно, фреймами деаутентификации или деассоциации реализуют DoS-воздействие.

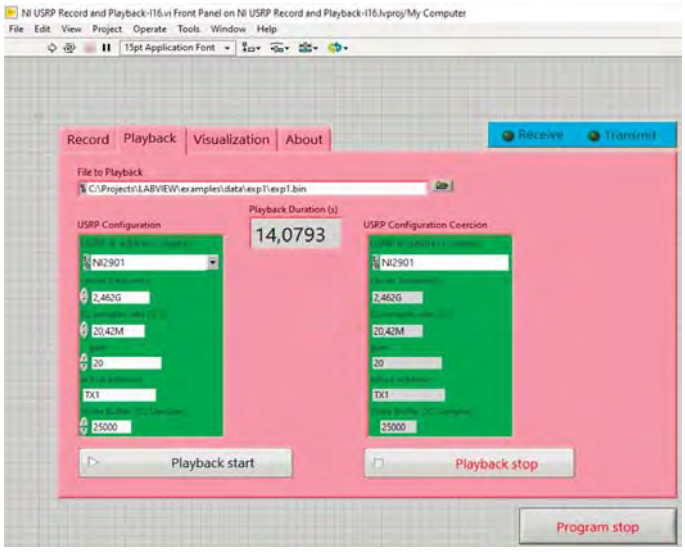

Рис. 16. Настройка усиления «gain» во вкладке трансляции

В статье [11] отмечено, что злоумышленник может определить порядковый номер текущего фрейма сеанса пользователя и ТД и начать воздействия не с нулевого, а с нужного номера, чтобы избежать обнаружения. Однако распространенные утилиты начинают инжекцию с нулевого номера (SN=0), нарушая порядок. Данный маркер можно применить и для сигналоподобных помех, хотя и с некоторыми оговорками. На рисунке 17 видно, как в записи первого эксперимента («A») наблюдается некая последовательность фреймов SN=1716…1723 и следующих фреймов (в фильтре Wireshark указана сортировка по времени только фреймов от пользователя к ТД).

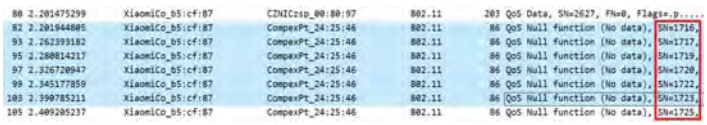

Рис. 17. Подмножество фреймов записанной помехи

Эта же последовательность видна уже при трансляции помехи (рис. 18). Зеленым цветом указано подмножество фреймов легального трафика, которые передавался в моделе «A», а красным – подмножество интерпретации помехи.

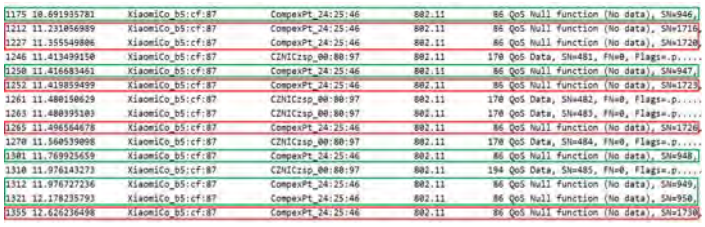

Рис. 18. Разделение подмножеств фреймов помехи и легального трафика

На рисунке 18 видно, как помеха нарушает порядок SN: после номера 946 неожиданно идет скачок к номеру 1716, и такая аномалия наблюдается на протяжении всего выделенного фрагмента.

То есть теоретически система обнаружения воздействия может хранить в некотором буфере порядковый номер фрейма и при резком изменении, считать его одим из признаков начала воздействия.

Незначительное изменение метки времени.

Формально, этот признак тесно связан с первым признаком количества фреймов управления [11]. Однако в этом признаке отслеживается не количество фреймов управления, а их интенсивность, которую можно отслеживать по метке времени фрейма. Утилиты реализуют инжекцию фреймов управления с высокой интенсивностью, поэтому метка времени изменяется незначительно. Если использовать разработанные 5 моделей помех не в качестве DoS-воздействия, а с целью перехвата процедуры EAPOL, то их обнаружить будет невозможно, так как в помехе интерпретируется лишь один фрейм управления. Как было упомянуто ранее, исключением является модель «C»: хотя, формально, помеха не содержит ни одного фрейма управления, она приводит к тому, что легальная ТД начинает инициировать эти самые фреймы в большом количестве, что в свою очередь и будет замечено системой мониторинга.

Таким образом, результаты анализа скрытности сигналоподобных помех можно представить в таблице 1, где столбцы – известные в научной литературе актуальные признаки обнаружений DoS-атак, а строки – методы воздействия. Если признак может обнаружить воздействие, то на пересечении ставится соответствующая отметка «✓».

Таблица 1

Эффективность обнаружения воздействия

	Отправка большого количества фреймов управления	Код причины 0x07	Изменение мощности сигнала	Неверное отображение порядковых номеров фреймов	Незначительное изменение метки времени
Утилиты aireplay-ng и др.	✓	✓	✓	✓	✓
Модель «A»				✓	
Модель «B»				✓	
Модель «C»	✓	✓		✓	✓
Модель «D»				✓	
Модель «E»				✓	

Таким образом, сигналоподобные помехи достаточно трудно обнаружить без модификации существующих систем защиты.

Заключение

1. В статье разработаны пять моделей и сценариев применения сигналоподобных помех, реализующих DoS-воздействие с целью нарушения доступа к инфраструктуре беспроводной сети или компрометации соединения. В основе записанных сценариев лежат состояния протокольной машины стандарта IEEE 802.11, при которых пользователь или ТД отправляет фрейм деаутентификации.

2. Проведена успешная апробация всех разработанных моделей сигналоподобных помех, доказавших свою эффективность как с позиции DoS-воздействия, так и инициацией процедуры EAPOL для дешифрования трафика. Запись и трансляция сигнала выполнено с помощью программно-аппаратного комплекса: USRP 2901 и проекта «NI USRP Record and Playback - I16» в среде LabVIEW 2018.

3. Выполнен анализ известных признаков обнаружения DoS-воздействий в современной научной литературе. Выделено пять основных признаков, которые используются в современных IDS/IPS-системах: отправка большого количества фреймов управления, код причины 0x07, изменение мощности сигнала, неверное отображение порядковых номеров фреймов, незначительное изменение метки времени.

4. Анализ скрытности разработанных сигналоподобных помех показал их высокую эффективность. Во-первых, при трансляции нет наличия активного сетевого адаптера злоумышленника в отличии от варианта инжекции пакетов на логическом уровне, которые компрометируют атакующее воздействие злоумышленника. Во-вторых, анализ трафика записи и трансляции помех в Wireshark показал, что четыре из пяти моделей практически никак не нарушают логику работы стандарта IEEE 802.11, в отличие от утилит, осуществляющих инжекцию на логическом уровне. Для обнаружения сигналоподобных помех в системах мониторинга необходимо уточнить признак нарушения порядкового номера SN, так как сброс до 0 не происходит и возможно минимальное изменение номера. Также в дальнейшем необходимо дополнить признаки обнаружения DoS-воздействий с учетом особенностей реализации сигналоподобных помех.

Литература

1. *Uygar Dincalp, Mehmet Serdar Güzel, Omer Sevine, Erkan Bostanci, Iman Askerzade.* Anomaly Based Distributed Denial of Service Attack Detection and Prevention with Machine Learning // 2018 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey. DOI: 10.1109/ISMSIT.2018.8567252.

2. *Abdelrahman A., Khaled H., Shaaban Eman, Elkilani Wail S.* WPA-WPA2 PSK Cracking Implementation on Parallel Platforms // 2018 13th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt. DOI: 10.1109/ICCES.2018.8639328.

3. *David Janos Feher, Barnabas Sandor*. Effects of the WPA2 KRACK Attack in Real Environment // 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia. DOI: 10.1109/SISY.2018.8524769.

4. *Neil Dalal, Nadeem Akhtar, Anubhav Gupta, Nikhil Karamchandani, Gaurav S. Kasbekar, Jatin Parekh.* A Wireless Intrusion Detection System for 802.11 WPA3 Networks // 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bangalore, India, January, 2022. DOI: 10.1109/COMSNETS53615.2022.9668542

5. *Korolkov R., Kutsak S., Voskoboinyk V.* Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection, 2021.

6. *Jaspreet Kaur*. Mac Layer Management Frame Denial of Service Attacks // 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), 2017.

7. *Pratik Satam, Salim Hariri*. WIDS: An Anomaly Based Intrusion Detection System for Wi-Fi (IEEE 802.11) Protocol // IEEE Transactions on Network and Service Management, Vol. 18, Issue 1, March 2021.

8. *Rajinder Singh1 and Satish Kumar*. A light weight solution for detecting de-authentication attack // International Journal of Network Security & Its Applications (IJNSA), Vol. 11, No.1. 2019.

9. *Afzal Z., Rossebø J., Talha B., Chowdhury M.* A Wireless Intrusion Detection System for 802.11 networks // 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 828-834.

10. *Eian M*. Fragility of the robust security network: 802.11 denial of service // International Conference on Applied Cryptography and Network Security, LNSC, Vol. 5536, 2009, pp. 400-416.

11. *Mayank Agarwal, Santosh Biswas, Sukumar Nandi*. Detection of De-authentication Denial of Service attack in 802.11 networks // 2013 Annual IEEE India Conference (INDICON). DOI: 10.1109/INDCON.2013.6726015.

12. *Anjum F., Das S., Gopalakrishnan P., Kant L., Kim B.* Security in an insecure WLAN network // WCNM, 2005, pp. 292-297.

13. *Mikhaylov V.Y., Mazepa R.B.* USRP Devices Application for Modeling Signal-Like Interference in Wireless Networks // Journal "Systems of Signal Synchronization, Generating and Processing". 2020. Vol.11. no.3, pp. 43-51.

14. *Mikhaylov V.Y., Mazepa* R.B. USRP Devices Application for Modeling Signal-Like Interference in Wireless Networks // 2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2020, Svetlogorsk, 01-03 July 2020. Svetlogorsk, 2020. P. 9166121.

15. *Mikhaylov V.Y., Mazepa R.B.* Modeling and the effectiveness evaluati n of signal-like interference exploiting the vulnerabilities of the RTS/CTS mechanism in 802.11 networks // 2022 Systems of Signal Synchronization Generating and Processing in Telecommunications SYNCHROINFO-2022, June 29-July 01, 2022. Arkhangelsk, Russia, 2021.

16. *Khasanova, A.M*. Detection of Attacks on Wi-Fi Access Points // Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021, Moscow, 26-28 January 2021. Moscow, 2021, pp. 28-31. DOI: 10.1109/ElConRus51938.2021.9396420. EDN FJJLQK.

17. *Yin Y., Gao Y., Manzoor S., Hei X*. Optimal RTS Threshold for IEEE 802.11 WLANs: Basic or RTS/CTS? // 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2019, pp. 1620-1625. DOI: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00289.

18. *Pant P.K*. The Impact of SGI and RTS/CTS in WLAN Throughput // 2020 nternational Conference on Intelligent Engineering and Management (ICIEM), 2020, pp. 207-211. DOI: 10.1109/ICIEM48762.2020.9160158.

DEVELOPMENT OF MODELS OF SECRETLY INFLUENCE ON THE WIRELESS NETWORKS INFRASTRUCTURE USING SIGNAL-LIKE INTERFERENCE AND EVALUATION OF THEIR RESISTANCE TO DETECTION

VLADIMIR Y. MIKHAYLOV
Moscow, Russia

ARTEM A. ABRAMOV
Moscow, Russia

ROMAN B. MAZEPA
Moscow, Russia

NIKITA A. YAKUSH
Moscow, Russia

KEYWORDS: *IEEE 802.11, USRP, LabVIEW, signal-like interference, EAPOL, DoS-impact, IDS/IPS-systems.*

ABSTRACT

Introduction: The article discusses scenarios in which, according to the 802.11 standard, deauthentication frames should be sent from a user or access point. The developed hardware and software complex records such interaction and then broadcasts it as interference. The object of research is IEEE 802.11 wireless networks, the development of models for the covert effect of signal-like interference using USRP on the physical data transmission medium.The subject of the study is the development of signs of detection of DoS effects by these models of signal-like interference.**The hardware basis** is the equipment of National Instruments USRP NI 2901, and the software basis is NI LabVIEW 2018, with which the configuration and management of USRP equipment takes place. **The results** of the study can be applied when setting up automatic network administration systems (IDS/IPS systems), which will allow timely detection of the impact, increasing the security of wireless communication networks.

REFERENCES

1. Uygar Dincalp, Mehmet Serdar Guzel, Omer Sevine, Erkan Bostanci, Iman Askerzade (2018). Anomaly Based Distributed Denial of Service Attack Detection and Prevention with Machine Learning. *2018 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, Ankara, Turkey. DOI: 10.1109/ISMSIT.2018.8567252.

2. A. Abdelrahman, H. Khaled, Eman Shaaban, Wail S. Elkilani. WPA-WPA2 PSK Cracking Implementation on Parallel Platforms (2018). *2018 13th International Conference on Computer Engineering and Systems (ICCES)*, Cairo, Egypt. DOI: 10.1109/ICCES.2018.8639328.

3. David Janos Feher; Barnabas Sandor (2018). Effects of the WPA2 KRACK Attack in Real Environment. *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, Subotica, Serbia. DOI: 10.1109/SISY.2018.8524769.

4. Neil Dalal, Nadeem Akhtar, Anubhav Gupta, Nikhil Karamchandani, Gaurav S. Kasbekar, Jatin Parekh (2022). A Wireless Intrusion Detection System for 802.11 WPA3 Networks. *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, Bangalore, India, January, 2022. DOI: 10.1109/COMSNETS53615.2022.9668542

5. R. Korolkov, S. Kutsak, V. Voskoboinyk (2021). Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection.

6. Jaspreet Kaur (2017). Mac Layer Management Frame Denial of Service Attacks. *2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*.

7. Pratik Satam, Salim Hariri (2021). WIDS: An Anomaly Based Intrusion Detection System for Wi-Fi (IEEE 802.11) Protocol. *IEEE Transactions on Network and Service Management*. Vol.: 18, Issue: 1, March 2021.

8. Rajinder Singh1 and Satish Kumar (2019). A light weight solution for detecting de-authentication attack. *International Journal of Network Security & Its Applications (IJNSA)*, Vol. 11, No.1.

9. Z. Afzal, J. o B. Talha and M. Chowdhury (2016). A Wireless Intrusion Detection System for 802.11 networks. *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, pp. 828-834.

10. M. Eian (2009). Fragility of the robust security network: 802.11 denial of service. *International Conference on Applied Cryptography and Network Security, LNSC*. Vol. 5536, pp. 400-416.

11. Mayank Agarwal; Santosh Biswas; Sukumar Nandi (2013). Detection of De-authentication Denial of Service attack in 802.11 networks. *2013 Annual IEEE India Conference (INDICON)*. DOI: 10.1109/INDCON.2013.6726015.

12. F. Anjum, S. Das, P. Gopalakrishnan, L. Kant, and B. Kim (2005). Security in an insecure WLAN network. *WCNM*, pp. 292-297.

13. V.Y. Mikhaylov, R.B. Mazepa (2020). USRP Devices Application for Modeling Signal-Like Interference in Wireless Networks. *Systems of Signal Synchronization, Generating and Processing*. Vol.11. no.3, pp. 43-51.

14. V.Y. Mikhaylov, R.B. Mazepa (2020). USRP Devices Application for Modeling Signal-Like Interference in Wireless Networks. *2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2020*, Svetlogorsk, 01-03 July 2020, pp. 9166121.

15. V.Y. Mikhaylov, R.B. Mazepa (2022). Modeling and the effectiveness evaluation of signal-like interference exploiting the vulnerabilities of the RTS/CTS mechanism in 802.11 networks.*2022 Systems of Signal Synchronization Generating and Processing in Telecommunications SYNCHROINFO-2022*, June 29-July 01, 2022. Arkhangelsk, Russia.

16. A.M. Khasanova (2021). Detection of Attacks on Wi-Fi Access Points. *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021*, Moscow, 26-28 January 2021, pp. 28-31. DOI: 10.1109/ElConRus51938.2021.9396420.

17. Y. Yin, Y. Gao, S. Manzoor and X. Hei (2019). Optimal RTS Threshold for IEEE 802.11 WLANs: Basic or RTS/CTS? *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 1620-1625. DOI: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00289.

18. P.K. Pant (2020). The Impact of SGI and RTS/CTS in WLAN Throughput. *2020 International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 207-211. DOI: 10.1109/ICIEM48762.2020.9160158.

For citation: Mikhaylov V.Y., Abramov A.A., Mazepa R.B., Yakush N.A. Development of models of secretly influence on the wireless networks infrastructure using signal-like interference and evaluation of their resistance to detection. H&ES Reserch. 2023. Vol. 15. No 3. P. 38-46. doi: 10.36724/2409-5419-2023-15-3-38-46 (In Rus)

doi: 10.36724/2409-5419-2023-15-3-47-56

АНАЛИЗ И ОПТИМИЗАЦИЯ СХЕМ КОДИРОВАНИЯ ДЛЯ КАНАЛОВ С РЭЛЕЕВСКИМИ ЗАМИРАНИЯМИ

ОВЧИННИКОВ
Андрей Анатольевич [1]

ФОМИНЫХ
Анна Александровна [2]

АННОТАЦИЯ

Введение: традиционным подходом к декодированию в каналах с памятью является применение перемежителя, который увеличивает как сложность обработки, так и задержку на стороне приемника. Для того, чтобы избежать этих недостатков, могут использоваться подходы адаптации схемы помехоустойчивого кодирования для каналов с памятью. Одним из подходов является использование помехоустойчивых кодов, с модифицированными конструкцией и процедурой декодирования с учётом наличия в канале пакетов ошибок. Другим подходом к адаптации схемы кодирования для исправления с пакетов ошибок является использование кодов-произведений с итеративными алгоритмами декодирования. Компонентные коды кодов-произведений сами по себе могут быть не способны исправлять пакеты ошибок, но двумерная структура кодов-произведений, работающая как искусственный перемежитель, и итеративное декодирование позволяют исправлять группирующиеся ошибки. **Цель исследования:** целью исследования является анализ методов адаптации некоторых помехоустойчивых кодовых конструкций для исправления пакетов ошибок в каналах с памятью с целью понижения вероятности ошибки. **Результаты:** рассмотрены методы адаптации кодов с малой плотностью проверок на четность, полярных кодов, а также кодов-произведений для исправления пакетов ошибок в канале Гилберта-Эллиотта (ГЭ) и коррелированном Рэлеевском канале с разными коэффициентами корреляции. Оптимизированы весовые распределения кода с малой плотностью проверок на четность для канала ГЭ. Проанализировано влияние выбранных параметров компонентных кодов кодов-произведений на исправление пакетов ошибок в канале ГЭ. Оптимизирована структура полярного кода с помощью генетического алгоритма для коррелированного Рэлеевского канала, выигрывающая по вероятности ошибки конструкцию из стандарта 5G. **Обсуждение:** текущие кодовые конструкции не обеспечивают теоретически возможных пределов, поэтому остается открытым вопрос разработки схем помехоустойчивого кодирования и декодирования, способных достигать теоретических границ.

Сведения об авторах:

[1] кандидат технических наук, доцент, доцент кафедры инфокоммуникационных технологий и систем связи Санкт-Петербургского государственного университета аэрокосмического приборостроения, Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия, mldoc@mail.ru

[2] ассистент кафедры инфокоммуникационных технологий и систем связи Санкт-Петербургского государственного университета аэрокосмического приборостроения, Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия, aawat@ya.ru

КЛЮЧЕВЫЕ СЛОВА: *каналы с памятью; коды с малой плотностью проверок на четность; коды-произведения; итеративное декодирование, полярные коды.*

Для цитирования: Овчинников А.А., Фоминых А.А. Анализ и оптимизация схем кодирования для каналов с рэлеевскими замираниями // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 3. С. 47-56. doi: 10.36724/2409-5419-2023-15-3-47-56

Введение

Одним из наиболее ценных ресурсов в развивающемся мире является информация, которая может искажаться во время обработки, передачи и хранения, что приводит к возникновению ошибок. Реальные модели каналов связи описываются математическими моделями, в которых появляющиеся ошибки являются зависимыми, что приводит к образованию пакетов ошибок. Данный эффект принято называть наличием памяти в канале. В случае, когда памяти в канале нет, канал называется каналом без памяти, и ошибки в канале являются независимы. Эффект памяти в канале обуславливается физическими характеристиками, такими как многолучевое распространение, рассеивание, свойства оборудования системы хранения и др. [1]. Известно, что учёт памяти канала при декодировании теоретически позволяет увеличить достижимые скорости надёжной передачи. Это замечание мотивирует поиск эффективных методов помехоустойчивого кодирования для каналов с зависимыми ошибками. Среди математических моделей, описывающих каналы с памятью, можно выделить канал Гилберта [2], канал Гилберта-Эллиотта [3], коррелированный Рэлеевский канал [4].

Чтобы преодолеть влияние канала, теория кодирования предлагает использовать помехоустойчивые коды, которые добавляют избыточность в данные во время кодирования и используют её для исправления поврежденных данных во время декодирования [5]. Искусственная декорреляция канала связи является традиционным способом обработки пакетов ошибок, но она снижает эффективность вносимой кодом избыточности, увеличивает сложность и задержку в обработке. Для преодоления упомянутых недостатков, связанных с использование перемежителя, может быть применено несколько подходов к адаптации схемы кодирования.

Один из подходов заключается в том, чтобы модифицировать структуру кода и декодера, принимая во внимание модель канала и наличие пакетов ошибок. Например, в [6] был представлен набор весовых распределений для кодов с малой плотностью проверок на четность, оптимизированных для канала Гилберта-Эллиотта. В работе [7] авторы представили процедуру декодирования кодов с малой плотностью проверок на четность, которая добавляет новую фазу к процедуре декодирования, называемую этапом оценки состояний канала, что позволяет учитывать эффект группирования ошибок для снижения вероятности ошибок.

Модифицированный алгоритм декодирования полярного кода при передаче по обобщённому каналу Гилберта-Эллиота был предложен в работе [8]. Другим подходом к адаптации схемы кодирования для исправления пакетов ошибок является использование кодов-произведений с итеративным декодированием [9]. Хотя компонентные коды кодов-произведений могут быть неспособны исправлять пакеты ошибок, группирующиеся ошибки могут быть исправлены благодаря двумерной структуре кодов-произведений, которая выступает в качестве искусственного перемежителя, и итеративному декодированию.

В данной работе рассматривается адаптация схем помехоустойчивого кодирования и декодирования для исправления пакетов ошибок при передаче по каналам с памятью. Приводятся анализ и результаты сравнения по вероятности ошибки следующих кодовых конструкций: коды с малой плотностью проверок на четность, коды-произведения и полярные коды. Исследование помехоустойчивости производится в модели канала Гилберта-Эллиотта и модели коррелированного Рэлеевского канала. Оптимизируются весовые распределения кода с малой плотностью проверок на четность для канала ГЭ. Анализируется подбор параметров компонентных кодов кодов-произведений для исправления пакетов ошибок. Оптимизируется структура полярного кода для коррелированного Рэлеевского канала. Приводится сравнение рассмотренных конструкций по вероятности ошибки.

Каналы с памятью

Для описания влияния шума на передаваемую информацию при построении моделей каналов связи и способов кодирования и декодирования часто используется аддитивная модель. Предположим, на вход канала подается символ x, а на выходе канала наблюдается символ y. Согласно аддитивной модели, передача по каналу может быть выражена как $y = x + e$, где e — это символ ошибки. Данное выражение обобщается на случай векторов $\mathbf{x}$, $\mathbf{y}$ длины n как $\mathbf{y} = \mathbf{x} + \mathbf{e}$, где $\mathbf{x}$ – это передаваемый вектор, $\mathbf{y}$ – это принятый вектор, $\mathbf{e}$ – это вектор ошибки. Вектор ошибок в каналах с памятью содержит ошибки, образующие пакеты ошибок, являющиеся областями вектора ошибок, которые начинаются и заканчиваются единицей.

Предположим, что канал в процессе передачи данных может переходить из состояния в состояние. В математической модели канала такой переход характеризуется соответствующими переходными вероятностями. Данное описание позволяет определить канал как марковскую цепь. При моделировании каналов часто рассматривается скрытая модель Маркова, в которой предполагается, что параметры модели канала неизвестны на стороне приемника даже при знании вектора ошибок, производимого этой моделью. Это является одним из факторов, приводящих к тому, что изучение каналов с памятью, включая оценку пропускной способности, оказывается трудной задачей. В результате, сложность получения аналитических результатов для каналов с памятью, является одной из причин по которой разработка методов кодирования сосредоточена на каналах без памяти.

Моделирование канала с использованием цепи Маркова обычно подразумевает, что число состояний, в которых может находиться канал связи, является конечным, и в этом случае канал называется каналом с конечным числом состояний (ККЧС). Каждое состояние модели ККЧС описывается двоичным симметричным каналом с различными вероятностями ошибок. Часто предполагается, что модель ККЧС состоит только из двух состояний: «хорошего» и «плохого». В «хорошем» состоянии G вероятность ошибки, как правило, низкая, а в «плохом» состоянии B она может изменяться в зависимости от модели канала. Из этой фундаментальной модели могут быть получены многочисленные вариации, такие как модель Гилберта [2] и модель Гилберта-Эллиота (ГЭ) [3]. Модель Гилберта предполагает, что ошибок в состоянии G нет, тогда как ошибки могут присутствуют в состоянии B с

вероятностью *p*. В 1963 году Э. Эллиотт предложил обобщение модели Гилберта, в которой состояние *G* также не является безошибочным. Будучи одной из первых моделей канала памяти, модель Гилберта-Эллиота по-прежнему актуальна и часто используется для описания реальных систем. Согласно модели Гилберта-Эллиота, следующее состояние канала определяется его предыдущим состоянием. Канал состоит из двух состояний, *B* и *G*. В состоянии *G*, вероятность ошибки – P_G, и в состоянии B – P_B.

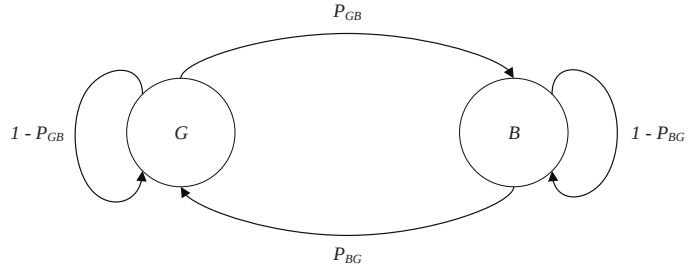

Рис. 1. Модель канала Гилберта-Эллиотта

Канал может переходить из состояния в состояние в любой момент времени. Положим, что P_{GB} – вероятность перехода из состояния *G* в состояние *B*, и P_{BG} – вероятность перехода из состояния *B* в состояние *G*. Тогда, безусловная вероятность нахождения в состояниях *B* и *G*

$$P_B = \frac{P_{GB}}{P_{GB} + P_{BG}},\ P_G = \frac{P_{BG}}{P_{GB} + P_{BG}}.$$

Канал Гилберта-Эллиотта может описывать модель канал с Рэлеевскими замираниями. Явления замирания и рассеяния традиционно описываются на примере каналов беспроводной связи с учётом особенностей распространения радиосигнала (многолучевого распространения): если передающая антенна посылает сигнал-импульс в радиоканал, то радиосигнал при взаимодействии с препятствиями отражается в виде нескольких искаженных копий, а сумма сигналов представляет собой множество откликов одного и того же передаваемого импульса. Амплитуда принятого сигнала затем может быть промоделирована с помощью распределения Рэлея, чья функция плотности вероятности равна

$$p(r) = \frac{r}{\sigma^2}\exp\left(-\frac{r^2}{2\sigma^2}\right), r \geqslant 0.$$

Случайная величина Рэлея μ может быть записана как $\mu = \sqrt{x^2 + y^2}$, где $x, y \in N(0, \sigma^2)$ независимые гауссовы случайные величины с нулевым средним и дисперсией σ^2. Замирание амплитуды сигнала может быть выражено с помощью следующей модели канала связи Рэлея: $y = \mu x + \eta$, где x – это передаваемый сигнал, μ – коэффициент затухания, которая является случайной величиной Рэлея с $E[\mu^2] = 1$, и $\eta \in N(0, \sigma^2)$ – аддитивный белый гауссовский шум.

Модель канала связи Рэлея очень проста, и является обобщением модели с аддитивным белым гауссовским шумом, путём введения, помимо аддитивной составляющей, мультипликативной составляющей шума, называемой коэффициентом усиления канала. Сегодня для моделирования систем связи используются гораздо более сложные и вычислительно трудоемкие модели, но базовой математической моделью остается модель Рэлея, с помощью которой при построении схем кодовой модуляции можно учитывать эффект замирания канала [10].

Для генерации рэлеевских случайных величин ранее предполагалось, что гауссовы компоненты (а следовательно, и результирующие рэлеевские значения) независимы; однако в реальных каналах связи они часто не являются независимыми. Этот эффект можно принять во внимание, введя корреляционный коэффициент ρ, тогда значения μ_i, полученные в *i*-й момент времени:

$$\mu_i = \sqrt{x_i^2 + y_i^2}$$

где

$$x_i = \rho x_{i-1} + \sqrt{1-\rho^2}\,\eta_x,$$
$$y_i = \rho y_{i-1} + \sqrt{1-\rho^2}\,\eta_y,$$

где $\eta_x, \eta_y \in N(0, \sigma^2)$. При $\rho = 0$ замирание независимые, в некоторых каналах параметр коэффициента корреляции может достигать 0.99-0.999 или более [11].

Коды с малой плотностью проверок на четность

Коды с малой плотностью проверок на четность (low-density parity-check, LDPC) были разработаны Робертом Г. Галлагером в 1962 году [12] и почти не использовались в течение 30 лет из-за низких вычислительных возможностей того времени. Дэвид Маккей заново открыл LDPC-коды в 1990-х годах, и по мере увеличения вычислительной мощности появился новый рост интереса к LDPC-кодам, которые обладают многими преимуществами, такими как исправление ошибок вплоть до предела Шеннона, низкая полка и эффективные методы кодирования и декодирования. Проведено много исследований об эффективности LDPC-кодов в каналах без памяти и, однако, их способность исправлять ошибки в каналах с памятью является не так хорошо разработанной областью.

Двоичный (*n*, *k*) линейный код — это *k*-мерное подпространство *n*-мерного пространства двоичных векторов. LDPC-код может быть задан проверочной матрицей **H**. Если проверочная матрица кода является разреженной, то соответствующий код называется LDPC-кодом. Разреженность LDPC-кодов позволяет реализовывать эффективные процедуры кодирования и декодирования. LDPC-код называется регулярным, если веса строк и столбцов проверочной матрицы одинаковы. Но если веса строк и столбцов различны, то LDPC-код называется нерегулярным. Как правило, построение регулярных кодов является более простой процедурой по сравнению с построением нерегулярных кодов, однако, нерегулярные конструкции чаще оказываются более эффективными для исправления ошибок. Проверочная матрица LDPC-

кода может быт представлена в виде двудольного графа (графа Таннера), который состоит из двух типов узлов, символьных, соответствующих столбцам матрицы **H**, и проверочных, соответствующих строкам матрицы **H**. Ансамбль LDPC-кодов характеризуется весовым распределением $(\boldsymbol{\lambda}, \boldsymbol{\rho})$, где $\boldsymbol{\lambda} = [\lambda_1, \lambda_2, \ldots, \lambda_J]$, в котором каждый элемент λ_i – вероятность того, что случайно выбранное ребро соединено с символьным узлом степени i. Таким же образом, $\boldsymbol{\rho} = [\rho_1, \rho_2, \ldots, \rho_K]$, где ρ_j – вероятность того, что случайно выбранное ребро соединено с проверочным узлом узлу степени j.

В распределениях J – это максимальная степень символьного узла и K – это максимальная степень проверочного узла. Весовое распределение кода определяет его предельную способность к исправлению ошибок, для анализа которой может быть применен алгоритм эволюции плотностей. Алгоритмы декодирования низкоплотностных кодов представляют собой алгоритмы передачи сообщений по ребрам графа Таннера между символьными и проверочными узлами. Широко известным алгоритмом является алгоритм распространения доверия (belief propagation, BP) [10].

Коды-произведения

Основным подходом к объединению кодов является использование итеративной структуры кода, которая была предложена П. Элиасом в 1954 году [13]. В данной схеме использует два компонентных кода, C_1 и C_2. Последовательности символов, закодированные первым кодом, подаются в качестве информационных последовательностей для кодирования вторым кода. Конкатенированная последовательность по строкам или столбцам является кодовым словом итеративного кода. В итеративной схеме может использоваться быть более двухкомпонентных кодов, но каждый дополнительный код уменьшает общую кодовую скорость. Далее рассмотрим подробнее итеративную схему с двумя компонентными кодами.

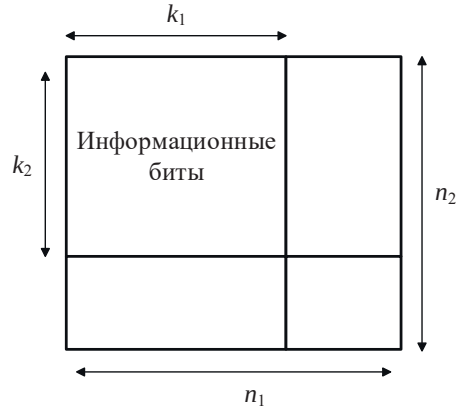

Рис. 2. Пример кода-произведения

Для построения кода-произведения требуются два компонентных кода – C_1 с параметрами (n_1, k_1), и C_2 с параметрами (n_2, k_2). Предположим, что оба компонентных кода представлены в систематической форме. Сначала, k_2 информационных блока по k_1 битов помещаются в k_2 строки массива $k_2 \times k_1$, как показано на рисунке 1.

В каждой строке вектор информационных символов длины k_1 кодируется с использованием кода C_1 в вектор кодовых символов длины n_1. Каждый столбец полученного массива является вектором информационных символов для второго кода, то есть каждый из n_1 векторов информационных символов длины k_2 кодируется с использованием кода C_2 в вектор кодовых символов длины n_2. Результирующее кодовое слово кода-произведения имеет длину $n = n_1 n_2$. Обычно в качестве компонентных кодов для кодов-произведений используются линейные блоковые коды, такие как коды Хэмминга, БЧХ коды и коды с проверкой на четность.

Алгоритмы декодирования кодов-произведений представляют собой итеративные процедуры, применяющие компонентные декодеры последовательно по столбцам, а после по строкам, или наоборот. В зависимости от выбранных компонентных декодеров, декодирование может быть жестким, оперирующим с символами кодового алфавита, или мягким, с использованием информации о надежностях символов из канала [10].

Полярные коды

Полярные коды, предложенные Эрдалом Ариканом в 2009 году, являются первыми кодами с явной конструкцией, в асимптотике достигающими пропускной способности симметричного канала, обладая при этом простыми процедурами кодирования и декодирования [14]. Новая волна интереса к полярным кодам возникла в связи с принятием полярных кодов консорциумом 3GPP (3rd Generation Partnership Project) в стандарт беспроводной связи пятого поколения для кодирования в восходящих и нисходящих каналах сервиса расширенной мобильной широкополосной связи (enhanced mobile broadband, eMBB) [15].

В основе процедуры кодирования полярными кодами лежит явление поляризации канала, суть которого состоит в том, что путем некоторых преобразований канал передачи информации может быть расщеплен на подканалы, вероятность ошибки в которых стремится к нулю, и подканалы, вероятность ошибки в которых стремится к единице. Учитывая возникающие свойства подканалов, целесообразно передавать биты данных по наиболее надежным подканалам, а по наименее надежным подканалам передавать некоторые предопределенные данные, как правило, нули.

Полярный код – это линейный код с длиной $N = 2^n$ и скоростью $R = K/N$. Полярный код строится с использованием ядра поляризации

$$\mathbf{G} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

как

$$\mathbf{x} = \mathbf{u}\mathbf{G}^{\otimes n}$$

который преобразует вектор $\mathbf{u} = [u_0, u_1, \ldots, u_{N-1}]$ в вектор $\mathbf{x} = [x_0, x_1, \ldots, x_{N-1}]$, где матрица $\mathbf{G}^{\otimes n}$ вычисляется как n-ое Кронекеровское произведение матрицы $\mathbf{G}$.

Процедура кодирования заключается в определении K надежных битовых подканалов, составляющих множество

индексов информационных символов A, и применения полярного преобразования. Оставшиеся $N - K$ подканалов образуют множество замороженных символов F. Информационные биты присваиваются на позиции из A в несущем векторе **u**, а оставшиеся позиции из F инициализируются предопределёнными значениями, обычно нулями. Кодовое слово полярного кода получатся применением полярного преобразования к вектору **u**. Позиции наиболее надежных символов могут различаться в зависимости от типа канала.

Для определения позиций наиболее надежных символов может использоваться теоретический подход с оценками вероятностей ошибок в канале, или более практический, путем использования компьютерного моделирования. Стандарт 5G предлагает последовательность 1024-битовых индексов канала, представленных в порядке возрастания надежности канала. Эта последовательность сформировалась на основе ряда исследовательских работ и может быть использована для выбора достоверности положений каналов с разными условиями и кодами длиной до 1024 бит.

По своей природе полярные коды имеют последовательные процедуры кодирования и декодирования. В оригинальной работе Э. Арикана для декодирования полярных кодов был предложен алгоритм последовательного исключения (successive cancellation, SC) [14], который в силу последовательной природы страдает от распространения ошибок. В 2015 году Э. Арикан предложил способ разрешения данного недостатка в работе [16], в которой описал модификацию алгоритма последовательного исключения – списочный алгоритм последовательного исключения (successive cancellation list, SCL). Далее было предложено конкатенировать полярный код с циклическим избыточным кодом (cyclic redundancy check, CRC), что приводит к увеличению минимального расстояния полярного кода и позволяет разрешить проблему выбора из слова списка в алгоритме SCL [17]. Одним из примеров итеративного алгоритма декодирования полярных кодов является алгоритм распространения доверия (belief propagation, BP) [18].

Адаптация кодовых схем

LDPC. Для адаптации кодовой схемы к исправлению пакетов ошибок, изменению может быть подвержена как на структура кода, так и структура декодера. В литературе было предложено несколько подходов к изменениям в структуре кода. Авторы в [19] показали, что достаточно длинные случайные структурированные коды служат как перемежители, преодолевая канальные эффекты. В работе [6] авторы представили метод оптимизации весовых распределений LDPC-кодов, основанный алгоритме на эволюции плотности для канала ГЭ. Существуют исследования, рассматривающие подходы для адаптации структуры декодера.

Один из подходов состоит в объединении графа помехоустойчивого кода и графа канала. В [7] описано двухэтапное декодирование, которое предлагает ввести дополнительный этап в процесс декодирования, а именно этап оценки состояния канала, который позволяет использовать эффект группирования ошибок для уменьшения вероятности ошибки. В [20, 21] авторы предложили алгоритмы для исправления пакетов ошибок применимые для блочно-перестановочных LDPC-кодов.

Коды-произведения. Использование кодов-произведений является традиционным подходом для борьбы с пакетами ошибок. Хотя компонентные коды могут быть не предназначены для исправления пакетов ошибок, двумерная структура и итеративное декодирование способствует исправлению пакетов ошибок.

Предположим, что кодовое слово кода-произведения получено путем конкатенирования кодовых слов столбцов. В этой конфигурации кодовые слова в столбцах в большей степени подвержены пакетам ошибок после передачи через канал. На кодовые слова в строках оказывается меньшее влияние, что наглядно демонстрирует эффект искусственной декорреляции, обусловленной структурой кода. Так как пакеты ошибок накладываются по столбцам, количество ошибок в столбцах может превышать корректирующую способность кода, но количество ошибок по строкам может быть небольшим и, таким образом, может быть исправлено.

В зависимости от параметров каналов с памятью и длины пакетов, структура кодов-произведений может быть адаптирована для уменьшения концентрации числа ошибок для кодов по строкам или столбцам путем настройки параметров компонентных кодов. Например, зафиксировав общую длину кода-произведения $N = 961$ и число информационных битов $K = 441$, можно подобрать три набора параметров БЧХ кодов C_1:(n_1, k_1), C_2:(n_2, k_2), подходящих под заданные требования, а именно – ((63, 51), (15, 7)), ((31, 21), (31, 21)) и ((15, 7), (63, 51)). Предположение состоит в том, что пакеты ошибок будут оказывать разное влияние на коды по столбцам и строкам в зависимости от выбранных параметров компонентных кодов.

Полярные коды. Оптимизация структуры полярного (N, K)-кода заключается в определении позиций и взаиморасположения замороженных и информационных битов, которые позволяют достигать наименьшей вероятности ошибки P_e

$$\mathcal{A} = \arg\min_{\mathcal{A},|\mathcal{A}|=K} P_e(\mathcal{A}).$$

При моделировании системы передачи с использованием канального кодирования в качестве вероятности ошибки чаще всего рассматривают вероятность ошибки на информационный бит (bit error rate, BER) или вероятность ошибки на информационное слово (block error rate, BLER).

$$\mathcal{A} = \arg\min_{\mathcal{A},|\mathcal{A}|=K} \mathrm{BER}(\mathcal{A}) \text{ или } \mathrm{BLER}(\mathcal{A}).$$

Для построения полярных кодов (определения информационных позиций) в литературе предлагается ряд подходов, которые можно подразделить на три вида: интенсивное компьютерное моделирование, использование алгоритмических подходов или использование алгоритмов искусственного интеллекта. Среди алгоритмических подходов в качестве примеров можно привести алгоритм эволюции плотности (density evolution, DE), алгоритм Гауссовской аппроксимации (Gaussian approximation, GA), процедуру, основанную на оптимизации параметра Бхаттачария [22].

Генетические алгоритмы относятся к числу наиболее широко используемых эволюционных алгоритмов с точки зрения разнообразия применения [23]. Генетический алгоритм – это эвристический поиск, который основан на теории естественного отбора, выдвинутой Чарльзом Дарвином. Генетические алгоритмы (genetic algorithms, GA) воспроизводят естественный отбор, где наиболее приспособленные особи отбираются для размножения, чтобы произвести потомство следующего поколения.

Основными шагами генетического алгоритма являются инициализация популяции, расчет фитнес-функции, родительский отбор, перекрестная операция, мутация и отбор выживших. Оптимизация построения полярного кода с использованием генетического алгоритма для канала с АБГШ рассмотрена в [24]. В следующем разделе представлена конструкция, оптимизированная для коррелированного Рэлеевского канала.

Результаты моделирования

В данном разделе приводятся результаты применения процедур адаптации к кодовым схемам и их влияние на способность к исправлению пакетов ошибок. Рассматривается три сценария

- Оптимизация весовых распределений LDPC-кодов для канала ГЭ и сравнение оптимизированного кода по вероятности ошибки, с кодом, построенным по распределению, оптимизированному для двоично-симметричного канала.
- Исследование влияния параметров компонентных кодов на пакетную корректирующую способность в канале ГЭ.
- Оптимизация структуры полярного кода для коррелированного Рэлеевского канала с различными коэффициентами корреляции. Сравнение оптимизированной конструкции по вероятности ошибки с конструкцией полярного кода из стандарта 5G.

Для первого и второго сценариев моделирование передачи выполняется по каналу ГЭ с параметрами (P_{GB}, P_{BG}, P_G, P_B). На рисунках с моделированием по оси x указана битовая вероятность ошибки в канале (channel bit error probability, CBEP), которая вычисляется как CBEP = $(P_{GB}P_B + P_{BG}P_G)/(P_{GB} + P_{BG})$. Способность к исправлению ошибок оценивается с помощью ошибки на информационное слово (frame error rate, FER).

В первом сценарии мы представляем сравнение LDPC-кода, построенного по оптимизированным весовым распределениям, с кодом, построенным по весовым распределениями, оптимизированными для двоично-симметричного канала. Также приводятся результаты влияние дополнительного шага оценки состояний канала перед алгоритмом распространения доверия (Gilbert-Elliott Belief Propagation, GE-BP) [7]. Построение LDPC-кодов на основе весовых распределений выполняется с использованием алгоритма наращивания ребер [25]. Алгоритм BP и GE-BP алгоритм используют 30 итераций. Логарифмические отношения правдоподобия для BP и GE- BP алгоритмов вычисляются из принятых символов канала y_i как $L_i = (1 - 2y_i)\log(1 - p)/p$, где p это эквивалентная вероятность ошибки на бит, вычисляемая как CBEP.

На рисунке 3, результаты моделирования представлены для канала ГЭ с параметрами $P_{GB} = 0.01$, $P_G = 0.01$, $P_B = 0.5$, и изменяющейся вероятностью P_{BG}. Рассматривается код длины $N = 961$ и числом информационных символов $K = 441$. Можно заметить, что вероятность ошибки декодирования кода, основанного на оптимизированном (обозначенном звездочкой) весовом распределении, ниже по сравнению с декодированием кода, построенного по весовым распределениям для двоично-симметричного канала. Таким образом, можно заключить, что оптимизированная конструкция кода обеспечивает более эффективное исправление пакетов ошибок в канале ГЭ.

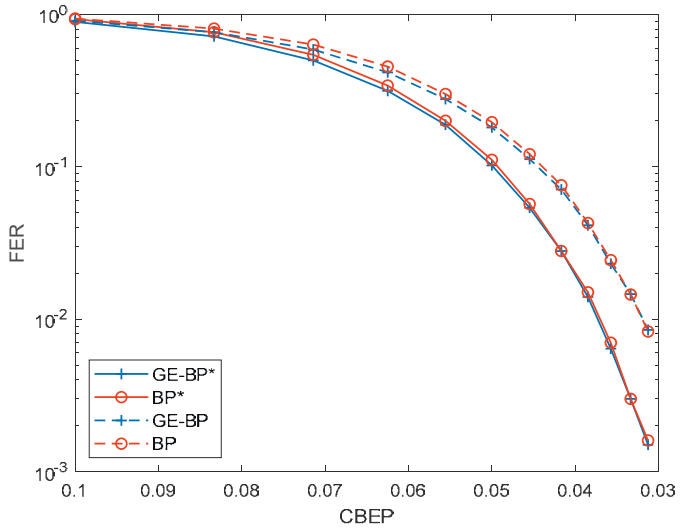

Рис. 3. Сравнение конструкций LDPC-кодов ($P_{GB} = 0.01$)

На рисунке 4, результаты моделирования представлены для канала ГЭ с параметрами $P_{GB} = 0.001$, $P_G = 0.01$, $P_B = 0.5$, и изменяющейся вероятностью P_{BG}. Можно видеть, что в условиях канала с более редкими пакетами код с оптимизированным распределением все еще дает показывает низкую вероятность ошибки. Из рисунков 3 и 4 можно видеть, что декодирование BP с дополнительным этапом оценки состояний канала, позволяет уменьшить вероятность ошибки в случае более частых пакетов.

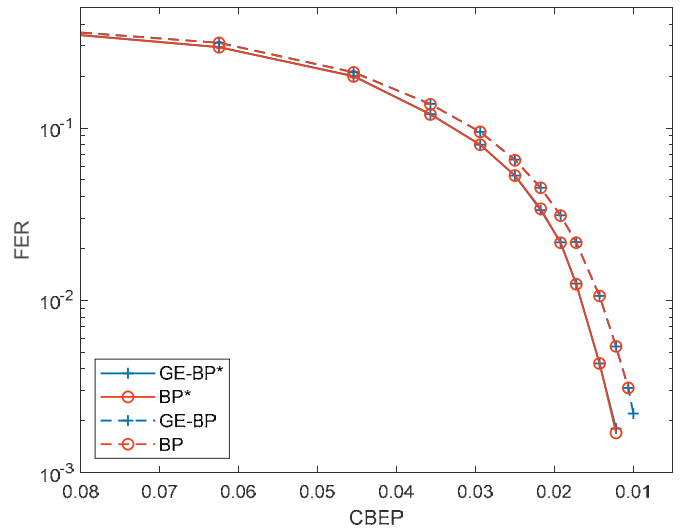

Рис. 4. Сравнение конструкций LDPC-кодов ($P_{GB} = 0.001$)

Второй сценарий исследует вероятность ошибки (n, k) LDPC-кода и кода-произведения с использованием двухкомпонентных БЧХ-кодов с параметрами (n_1, k_1) и (n_2, k_2) при передаче по каналу ГЭ. На рисунке 5, коды-произведения с компонентными БЧХ кодами с различными параметрами сравниваются в канале ГЭ с параметрами P_{GB} = 0.01, P_G = 0.01, P_B = 0.5, и изменяющейся вероятностью P_{BG}. Рассматриваются следующие пары параметров компонентных кодов (n_1, k_1), (n_2, k_2): первая пара – (63, 51), (15, 7), вторая пара – (31, 21), (31, 21), и третья пара – (15, 7), (63, 51). Декодирование осуществляется алгоритмом Берлекампа-Месси (Berlekamp-Massey, BM).

Результаты моделирования показывают, что код с большим числом строк достигает более низкой вероятности ошибки. Это происходит из следующего наблюдения: предположим, что финальное кодовое слово, передаваемое в канал, состоит из конкатенации векторов столбцов кода-произведения в один вектор. После того, как канал воздействует на передаваемый вектор, можно заметить, что пакеты влияют на передаваемый вектор по столбцам, и чем больше длина кода, тем меньше столбцов будет воздействовать на пакеты. Хотя некоторые кодовые слова столбцов будут почти повреждены, на код строки ошибки окажут меньшее влияние, что приведет к более эффективному исправлению ошибок.

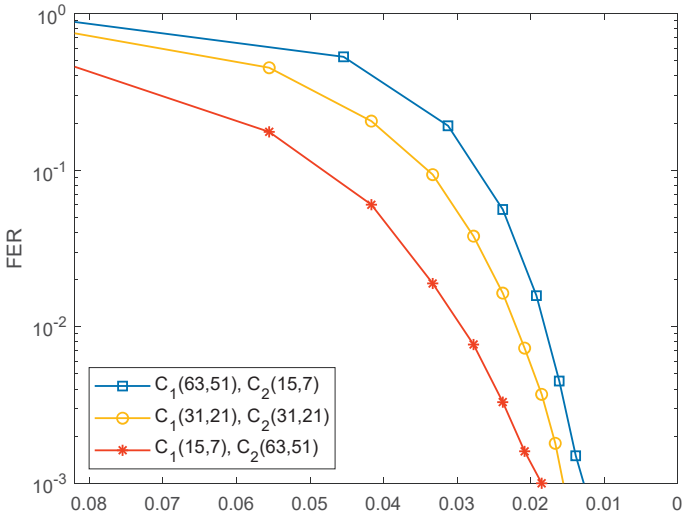

Рис. 5. Сравнение конструкций компонентных кодов (P_{GB} = 0.01)

На рисунке 6 представлено сравнение по вероятности ошибки для оптимизированного (961, 441) LDPC-кода и кода-произведения с двумя БЧХ компонентными кодами с параметрами (15, 7) и (63, 51) в канале ГЭ с параметрами P_{GB} = 0.01, P_G = 0.01, P_B = 0.5. LDPC-код показывает меньшую вероятность ошибки на больших значениях СВЕР и более высокую вероятность ошибки на меньших значениях СВЕР.

На рисунке 7 представлены результаты сравнение по вероятности ошибки полярного кода, оптимизировано с использованием генетического алгоритма (GA), и полярного кода с конструкцией из стандарта 5G для коррелированного Рэлеевского канала с различными коэффициентами корреляции. Параметры полярного кода – N = 1024, K = 512.

В генетическом алгоритме используется турнирный отбор и равномерный кроссовер, размер популяции равен 20 [23].

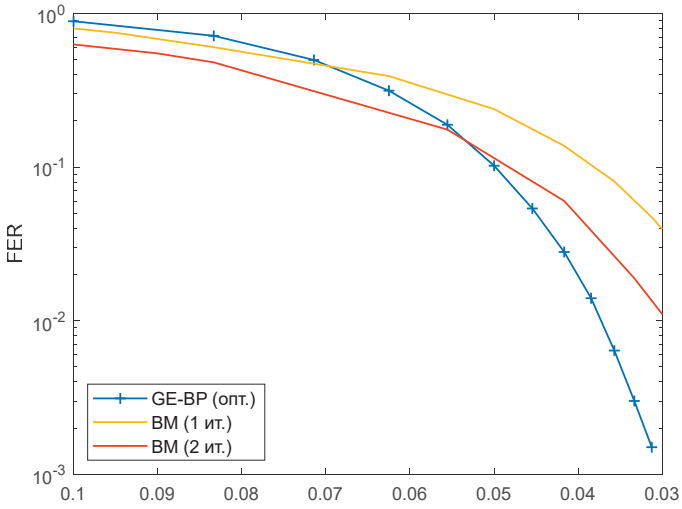

Рис. 6. Сравнение LDPC-кода и кода-произведения (P_{GB} = 0.01)

Исходная популяция получена из последовательности 5G и ее случайных модификаций. Оптимизация конструкции выполнялась для алгоритма SC и различных коэффициентов корреляции канала. Можно заметить, что для каждого коэффициента корреляции оптимизированный полярный код достигает более низкой вероятность ошибки с наибольшим выигрышем в 0,3 дБ при ρ = 0.999.

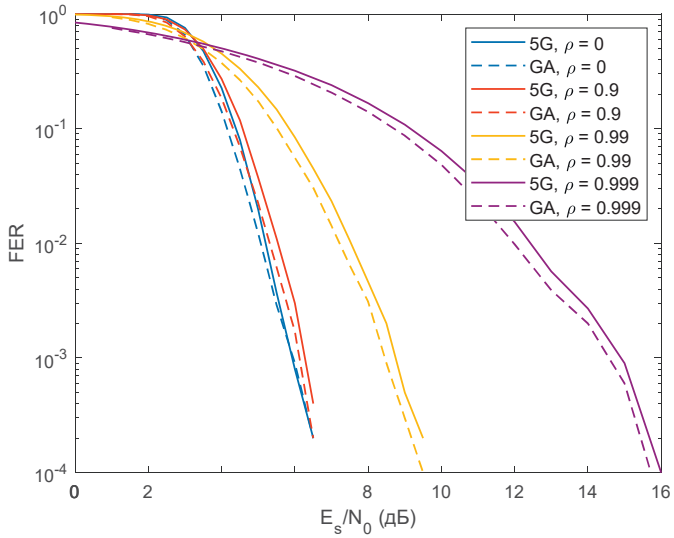

Рис. 7. Сравнение конструкций полярных кодов при декодировании алгоритмом последовательного исключения

Заключение

В данной статье приводится исследование адаптации кодовых схем для каналов с памятью. Рассмотрены методы оптимизации LDPC-кодов со стороны кодера и декодера, позволяющие уменьшить вероятность ошибки в канале ГЭ и достигать выигрыша в 0.5 СВЕР на вероятности ошибки 10^{-2}.

Исследовано влияние параметров компонентных кодов кодов-произведений на пакетную корректирующую способность. Показано, что адаптированные под параметры канала и длину пакетов компонентные коды позволяют достигать выигрыша в 0,15 СВЕР на вероятности ошибки 10^{-2}. Показано, что адаптированные коды-произведения по сравнению с a LDPC-кодами показывают меньшую вероятность ошибки на больших значениях СВЕР, и большую на меньших значениях СВЕР.

Приведены результаты моделирования оптимизированного полярного кода канале с памятью, описываемого моделью коррелированного Рэлеевского канала с различными коэффициентами корреляции. Замечено, что оптимизированная конструкция полярного кода с использованием генетического алгоритма лучше справляется с исправлением пакетов ошибок по сравнению с конструкцией полярного кода из стандарта 5G с наибольшим выигрышем в 0.3 дБ при $\rho = 0.999$.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2023-0003, "Фундаментальные основы построения помехозащищенных систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга".

Литература

1. *Burr A.* Modulation and coding: for wireless communications. NJ: Prentice Hall, 2001. 360 p.

2. *Gilbert E.N.* Capacity of a burst-noise channel // The Bell System Technical Journal. 1960. Vol. 39. No. 5, pp. 1253-1265.

3. *Elliott E.O.* Estimates of error rates for codes on burst-noise channels // The Bell System Technical Journal. 1963. Vol. 42. No. 5, pp. 1977-1997.

4. *Kennedy R.S.* Fading dispersive communication channels. NY: Wiley-Interscience, 1969. 282 p.

5. *Lin S., Li J.* Fundamentals of Classical and Modern Error-Correcting Codes. Cambridge, MA: Cambridge University Press, 2022, 840 p.

6. *Eckford A.W., Kschischang F.R., Pasupathy S.* Analysis of low-density parity-check codes for the Gilbert-Elliott channel // IEEE Transactions on Information Theory. 2005. Vol. 51, pp. 3872-3889.

7. *Eckford A.W., Kschischang F.R., Pasupathy S.* On designing good LDPC codes for Markov channels // IEEE Transactions on Information Theory. 2006, Vol. 53, pp. 5-21.

8. *Fang Y., Chen J.* Decoding Polar Codes for a Generalized Gilbert-Elliott Channel with Unknown Parameter // IEEE Transactions on Communications. 2021. Vol. 69. No. 10, pp. 6455-6468.

9. *Pyndiah R.M.* Near-Optimum Decoding of Product Codes: Block Turbo Codes // IEEE Transactions on Communications. 1998. Vol. 46. No. 8, pp. 1003-1010.

10. *Richardson T., Urbanke R.* Modern coding theory. Cambridge, MA: Cambridge university press, 2008. 590 p.

11. *Berber S.* Discrete Communication Systems. Oxford, MA: Oxford University Press, 2021. 912 p.

12. *Gallager R.G.* Low Density Parity Check Codes. Cambridge, MA: MIT Press, 1963. 90 p.

13. *Elias* P. Error-free coding // IRE Transactions on Information Theory. 1954. Vol. 4, pp. 29-37.

14. *Arıkan E.* Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels // IEEE Trans. Inf. Theory. 2009. Vol. 55. No. 7, pp. 3051-3073.

15. Chairman's Notes of Agenda Item 7.1.5 Channel Coding and Modulation, document R1-1613710, 3GPP, Nov. 2016. [Online]. URL: http://www.3gpp.org/ftp/TSG_RAN/WG1_RL1/TSGR1_87/Docs/R1-1613710.zip

16. *Tal I., Vardy A.* List decoding of polar codes. IEEE Transactions on Information Theory. 2015. Vol. 61. No. 5, pp. 2213-2226.

17. *Niu K, Chen K.* CRC-aided decoding of polar codes. IEEE Communications Letters. 2012. Vol. 16. No. 10, pp. 1668-1671.

18. *Arıkan E.* Polar codes: A pipelined implementation. Proceedings of the 4th International Symposium on Broadband Communication (ISBC 2010) (Melaka, Malaysia, on July 11-14, 2010). Malaysia, 2010, pp. 1-3.

19. *Hou J., Siegel P.H., Milstein L.B.* Performance analysis and code optimization of low-density parity-check codes on Rayleigh fading channels // IEEE Journal on Selected Areas in Communications. 2001. Vol. 19, No. 5, pp. 924-934.

20. *Ovchinnikov A., Fominykh A.* About Burst Decoding for Block-Permutation LDPC Codes. Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y. (eds) Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN ruSMART 2020 // Lecture Notes in Computer Science. 2020. Vol. 12525, pp. 393-401.

21. *Veresova A.M., Ovchinnikov A.A.* About one algorithm for correcting bursts using block-permutation LDPC-codes. 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) (Saint Petersburg, on June 03-07, 2019), Saint Petersburg, 2019, pp. 1-4.

22. *Vangala H., Viterbo E., Hong Y.* A comparative study of polar code constructions for the AWGN channel //arXiv preprint arXiv:1501.02473. 2015, pp.1-9.

23. *Abdelkhalik O.* Algorithms for Variable-Size Optimization: Applications in Space Systems and Renewable Energy (1st ed.). Boca Raton: CRC Press, 2021, 230 p.

24. *Elkelesh A., Ebada M., Cammerer S., ten Brink S.* Decoder-tailored polar code design using the genetic algorithm. IEEE Transactions on Communications. 2019. Vol. 67. No. 7, pp. 4521-4534.

25. *MacKay D.J.C.* Good error-correcting codes based on very sparse matrices // IEEE Transactions on Information Theory, 1999. Vol. 45. No. 2, pp. 399-431.

ANALYSIS AND OPTIMIZATION OF ERROR-CORRECTING CODING SCHEMES FOR CHANNELS WITH RAYLEIGH FADING

ANDREI A. OVCHINNIKOV
St-Petersburg, Russia

ANNA A. FOMINYKH
St-Petersburg, Russia

KEYWORDS: *channels with memory, low-density parity-check codes, product codes, iterative decoding, polar codes.*

ABSTRACT

Intoduction: Conventional approach to perform error-correcting decoding in channels with memory is an adoption of interleaving, which increases the receiver complexity and delay. In order to avoid these limitations, approaches for adapting an error-correcting scheme for memory channels may be used. One approach is to use error-correcting codes with modified design and decoding procedure, taking into account the presence of error bursts in the channel. Another approach to adapting the coding scheme for burst error correction is to use product codes with iterative decoding algorithms. Component codes of product codes themselves may not be able to correct error bursts, but a two-dimensional structure of product codes operating as an artificial interleaver and iterative decoding allow for correction of grouping errors. **Purpose:** The purpose of the study is to analyze the methods of error-correcting code adaptation to burst error correction in channels with memory in order to reduce the probability of error. **Results:** The study considered methods of error-correcting code scheme adaptation for low-density parity-check codes, polar codes, and product codes for burst error correction in Gilbert-Elliott channel (GE) and correlated Rayleigh fading channel with different correlation coefficients. Degree distribution of low-density parity-check code was optimized for GE channel. The influence of selected parameters of product code component codes on burst error correction in the GE channel was analyzed. The structure of the polar code has been optimized using a genetic algorithm for the correlated Rayleigh channel, which outperforms the 5G polar code design in terms of error probability. **Discussion:** Existing error-correcting code schemes do not provide theoretically possible limits, so the question remains of developing coding and decoding schemes capable of reaching theoretical limits.

REFERENCES

1. A. Burr (2001). Modulation and coding: for wireless communications. NJ: Prentice Hall, 360 p.

2. E.N. Gilbert (1960). Capacity of a burst-noise channel. *The Bell System Technical Journal*. Vol. 39. No. 5, pp. 1253-1265.

3. E.O. Elliott (1963). Estimates of error rates for codes on burst-noise channels. *The Bell System Technical Journal*. Vol. 42. No. 5, pp. 1977-1997.

4. R.S. Kennedy (1969). Fading dispersive communication channels. NY: Wiley-Interscience, 282 p.

5. S. Lin, J. Li (2022). Fundamentals of Classical and Modern Error-Correcting Codes. Cambridge, MA: Cambridge University Press, 840 p.

6. A.W. Eckford, F.R. Kschischang, S. Pasupathy (2005). Analysis of low-density parity-check codes for the Gilbert-Elliott channel. *IEEE Transactions on Information Theory*. Vol. 51, pp. 3872-3889.

7. A.W. Eckford, F.R. Kschischang, S. Pasupathy (2006). On designing good LDPC codes for Markov channels. IEEE Transactions on Information Theory. Vol. 53, pp. 5-21.

8. Y.Fang, J. Chen (2021). Decoding Polar Codes for a Generalized Gilbert-Elliott Channel With Unknown Parameter. *IEEE Transactions on Communications*. Vol. 69. No. 10, pp. 6455-6468.

9. R.M. Pyndiah (1998). Near-Optimum Decoding of Product Codes: Block Turbo Codes. *IEEE Transactions on Communications.* Vol. 46. No. 8, pp. 1003-1010.

10. T. Richardson, R. Urbanke (2008). Modern coding theory. Cambridge, MA: Cambridge university press, 590 p.

11. S. Berber (2021). Discrete Communication Systems. Oxford, MA: Oxford University Press, 912 p.

12. R.G. Gallager (1963). Low Density Parity Check Codes. Cambridge, MA: MIT Press, 90 p.

13. P. Elias (1954). Error-free coding. *IRE Transactions on Information Theory*. Vol. 4, pp. 29-37.

14. E. Arikan (2009). Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inf. Theory*. Vol. 55. No. 7, pp. 3051-3073.

15. Chairman's Notes of Agenda Item 7.1.5 Channel Coding and Modulation, document R1-1613710, 3GPP, Nov. 2016. [Online]. URL: http://www.3gpp.org/ftp/TSG_RAN/WG1_RL1/TSGR1_87/Docs/R1-1613710.zip

16. I. Tal, A. Vardy (2015). List decoding of polar codes. *IEEE Transactions on Information Theory*. Vol. 61. No. 5, pp. 2213-2226.

17. K. Niu, K. Chen (2012). CRC-aided decoding of polar codes. *IEEE Communications Letters*. Vol. 16. No. 10, pp. 1668-1671.

18. E. Arikan (2010). Polar codes: A pipelined implementation. *Proceedings of the 4th International Symposium on Broadband Communication (ISBC 2010)* (Melaka, Malaysia, on July 11-14, 2010). Malaysia, pp. 1-3.

19. J. Hou, P.H. Siegel, L.B. Milstein (2021). Performance analysis and code optimization of low-density parity-check codes on Rayleigh

fading channels. *IEEE Journal on Selected Areas in Communications*. Vol. 19. No. 5, pp. 924-934.

20. A. Ovchinnikov, A. Fominykh (2020). About Burst Decoding for Block-Permutation LDPC Codes. Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y. (eds) Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN ruSMART 2020. *Lecture Notes in Computer Science*. Vol. 12525, pp. 393-401.

21. A.M. Veresova, A.A. Ovchinnikov (2019). About one algorithm for correcting bursts using block-permutation LDPC-codes. *2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, Saint Petersburg, 2019, pp. 1-4.

22. H. Vangala, E. Viterbo, Y. Hong (2015). A comparative study of polar code constructions for the AWGN channel //arXiv preprint arXiv:1501.02473, pp.1-9.

23. O. Abdelkhalik (2021). Algorithms for Variable-Size Optimization: Applications in Space Systems and Renewable Energy (1st ed.). Boca Raton: CRC Press, 230 p.

24. A. Elkelesh, M. Ebada, S. Cammerer, S. ten Brink (2019). Decoder-tailored polar code design using the genetic algorithm. *IEEE Transactions on Communications*. Vol. 67, No. 7, pp. 4521-4534.

25. D.J.C. MacKay (1999). Good error-correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory*. Vol. 45. No. 2, pp. 399-431.

INFORMATION ABOUT AUTHORS:

Andrei A. Ovchinnikov, PhD, Docent, Docent of Institute of Radio Engineering, Electronics and Communications Technologies, Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg,Russia, mldoc@vu.spb.ru

Anna A. Fominykh, Assistant of Institute of Radio Engineering, Electronics and Communications Technologies, Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia, aawat@ya.ru

For citation: Ovchinnikov A.A., Fominykh A.A. Analysis and optimization of error-correcting coding schemes for channels with Rayleigh fading. *H&ES Reserch*. 2023. Vol. 15. No 3. P. 47-56. doi: 10.36724/2409-5419-2023-15-3-47-56 (In Rus)

doi: 10.36724/2409-5419-2023-15-3-57-64

ПЕРСПЕКТИВНЫЕ ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СЕТЕВЫЕ УСЛУГИ

ПШЕНИЧНИКОВ
Анатолий Павлович [1]

КОРОТКОВА
Виктория Игоревна [2]

ПОСКОТИН
Леонид Сергеевич [3]

АННОТАЦИЯ

Введение: суть Четвертой промышленной революции заключается не только в появлении новых технологий, но и в интеграции уже существующих в единую систему, доступную для широкого использования. Технологическая революция проникает во все сферы общественной жизни, автоматизирует производственные процессы, настраивает связь между физическими и вычислительными ресурсами. Данные преобразования подкреплены такими инновациями как: киберфизические системы, искусственный интеллект, большие данные, Интернет вещей, робототехника, облачные технологии, космические технологии, виртуальная реальность и некоторые другие. Новые цифровые технологии могут оказывать на различные сферы жизни общества как позитивное, так и негативное влияние, например: безработица, неравенство, экономическое развитие, безопасность и другие. **Целью работы** является получение минимального уровня понимания цифровых прорывных технологий, раскрытие их потенциала и их связи с вызванными промышленной революцией системными изменениями. **Методы:** при рассмотрении влияния прорывных технологий на реализацию Четвертой промышленной революции следует использовать системную методологию. Рассмотрены перспективные технологии, которые существенно влияют на реализацию промышленной революции. **Результаты:** Приведены графические зависимости скорости фиксированных сетей связи при реализации концепций их развития за период 1960-2030 гг. и графические зависимости скорости сетей сотовой мобильной связи поколений 1G-6G за период 1970-2030 гг. Отмечено, что смена концепций развития фиксированных сетей связи и поколений сотовых мобильных сетей связи с 2000 года согласуются по времени в соответствие с "правилом 10 лет". Представлена эволюция технологий и услуг сетей сотовой мобильной и фиксированной связи. В Будущих сетях прогнозируются базовые и составные сетевые услуги. В работе кратко рассмотрены базовые сетевые услуги с перечнем необходимых функций для реализации коммуникаций. Аналогичным образом представлен краткий анализ составных сетевых услуг и приложений с перечислением требованием к сетям для их реализации. Для полного раскрытия потенциала инновационных технологий и услуг промышленной революции необходимы значительные преобразования в экономических, социальных, политических и духовных сферах общества.

КЛЮЧЕВЫЕ СЛОВА: *цифровые прорывные технологии, базовые и составные сетевые услуги, технологическая революция, промышленная революция, искусственный интеллект, роботы, фиксированные сети связи, сотовые мобильные сети связи.*

Сведения об авторах:

[1] к.т.н., профессор, профессор Московского технического университета связи и информатики, Москва, Россия, pshenichnikov@mtuci.ru

2 аспирант Московского технического университета связи и информатики, Москва, Россия, v.i.korotkova@yandex.ru,

[3] аспирант Московского технического университета связи и информатики, Москва, Россия, svp_vpl@yahoo.com

Для цитирования: *Пшеничников А.П., Короткова В.И., Поскотин Л.С.* Перспективные инфокоммуникационные технологии и сетевые услуги // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 3. С. 57-64. doi: 10.36724/2409-5419-2023-15-3-57-64

Введение

Начало второго десятилетия XXI века отмечено провозглашением бизнесменами, политиками и учёными в Германии Четвёртой промышленной революции (*The Fourth Industrial Revolution*) (индустрия 4.0), новой технологической революции, которая должна привнести коренные изменения в производственные процессы с помощью использования глубокой интеграции «киберфизических систем». Для гибкости производства необходима замена соединительных кабелей на беспроводную связь со сверхнизкой задержкой порядка 1 мс и сверхвысокой надёжностью, превышающей 99,9999%. Киберфизическая система (*cyber-physical system*) – концепция, предлагающая интеграцию вычислительных средств в физические объекты, включая биологические и рукотворные объекты [1].

Сущность индустрии 4.0 заключается в синтезе и взаимодействии технологий физического, инфокоммуникационного и биологического блоков. При этом цифровые технологии являются катализатором при синтезе и взаимодействии различных технологий для достижения поставленных целей и получения при этом синергетического эффекта.

Причинами промышленных революций являются не технологии, а их влияние на экономические, политические, социальные, духовные сферы (подсистемы) общества как целостной системы. Технологии создают условия для построения новых или совершенствования существующих систем. Под искусственными системами понимается совокупность взаимодействующих элементов, упорядоченная для достижения поставленных целей.

О роли цифровых технологий в реализации задач Четвёртой промышленной революции

При рассмотрении влияния инновационных технологий на реализацию систем Четвёртой промышленной революции (ЧПР) следует использовать системную методологию [2].

Четвёртая промышленная революция должна способствовать ускорению процессов развития человеческого общества. Чтобы воспользоваться её потенциалом, необходимо решение следующих задач:

– гарантировать – справедливое распределение полученного блага от прорывных технологий;

– контролировать и управлять рисками и негативными последствиями ЧПР;

– гарантировать, что ЧПР будет происходить в интересах и под контролем человека.

Большинство экспертов выделяют 12 взаимосвязанных прорывных технологий, оказывающих существенное влияние на раннем этапе реализации ЧПР (табл. 1) [3]. Все новые технологии – это продолжение Третьей (цифровой) промышленной революции, которая началась в 1950 г. с прорывов в теории информации, вычислительной технике, цифровых телекоммуникациях. Известные эксперты по новейшим технологиям считают, что наибольшие шансы стать фундаментом ЧПР будут: искусственный интеллект, распределённые реестры и перспективные вычислительные технологии.

Представленные в таблице 1 технологии не претендуют на полноту.

Таблица 1

Технологии Четвёртой промышленной революции

Блоки технологий	Технологии		Комментарии
Расширение цифровых технологий	1.	Новые вычислительные технологии	Квантовые, облачные, туманные, граничные, распределённые и встроенные вычисления. Разработка программного обеспечения. Фотоника – хранение, обработка и передача информации.
	2.	Блокчейн и технологии распределённого реестра	Блокче́йн – непрерывная последовательная цепочка блоков, содержащих информацию. Создание и обмен уникальными цифровыми, криптозащищёнными записями без централизованной доверенной стороны. Отсутствие посредников.
	3.	Интернет вещей (*IoT*)	*IoT* – базовый инфраструктурный элемент ЧПР при решении системных проблем, обеспечение кибербезопасности. «Интернет всего».
Преобразование физического мира	4.	Искусственный интеллект (ИИ) и роботы	Люди, роботы и ИИ вместе работают лучше. Цели системам и алгоритмы достижения этих целей на основе ИИ устанавливают люди. Машинное обучение. Универсальный ИИ пока не создан.
	5.	Передовые материалы	Разработка передовых материалов и нанотехнологий влияет на все аспекты ЧПР. Нанотехнологии оперируют с веществом на молекулярном или атомном уровне. Наночастица имеет размер от 1 до 100 нанометров.
	6.	Аддитивные производства и многомерная печать	«3D-печать» и «аддитивное производство» описывают процессы создания физических объектов путём послойного нанесения материала. 4D-технология – самоизменяющиеся свойства материалов.
Изменение человека	7.	Биотехнологии	Биотехнологии обещают увеличить продолжительность и качество человеческой жизни. Генная инженерия – эффективный метод улучшения сельхозкультур.
	8.	Нейротехнологии	Нейротехнологии позволяют усовершенствовать механизмы влияния на сознание и мыслительный процесс. Взаимодействие компьютера и мозга.
	9.	Виртуальная и дополненная реальность	Виртуальная реальность (ВР) – это создаваемый компьютером мир, с которым взаимодействует человек. Дополненная (ДР) и смешанная (СР) реальности позволяют дополнить реальный мир.
Интеграция окружающей среды	10.	Получение, накопление и передача энергии	Энергетика находится на пороге перехода от ископаемых видов топлива возобновляемым энергоресурсам. Новое в энергетике – от энергии приливов до термоядерного синтеза.
	11.	Геоинженерия	Геоинженерия – это вмешательство в природные системы планеты. Вмешательство в климат планеты может быть опасным.
	12.	Космические технологии	К 2030 г. ожидается всплеск развития технологий в освоении космоса. Планируется запустить около 12 тыс. коммерческих спутников для доступа в Интернет.

Преимущества и недостатки прорывных технологий связаны с такими важными вопросами, как неравенство, безработица, экономическое развитие, здоровье и безопасность.

Технологии ЧПР взаимосвязаны, так как основаны на цифровых технологиях и сетях, созданных во время Третьей (цифровой) промышленной революции.

Новейшие технологии распространяются с экспоненциальной скоростью. Благодаря цифровой совместимости, проникают в материальные объекты и в духовную сферу общества, комбинируются неожиданными, а иногда и вредными способами, создавая как преимущества, так и проблемы. Автоматизация влияет на уровень трудоустройства. Для решения этой проблемы необходимы инвестиции в переобучение взрослого населения.

В контексте ЧПР направление развития фиксированных сетей связи определено в концепциях МСЭ-Т «Будущие сети» [4-5] и «Сеть 2030» [6-11] (рис.1), а сотовых мобильных сетей связи – в поколениях 5G [12-13] и 6G [14-17] (рис. 2). Как видно из рисунков 1 и 2, МСЭ-Т согласовал по времени смену концепций развития фиксированных сетей связи со сменой поколений сетей сотовой мобильной связи («правило 10 лет»).

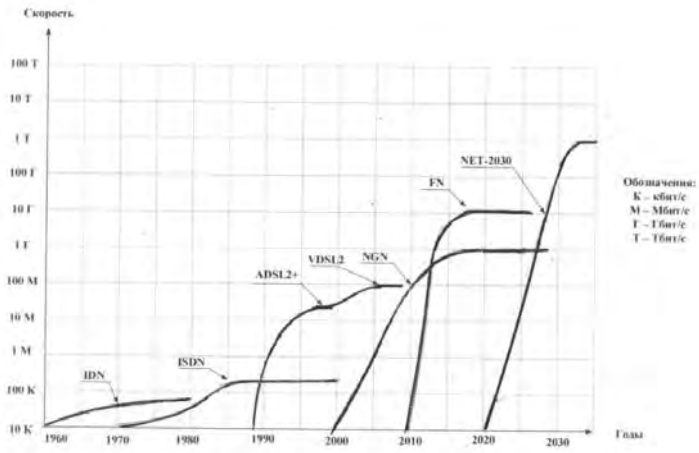

Рис. 1. Эволюция пиковой скорости фиксированных

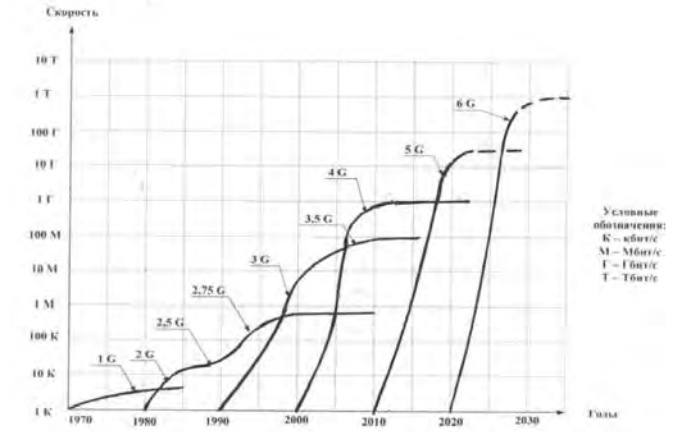

Рис. 2. Эволюция пиковой скорости сетей сотовой сетей связи мобильной связи

Сокращения:

IDN – Integrated Digital Network – Интегральная цифровая сеть;

ISDN – Integrated Services Digital Network – Цифровая сеть с интеграцией служб;

ADSL2+ – READSL2+ - Reach Extended ADSL2+ – «дальнобойный» *ADSL*;

VDSL2- Very-high data rate Digital Subscriber Line 2 – сверхвысокоскоростная цифровая абонентская линия 2;

NGN – Next Generation Networks – Сети следующего поколения;

FN – Future Networks – Будущие сети*;*

NET– 2030 – Network 2030 – Сеть 2030.

Для сопоставления названий поколений сотовой мобильной связи и концепций развития фиксированной связи *ETSI* (*European Telecommunications Standards Institute* – Европейский институт по стандартизации в области телекоммуникаций) и компания *Huawei* предложили концепции развития фиксированных сетей связи называть по аналогии с поколениями сетей сотовой мобильной связи следующим образом: концепцию *ISDN – FNG1 (FN – Fixed Network* – фиксированная сеть); *ADSL2+ – FNG2; VDSL2 – FNG3; NGN – FN4G; FN – FN5G; NET*-2030 –FNG6.

Эволюция технологий и услуг сетей сотовой мобильной связи и фиксированной связи приведена в таблице 2.

Развитие сетей идёт в направлении удовлетворения потребностей пользователей в инфокоммуникационных услугах и приложениях. Различные аспекты услуг цифровых сетей связи, реализованных по технологии коммутации пакетов, детально рассмотрены МСЭ-Т в концепции «Сети связи следующего поколения» (*NGN*) [18].

Особенности предоставления инфокоммуникационных услуг с использованием технологии сетевой виртуализации рассмотрены в концепции «Будущие сети». Преобразование физических ресурсов в виртуальные ресурсы выполняется с помощью технологий *SDN* (*Software-Defined Networking* – программно-конфигурируемая сеть)

и *NFV (Network Functions Virtualization* – виртуализация сетевых функций). Взаимодействие *SDN* и *NFV* позволяет создавать виртуальную транспортную сеть, с помощью которой производится управление пересылкой пакетов и предоставление услуг.

По прогнозам Целевой группы МСЭ-Т FG NET-2030г.

будущие сети должны обеспечивать три основных вида коммуникаций [19]:

- голографические /телепорт (holographic/teleport);
- высокоточные (high-precision communications);
- высококачественные (qualitative communications).

В будущих сетях прогнозируются базовые (foundational) и составные (compound или composite) сетевые услуги. Базовые требуют поддержки на узлах сети. Составные услуги могут состоять из нескольких базовых услуг и не требуют поддержки на транзитных узлах. Примерами составных услуг являются коммуникации голографического типа и Тактильный Интернет [20].

Таблица 2

Параметры сетей сотовой мобильной и фиксированной связи

Сотовые сети	**1*G***	**2*G***	**3*G***	**4*G***	**5*G***	**6*G***
«Правило 10 лет»	1970 ~1980	1980 ~1990	1990 ~2000	2000 ~2010	2010 ~2020	2020 ~2030
Скорость, задержка, услуги	Аналоговая голосовая связь	14,4 кБит/с голос и данные	2 Мбит/с, 150 мс, голос, видео, данные	1 Гбит/с, 10 мс *VoLTE, eMBMS*	20 Гбит/с 1-2 мс *eMBB, URLLC, mMTC*	1 Тбит/с <100 мкс *VLV&TIC, ManyNets, BBE&HPC*
Фиксированные сети	***FN1G***	***FN2G***	***FN3G***	***FN4G***	***FN5G***	***FN6G***
Скорость	< 2 Мбит/с	2 – 30 Мбит/с	30 –100 Мбит/с	0,1 – 1 Гбит/с	1 – 10 Гбит/с	1 Тбит/с
Концепции FN	*ISDN*	*ADSL2+*	*VDSL2*	*NGN*	*Future Network*	*Network* 2030
Услуги	Голос и данные с низкой скоростью	Голос, данные, доступ в Интернет	Голос, данные, доступ в Интернет, видео	Мультимедийные услуги, видео *Ultra-HD*	Интеллектуальные услуги, *FFC, eFBB, GRE*	Голографические, высококачественные, высокоточные услуги

Сокращения:
BBE&HPC – Beyond Best Effort and High-Precision Communications – коммуникации с качеством лучше *Best Effort* и высокоточные;
eFBB – enhanced Fixed Broadband – улучшенная фиксированная широкополосная связь;
eMBB – enhanced Mobile Broadband – сверхширокополосная мобильная связь;
eMBMS – evolved Multicast/Broadcast Multimedia Services – широковещательная/многоадресная передача мультимедийного контента;
FFC– Full-Fiber Connection – всестороннее применение оптоволоконных соединений;
Future Networks – Будущие сети;
FN – Fixed Network – фиксированная сеть;
G – Generation – поколение;
GRE – Guaranteed Reliable Experience – гарантированная надёжность доставки;
ManyNets –Many Networks –множество сетей;
mMTC – Massive Machine Type Communications – массовая межмашинная связь;
Ultra-HD – Ultra-High Definition – сверхвысокая чёткость;
URLLC – Ultra-Reliable Low Latency Communication – сверхнадёжная связь с малой задержкой;
VLV&TIC – Very Large Volume & Tiny Instant Communications – очень большой объём данных и крошечные мгновенные сообщения.

Базовые сетевые услуги и приложения

В будущих сетях время является главным свойством новых приложений и сетевых услуг, таких как [9-10]:

– тактильные приложения с задержкой не более 5 мс, иначе для пользователя теряется иллюзия удалённого «прикосновения». Это важно для удалённого управления оборудованием на основе тактильной обратной связи. Под задержкой понимается время с момента начала передачи первого бита пакета и до момента приёма последнего бита пакета. Нормируются сквозные задержки *E2E (end-to-end)* между точками отправки и получения;

– автономная критически важная инфраструктура, например, удалённое управление транспортными средствами. Допустимая задержка – не более 1 – 5 мс;

– промышленная и робототехническая автоматизация. Для контроллеров требуется очень точная синхронизация. При этом задержка должна быть детерминированной.

Услуги *in-time* и *on-time*. Услуги доставки пакетов не позже заданного момента времени t_i (*in-time*). Допустимую задержку при этом нельзя превышать.

Услуги доставки в заданный интервал времени Δt (*on-time*). Как и в случае *in-time*, задержку превышать нельзя. Эти услуги особенно актуальны для движущихся автономных объектов, например, автомобили или дроны.

Услуги скоординированной доставки обеспечивают доставку взаимозависимых или связанных потоков.

При этом гарантируется сохранение зависимостей и временных ограничений, наложенных на потоки.

Примерами скоординированных коммуникаций являются:

– мультисенсорные, которые возникают при передаче сигналов от различных сенсоров по разным потокам и, возможно, по разным путям. Доставка мультисервисной

информации должна быть синхронизирована между всеми источниками при доставке пользователю;

– виртуальный оркестр и /или концерты. Исполнители виртуального оркестра находятся в разных концах мира. Дирижер на сцене жестами управляет звуком ансамбля. Эти жесты должны быть получены одновременно всеми удалёнными музыкантами и аудио/видео от музыкантов к сцене;

– многосторонние голографические коммуникации. Потоки в сети из конца в конец обладают следующими зависимостями: временная зависимость требует, чтобы потоки соответствовали гарантиям, связанным со временем; зависимость порядка – потоки доставляются в определённой последовательности; зависимость качества – все потоки соответствуют заданному *QoS*.

Услуги высококачественных коммуникаций. В цифровой сети минимальной автономной единицей доставки является пакет. Пакеты теряются в сети по трём причинам:

сброс при перегрузке; сбой или отказ оборудования или канала; повреждение пакетов.

Эти услуги предполагают возможность сети различать фрагменты содержимого пакетов. Фрагментам приписывают относительные приоритеты при передаче в сети. При перегрузке в сети фрагмент с низким приоритетом может быть исключён из полезной нагрузки пакета, а фрагмент с более высоким приоритетом сохраняется для передачи к месту назначения.

Для качественных коммуникаций необходима поддержка следующих функций:

– новый метод пакетизации, в котором полезная нагрузка конструируется в виде набора фрагментов и информации для извлечения в заголовке пакета;

– функция исходного приложения определяется и назначается исходным приложением;

– функция узла пересылки выполняет операцию редактирования пакета, при которой фрагменты с низкой значимостью удаляются из пакета при перегрузке;

– функция конечного приложения. Получатель может отправить через обратную связь информацию об уровне своего удовлетворения в отношении принятого пакета.

Составные сетевые услуги и приложения

Голографические коммуникации. Голография позволяет записывать световое поле, создаваемое оптическим излучением. Для передачи голограмм необходимо иметь очень высокую пропускную способность канала связи из-за больших объёмов данных. Потоковая передача объёмных данных и массивов изображений накладывает дополнительные требования к синхронизации.

Коммуникации голографического типа *HTC (Holographic Type Communications)* для передачи больших объёмов данных требуют пропускной способности уровня Тбит/с. Дисплею на основе дополненной/виртуальной реальности *AR/VR* (*Augmented/Virtual Reality*) требуется пропускная способность порядка Гбит/с. Дополнительно необходимо обеспечить: сверхнизкие задержки не более 5 мс; при синхронизации параллельных потоков для удалённой работы изменения задержки по каналам не должны превышать 7 мс; необходимо обеспечить безопасность и гарантию доставки пакетов; ключевыми требованиями для *HTC* является наличие граничных (периферийных) вычислений высокой вычислительной мощности; в зависимости от массива изображений может потребоваться поддержка в сети порядка 1 тысячи параллельных потоков [9].

Тактильный Интернет для удалённой работы. Тактильные взаимодействия относятся к чувству прикосновения, фиксируемому рецепторами кожи. МСЭ-Т определяет Тактильный Интернет для удалённой работы TIRO *(Tactile Internet for Remote Operations)* как сеть, сочетающую сверхнизкую задержку с чрезвычайно высокой доступностью, гарантией доставки и безопасностью [20].

Тактильные сетевые приложения обычно включают следующие каналы: канал тактильной обратной связи для передачи тактильных данных от удалённых тактильных датчиков к тактильному эффектору (например, «информационная перчатка», передающая тактильные ощущения пользователю); канал управления дистанционным исполнительным механизмом; дополнительные каналы для трансляции видео, аудио и телеметрии из удалённого места.

Основные требования к сети со стороны услуг *TIRO*:

– пропускная способность для потоков VR – до 5 Гбит/с, а для голограмм – до 1 Тбит/с;

– задержка, которая остаётся незамеченной человеческим глазом, составляет около 5 мс. При реализации сверхнизкой задержки необходимо учитывать скорость распространения сигнала в одну сторону: в медном кабеле – 300 км за одну миллисекунду, в оптическом волокне – 200 км;

– синхронизация. Человеческий мозг имеет разное время реакции на различные сенсорные сигналы: тактильные (1мс), визуальные (10 мс), звуковые (100 мс). Каналы тактильной обратной связи должны быть строго синхронизированы;

– безопасность передачи данных без возможности взлома в критических тактильных случаях, связанных с человеческой жизнью или дорогостоящим оборудованием;

– гарантия доставки данных. В критических приложениях потеря данных должна быть минимальной. Надёжные схемы передачи и повторной передачи пакетов должны работать с допустимыми задержками;

– приоритизация потоков на основе их актуальности и важности.

Интеллектуальная операционная сеть. Создание интеллектуальной (эксплуатационной) сети *ION* (*Intelligent Operation Network*) будет способствовать эффективному предоставлению интеллектуальных услуг и приложений. Использование искусственного интеллекта *AI* (*Artificial Intelligence*) и обучения на реальных сетевых операциях будет способствовать определению и прогнозированию неисправностей и отказов в сети.

Требования к сети *ION*: интеллектуальное управление сетью с обратной связью с малой задержкой; реакция на события с низкой задержкой и приоритизация данных; мгновенный сбор данных с высокой пропускной способностью для определения состояния сети; программируемость и программная обработка данных.

Конвергенция сетей и вычислений. Реальная конвергенция (сближение) сетей и вычислений *NCC* (*Network and Computing Convergence*) необходима для внедрения в будущих сетях технологий искусственного интеллекта *AL,* интеллектуальной балансировки нагрузки между узлами, управления потоками нагрузки и сетевыми ресурсами, контроля и эксплуатации сети.

При этом должна быть реализована следующая функциональность: осведомлённость о вычислениях. Будущие сети должны поддерживать контролируемое во времени распределение вычислительной мощности сети и вычислительных ресурсов; распределённое и интеллектуальное управление сетью без ручного вмешательства; возможность множественного доступа; быстрая маршрутизация и ремаршрутизация трафика.

Цифровые двойники. Цифровой двойник *DT* (*Digital Twin*) определяется как представление физического объекта в цифровом виде в реальном времени. Цифровые двойники

позволяют управлять большими, сложными, стохастическими и динамическими системами с применением технологий искусственного интеллекта, глубокого машинного обучения, облачных вычислений с их безграничными вычислительными ресурсами, Интернета вещей и других перспективных технологий.

Для реализации *DT* должны выполняться следующие требования к будущим сетям: различная пропускная способность сети по требованию; задержки на уровне миллисекунд в случае критически важных услуг; мобильность по запросу; эластичность для обеспечения гибкого планирования ресурсов; безопасность обмена информацией и конфиденциальность данных.

Интегрированная наземно-космическая сеть. Космическая сеть обеспечивает коммуникации на большие расстояния и является весьма актуальной для нашей страны с её огромной территорией. Эта сеть считается одним из важных компонентов будущей сети, в которой она будет взаимодействовать с наземной сетевой инфраструктурой и в перспективе станет интегрированной наземно-космической сетью *STIN* (*Space-Terrestrial Integrated Network*).

Космическую сеть планируется реализовать на спутниковой системе на низкой околоземной орбите *LEO* (*Low Earth Orbit*). Спутники на средней околоземной орбите *MEO* (*Medium Earth Orbit*) и геостационарной орбите *GEO* (*Geostationary Earth Orbit*) могут обеспечить большую физическую стабильность спутников, но имеют большую задержку (таблица 3).

Таблица 3

Характеристики космических систем

Расстояние	Скорость передачи	Задержка
900 – 1200 км (*LEO*)	1 – 200 Гбит/с	35 мс
~ 2 000 км (*MEO*)	1 – 200 Гбит/с	~ 60 мс
Космос-космос ~ 100 км	~ Тбит/с	
Космос-космос ~ 1000 км	~ 10 Гбит/с	

Требования к будущей сети со стороны *STIN*:

– гибкая адресация и маршрутизация. Необходимо решить проблему IP-адресации тысяч спутников *LEO* с наземной интернет-инфраструктурой, поскольку IP-адреса в космосе будут динамически соединяться с различными автономными системами на Земле с разными сетевыми IP-префиксами.

– по сравнению с высокой пропускной способностью оптоволоконных линий, каналы, соединяющие спутники *LEO* в космосе и наземную инфраструктуру Интернета, могут стать узким местом с точки зрения пропускной способности;

– управление доступом к спутникам. В будущей сети необходимо обеспечить связь мобильного устройства со спутником. В этой ситуации спутник является точкой доступа, он должен обладать информацией о величине трафика в космической сети;

– граничные вычисления и хранение данных вызовет проблемы на стороне спутника *LEO*.

Индустриальный Интернет вещей *IIoT* с облачными технологиями. Концептуальные основы Индустриального Интернета вещей IIoT (*Industrial Internet of Things*) определены в контексте ЧПР. Требования к будущей сети со стороны *IIoT:*

- задержка. Подсистемы управления могут работать с длительностью цикла от субмиллисекунд (доли 1 мс) до 10 мс. Задержки сигнализации должны быть на уровне времени цикла с джиттером на уровне 1 мкс;

- временная синхронизация является фундаментальным требованием для многопроводных приложений;

- малый и ограниченный джиттер. Для систем управления движением и некоторых критических ситуаций он должен быть на уровне субмикросекунд;

- безопасность и безотказность. Требования доступности услуг для приложений IIoT обычно составляет от 99,9999% до 99,999999%.

Приложения больших научных данных. Для передачи и обработки больших научных данных *HSD* (*Huge Scientific Data)* от астрономических телескопов, ускорителей заряженных частиц, термоядерных реакторов к будущей сети предъявляются следующие требования:

– потребность в пропускной способности от 100 Гбит/с до 1 Тбит/с;

– сквозное качество обслуживания *QoS*. Сеть должна обеспечивать пропускную способность и распределение ресурсов динамически с учётом потребности;

– синхронизация. Телескопы имеют ограниченные локальные хранилища и непрерывно собираемые данные должны передаваться в реальном времени;

– готовность. Коэффициент готовности колеблется от 99,95% до 99,999%.

Пересылка пачек данных с учётом приложений *ABF (Application-aware Data Burst Forwarding)* используется для значительного сокращения времени передачи данных приложения. Сквозной виртуальный канал создаётся по запросу для каждой пачечной передачи. Сеть должна поддерживать быстрое установление виртуального канала и его разрушение. В отличие от алгоритмов контроля перегрузки механизм разрешения передачи работает как коммутатор для включения/выключения передачи пачек. Как только передача разрешена, пачка пересылается из источника данных с использованием всей скорости линии. Этот механизм используется в системах управления с обратной связью.

Услуги в зоне аварийно-спасательных операций *EDR (Emergency and Disaster Rescue)* должны обеспечить индивидуальное квалифицированное управление самоэвакуацией в ближайшую безопасную зону. Эти услуги должны быть доступны любому пользователю в любом месте и в любое время.

Для реализации этого требования при чрезвычайных ситуациях в масштабе объекта должны быть использованы сети связи общего пользования и сотовые мобильные сети. В перспективе необходимо сделать эту услугу доступной в региональном и глобальном масштабах.

Социальный Интернет вещей *SIoT (Social Internet Things)* предназначен для использования потенциала соци-

альных сетей. Будущие сети должны поддерживать: открытые интерфейсы сетевых услуг; мобильность по запросу; обеспечивать виртуализацию социальных объектов; доступность вычислительных ресурсов и ресурсов хранения на границе сети; предоставлять инструменты для защиты *SIoT* от атак; поддерживать энергоэффективность «вещей», большинство которых работает от батарей.

Связанный и совместный искусственный интеллект *CSAI (Connectivity and Sharing Artificial Intelligence).* В Интернете вещей (*IoT*) произойдёт сдвиг от подключения обычных вещей к подключённым интеллектуальным вещам. Так, автономные автомобили могут снабжаться алгоритмами распознавания изображений на основе данных, полученных с бортовых датчиков, позволяющих оперативно обнаруживать препятствия и соответственно маневрировать.

Основные требования *CSAIr* к будущим сетям: сеть должна поддерживать мобильность по требованию; необходимы сетевые протоколы для обеспечения низкого энергопотребления при взаимодействии между интеллектуальными объектами; использовать технологии виртуализации, позволяющие развернуть ИИ-компоненты гибким способом; совместная оркестровка сети, интеллекта и вычислений; при массовом использовании ИИ потребуется большая пропускная способность сети при малой задержки передачи данных (менее 1 мс); необходима адресация ИИ-компонентов; единообразные интерфейсы сети для описания ИИ-возможностей; программируемость сети – могут потребоваться специальные сетевые процедуры, которые распознают объекты и эффективно пересылают им данные; повышенные требования к обеспечению безопасности и конфиденциальности.

Заключение

Прошло более 10 лет с провозглашения Четвёртой промышленной революции, которая является естественным продолжением Третьей (цифровой) промышленной революции. В основе Четвёртой промышленной революции лежат прорывные технологии физического, цифрового и биологического блоков. Инновационные технологии способствуют реализации концепций «Будущие сети» и «Сети 2030» фиксированных сетей связи и сотовых мобильных сетей связи поколений 5G и 6G.

Четвёртая промышленная революция окажет фундаментальное воздействие на экономику. Ключевым вопросом становится способность экономики реализовывать инновации. Основным ресурсом инновационной экономики считается интеллект. Для стимулирования инновационной деятельности необходимы вложения в человеческий капитал и технологии.

Внедрение прорывных технологий обеспечивает совершенствование существующих и создание новых технологических систем в экономических, политических, социальных и духовных сферах общества, влияющих на жизнь каждого человека.

Литература

1. *Шваб Клаус*. Четвертая промышленная революция: пер. с анг. М.: Издательство «Эксмо», 2017. 208 с.

2. *Качала В.В.* Общая теория систем и системный анализ. Учебник для вузов. М.: Горячая линия – Телеком, 2017. 432 с.

3. *Шваб Клаус, Дэвис Николас*. Технологии Четвёртой промышленной революции, / пер. с англ. М.: Эксмо, 2019. 320 с.

4. *Росляков А.В., Ваняшин С.В.* Будущие сети (Future Networks). Самара: ПГУТИ, 2015. 274 с.

5. *Росляков А.В.* Будущие сети: обзор подходов к новой телекоммуникационной парадигме // Электросвязь. 2020. № 9. С. 30-37.

6. *Росляков А.В.* СЕТЬ 2030: архитектура, технологии, услуги. М.: Колосс-с, 2022. 324 с.

7. *Росляков А.В.* "СЕТЬ-2030": взгляд МСЭ-Т на будущее сетей фиксированной связи // Первая миля. 2021. №4. С. 50-59.

8. ITU-R, IMT traffic estimates for the years 2020 to 2030, Report ITU-R M. 2370-0, July 2015 (дата обращения 12.09. 2022).

9. Network 2030. A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond. FG-NET-2030. Geneva, 2019.

10. ITU-T FG NET2030 Deliverable "New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis". Geneva, 2019.

11. ITU-T FG NET-2030 Technical Report "Gap Analysis of New Services, Capabilities and Use Cases for the Networks in 2030 and Beyond". Geneva, 2020.

12. The Fifth Generation Fixed Network (F5G). Bringing Fibred to Everywhere and Everything. ETSI White Paper No. 41, 2020. 24 p.

13. *Тихвинский В.О., Терентьев С.В., Коваль В.А.* Сети мобильной связи 5G: Технологии, архитектура и услуги. М.: Издательский дом Медиа Паблишер, 2019. 376 с.

14. *Вэнь Тонг, Пейин Чжу*. Сети 6G. Путь от 5G к 6G глазами разработчиков. От подключённых людей и вещей к подключённому интеллекту, / пер. с англ. В.С. Яценкова. М.: ДМК Пресс, 2022. 624 с.

15. *Молчановс Д.А, Бегишев В.О., Самуйлов К.Е., Кучерявый Е.А*. Сети 5G/6G: архитектура, технологии, методы анализа и расчёта: монография. М.: РУДН, 2022. 516 с.

16. 6G (шестое поколение мобильной связи). https://www.tadviser.ru/index.php (дата обращения 20.09.2022).

17. Mobile Ad-h0c Networks (manet). https://datatracker.ietf.org/wg/manet/about/ (дата обращения 20.06.2022).

18. *Росляков А.В*. Сети следующего поколения NGN. М.: Эко-Трендз, 2009. 424 с.

19. Целевая группа по технологиям для Сети 2030. https://www.itu.int/en/ITUT/focusgroups/net2030/Pages/default.aspx#/ru (дата обращения 20.06.2022).

20. ITU-T. Tactile Internet. https//www.itu.int/en/ITU-T/techwatch/Pages/tactileinternet.aspx (дата обращения 12.09.2022).

PROMISING INFOCOMMUNICATION TECHNOLOGIES AND NETWORK SERVICES

ANATOLIY P. PSHENICHNIKOV
Moscow, Russia

VICTORIA I. KOROTKOVA
Moscow, Russia

LEONID S. POSKOTIN
Moscow, Russia

KEYWORDS: *digital breakthrough technologies, basic and composite network services, technological revolution, industrial revolution, artificial intelligence, robots, fixed communication networks, cellular mobile communication networks.*

ABSTRACT

Introduction. The essence of the Fourth Industrial Revolution is not only the emergence of new technologies, but also the integration of existing ones in a single system available for widespread use. The technological revolution penetrates in all spheres of public life, automates production processes, and adjusts the connection between physical and computing resources. Such innovations as cyber-physical systems, artificial intelligence, big data, the Internet of Things, robotics, cloud technologies, space technologies, virtual reality and some others supported these transformations. New digital technologies can have both a positive and a negative impact on various spheres of society, for example: unemployment, inequality, economic development, security and others. **The aim of the work** is to obtain a minimum level of understanding of digital breakthrough technologies, to reveal their potential and their connection with the systemic changes caused by the industrial revolution. When considering the impact of breakthrough technologies on the implementation of the Fourth Industrial Revolution, a systematic methodology should be used. Promising technologies are considered that significantly affect the implementation of the industrial revolution. **Discussion:** graphical dependences of the speed of fixed communication networks in the implementation of their development concepts for the period 1960-2030 and graphical dependences of the speed of cellular mobile networks of generations 1G-6G for the period 1970-2030 are given. It is noted that the change of concepts for the development of fixed communication networks and generations of cellular mobile communication networks since 2000 are consistent in time in accordance with the "10-year rule". The evolution of technologies and services of cellular mobile and fixed-line networks is presented. In future networks, basic and composite network services are predicted. The paper briefly discusses basic network services with a list of necessary functions for the implementation of communications. Similarly, a brief analysis of composite network services and applications is presented, listing the network requirements for their implementation. In order to fully unlock the potential of innovative technologies and services of the industrial revolution, significant reforms are needed in the economic, social, political and spiritual spheres of society.

REFERENCES

1. Klaus Schwab (2016). The Fourth Industrial Revolution. Switzerland: World Economic Forum, 172 p.

2. V.V. Kachala (2017).General theory of systems and system analysis. Textbook for universities. Moscow: Goriachaia liniia – Telekom, 432 p. (In Rus)

3.Klaus Schwab (2018). Shaping the Fourth Industrial Revolution. Switzerland: World Economic Forum, 320 p.

4. A.V. Rosljakov, S.V. Vanjashin (2015). Future Networks. Samara: PGUTI, 274 p. (In Rus)

5. A.V. Rosljakov (2020). Future networks: an overview of approaches to the new telecommunications paradigm. *Elektrosvjaz'*. No.9, pp. 30-37. (In Rus)

6. A.V. Rosljakov (2022). NETWORK 2030: architecture, technologies, services. Moscow: Koloss-s, 324 p. (In Rus)

7. A.V. Rosljakov (2021). NETWORK-2030": ITU-T's view on the future of fixed-line networks. Pervaja milja. No.4, pp. 50-59. (In Rus)

8. ITU-R, IMT traffic estimates for the years 2020 to 2030, Report ITU-R M. 2370-0, July 2015 (date of access 12.09. 2022).

9. Network 2030. A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond. FG-NET-2030. Geneva, 2019.

10. ITU-T FG NET2030 Deliverable "New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis". Geneva, 2019.

11. ITU-T FG NET-2030 Technical Report "Gap Analysis of New Services, Capabilities and Use Cases for the Networks in 2030 and Beyond". Geneva, 2020.

12. The Fifth Generation Fixed Network (F5G). Bringing Fibred to Everywhere and Everything. ETSI White Paper No. 41, 2020. 24 p.

13. V.O. Tihvinskij, S.V. Terent'ev, V.A. Koval' (2019). 5G mobile communication networks: Technologies, architecture and services. Moscow: Media Pablisher. 376 p. (In Rus)

14. Wen Tong, Peiying Zhu (2021). 6G: The Next Horizon. From Connected People and Things to Connected Intelligence. Cambridge University Press, 624 p.

15. D.A. Molchanov, V.O. Begishev, K.E. Samujlov, E.A. Kucherjavyj (2022). 5G/6G networks: architecture, technologies, methods of analysis and calculation. Moscow: RUDN, 2022. 16 p. (In Rus)

16. 6G (shestoe pokolenie mobil'noj svjazi) [6G (the sixth generation of mobile communications)]. URL: https://www.tadviser.ru/index.php (date of access 20.09.2022). (In Rus)

17. Mobile Ad-h0c Networks (manet). URL: https://datatracker.ietf.org/wg/manet/about/ (date of access 20.06.2022).

18. A.V. Rosljakov (2009). Next-generation NGN networks. Moscow: Jeko-Trendz, 424 p. (In Rus)

19. Technology Task Force for the 2030 Network. URL: https://www.itu.int/en/ITUT/focusgroups/net2030/Pages/default.aspx#/ru (date of access 20.06.2022). (In Rus)

20. ITU-T. Tactile Internet. URL: https//www.itu.int/en/ITU-T/techwatch/Pages/tactileinternet.aspx (date of access 12.09.2022).

INFORMATION ABOUT AUTHORS:

[1] **Anatoliy P. Pshenichnikov,** PhD, Full Professor, Professor at Moscow Technical Univesity of Communictions and Informatics, Moscow, Russia

[2] **Victoria I. Korotkova,** postgraduate student of Moscow Technical Univesity of Communictions and Informatics, Moscow, Russia

[3] **Leonid S. Poskotin,** postgraduate student of Moscow Technical Univesity of Communictions and Informatics, Moscow, Russia

For citation: Pshenichnikov A.P., Korotkova V.I., Poskotin L.S. Promising infocommunication technologies and network services. H&ES Reserch. 2023. Vol. 15. No. 3. P. 57-64. doi: 10.36724/2409-5419-2023-15-3-57-64 (In Rus)