

ISSN: 1812-5220 (Print)  
ISSN: 2658-7882 (Online)



Том 22, 2025, № 1  
Vol. 22, 2025, No. 1

Научно-практический журнал

# Проблемы анализа риска

Scientific and Practical Journal

## Issues of Risk Analysis

---

Главная тема номера:

Военно-политические и глобальные риски

Volume Headline:

Military-Political and Global Risks

Том 22, 2025, № 1  
Vol. 22, 2025, No. 1

ISSN: 1812-5220 (Print)  
ISSN: 2658-7882 (Online)

Научно-практический журнал

# Проблемы анализа риска

Scientific and Practical Journal

# Issues of Risk Analysis

Периодичность 6 выпусков в год  
*Frequency of 6 releases in a year*

Основан в 2004 г.  
*Founded in 2004*



Федеральное государственное бюджетное учреждение  
«Всероссийский научно-исследовательский институт по проблемам гражданской обороны  
и чрезвычайных ситуаций МЧС России» (федеральный центр науки и высоких технологий)  
*Federal State Budgetary Establishment "All-Russian Scientific Research Institute for Civil Defence  
and Emergencies of the EMERCOM of Russia" (Federal Science and High Technology Center)*

# Проблемы анализа риска

## *Problemy analiza riska*

### Цели и задачи журнала

**Цель:** способствовать становлению культуры управления рисками, обобщению опыта исследований риска, внедрению инновационных подходов, созданию баз знаний и данных, информационного пространства по риску, сопровождению научных проектов, созданию и внедрению профессиональных и образовательных стандартов и программ, координации деятельности специалистов по анализу и управлению рисками, разработке нормативных показателей допустимого (приемлемого) риска, законодательного и правового обеспечения.

**Задача:** дать информацию о результатах последних научных исследований в области анализа и управления рисками, что помогает специалистам по управлению рисками решать насущные проблемы, внедрять инновационные научные разработки и применять научный опыт в практической деятельности управления рисками в чрезвычайных ситуациях, обеспечения безопасности жизнедеятельности населения, глобальной и региональной безопасности, защите окружающей среды, построения и совершенствования систем управления рисками в организациях и на предприятиях различных отраслей экономики.

### *Aims and Scope of the journal*

**Aim:** to promote formation of culture of risk management, synthesis of experience of researches of risk, introduction of innovative approaches, creation of knowledge bases and data, information space on risk, support of scientific projects, creation and introduction of professional and educational standards and programs, coordination of activity of specialists in the analysis and risk management, development of standard indicators of admissible (acceptable) risk, legislative and legal support.

**Scope:** to give information on results of the last scientific research in the field of the analysis and risk management that helps specialists in risk management to solve pressing problems, to introduce innovative scientific developments and to apply scientific experience in practical activities of risk management in emergency situations, safety of activity of the population, global and regional security, environment protection, construction and improvement of risk management systems in the organizations and at the enterprises of various sectors of the economy.

### Учредитель *Founder*

Федеральное государственное бюджетное учреждение «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (федеральный центр науки и высоких технологий) 121352, г. Москва, ул. Давыдовская, д. 7

*Federal State Budgetary Establishment "All-Russian Scientific Research Institute for Civil Defence and Emergencies of the EMERCOM of Russia" (Federal Science and High Technology Center)  
7, St. Davydkovskaya, Moscow, 121352*

### Издатель и редакция журнала *Publisher and Editorial Office of the Journal*

Федеральное государственное бюджетное учреждение «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (федеральный центр науки и высоких технологий) 121352, г. Москва, ул. Давыдовская, д. 7

*Federal State Budgetary Establishment "All-Russian Scientific Research Institute for Civil Defence and Emergencies of the EMERCOM of Russia" (Federal Science and High Technology Center)  
7, St. Davydkovskaya, Moscow, 121352*

#### Главный редактор:

Быков Андрей Александрович,  
д.ф.-м.н., проф., заслуженный деятель науки РФ, г. Москва, Россия  
E-mail: parjournal@mail.ru

#### Editor-in-Chief:

Andrey A. Bykov,  
Doctor of physics and mathematics, Professor, honored scientist of Russia Federation, Moscow, Russia  
E-mail: parjournal@mail.ru

#### Ответственный секретарь:

Виноградова Лилия Владимировна,  
младший научный сотрудник научно-исследовательского центра ФГБУ ВНИИ ГОЧС (ФЦ), г. Москва, Россия  
E-mail: parjournal@mail.ru

#### Responsible secretary:

Lyliya V. Vinogradova,  
Junior Researcher, Research Center  
of the VNIi GOChS (FC), Moscow, Russia  
E-mail: parjournal@mail.ru

Верстка:  
Кожемякин Владимир Владимирович

*Imposition:*  
Vladimir V. Kozhemyakin

Корректур:  
Базанова Наталья Кирилловна

*Updates:*  
Natalia K. Bazanova

---

Журнал издается с 2004 года  
Периодичность: 6 номеров в год  
ISSN: 1812-5220 (Print)  
ISSN: 2658-7882 (Online)  
Свидетельство о регистрации средства массовой информации  
ПИ № ФС77-85693 от 14.08.2023

*The journal is issued since 2004*  
*Frequency: 6 numbers a year*  
*ISSN: 1812-5220 (Print)*  
*ISSN: 2658-7882 (Online)*  
*Certificate of registration of mass media ПИ № ФС 77-85693*  
*from 14.08.2023*

Журнал включен в Перечень ведущих рецензируемых научных журналов и изданий, рекомендованных Высшей аттестационной комиссией Минобрнауки России (ВАК) для опубликования основных научных результатов диссертаций на соискание ученых степеней доктора и кандидата наук.

Решением ВАК от 21.12.2023 г. № 3/пл/1 журнал с 01.01.2024 отнесен к категории К 1 сроком на три года.

Журнал индексируется РИНЦ, INDEX COPERNICUS, Science Index, Ulrich's

*The journal is included in the list of the leading reviewed scientific journals and editions recommended by the Highest certifying commission of the Ministry of Education and Science of the Russian Federation (VAK) for publication of the main scientific results of theses for a competition of academic degrees of the doctor and candidate of science.*

*By the decision of the VAK of 21.12.2023 No. 3/pl/1, the journal has been assigned to category K 1 for a period of three years since 01.01.2024.*

*The journal is indexed RINTS, INDEX COPERNICUS, Science Index, Ulrich's*

---

При перепечатке и цитировании ссылка на журнал «Проблемы анализа риска» обязательна. Присланные в редакцию материалы рецензируются и не возвращаются. Статьи, не оформленные в соответствии с Инструкцией для авторов, к рассмотрению не принимаются.

*At a reprint and citing the reference to the "Issues of Risk Analysis" journal is obligatory. The materials sent to edition are reviewed and are not returned. Articles which are not issued according to the Instruction for authors are not taken cognizance.*

---

Формат 60×84 1/8. Объем 12 печ. л. Печать цифровая.  
Тираж 1000 экз.

Подписано в печать: 24.02.2025

Цена свободная

© Проблемы анализа риска, 2025

Отпечатано в ООО «Типография Форпринт»,  
123298, г. Москва, ул. Маршала Бирюзова, д. 1, корп. 11  
*Format 60×84 1/8. Volume is 12 print. pages. Digital printing.*  
*Circulation is 1000 copies.*

*It is sent for the press: 24.02.2025*

*Free price*

© *Issues of Risk Analysis, 2025*

*Printed in the typography of Forprint Printing House LLC,*  
*1, Marshal Biryuzov St., bldg. 11, 123298, Moscow*

---

Распространяется по подписке

*Объединенный каталог Пресса России*

*Подписной индекс:*

*15704 — период подписки от 2 мес.*

*85800 — период подписки от 12 мес.*

*Оформить подписку можно:*

*– подписное агентство Урал Пресс Округ (подписка на печатную или электронную версию)*

*информация на сайте: <https://www.ural-press.ru/contact/>;*

*– подписное агентство АРЗИ (подписка на печатную версию)*

*<https://www.pressa-rf.ru/cat/1/section/2/>*

*Extends on a subscription*

*United Catalogue Press of Russia*

*Subscription index:*

*15704 — subscription period from 2 months*

*85800 — subscription period from 12 months*

*You can subscribe to:*

*– subscription agency Ural Press District (subscription to print and electronic version)*

*information or website: <https://www.ural-press.ru/contact/>;*

*– subscription agency ARZI (subscription to the printed version) <https://www.pressa-rf.ru/cat/1/section/2/>*

---

<http://www.risk-journal.com>

 <https://vk.com/parjournal>

## Наблюдательный совет

### Махутов Николай Андреевич (председатель)

Член-корреспондент РАН, доктор технических наук, профессор, председатель Комиссии РАН по техногенной безопасности, г. Москва, Россия

### Акимов Валерий Александрович (заместитель председателя)

Доктор технических наук, профессор, заслуженный деятель науки РФ, главный научный сотрудник, ФГБУ «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (ФЦ), г. Москва, Россия

### Верещагин Виктор Владимирович

Кандидат исторических наук, член Совета директоров Международной ассоциации федераций риск-менеджмента (IFRIMA), Президент Русского общества управления рисками (РусРиск), г. Москва, Россия

## Редакционная коллегия

### Быков Андрей Александрович (главный редактор)

Доктор физико-математических наук, профессор, заслуженный деятель науки РФ, действительный член Русского общества управления рисками, г. Москва, Россия

### Порфирьев Борис Николаевич (заместитель главного редактора)

Академик РАН, доктор экономических наук, профессор, научный руководитель, Институт народнохозяйственного прогнозирования РАН, г. Москва, Россия

### Башкин Владимир Николаевич (заместитель главного редактора по вопросам экологической безопасности)

Доктор биологических наук, профессор, главный научный сотрудник, Институт физико-химических и биологических проблем почвоведения РАН, г. Пушкино, Россия

### Каранина Елена Валерьевна (заместитель главного редактора по вопросам региональной и экономической безопасности)

Доктор экономических наук, доцент, член-корреспондент Российской академии естествознания, заведующий кафедрой финансов и экономической безопасности, ФГБОУ ВО «Вятский государственный университет», г. Киров, Россия

### Бродский Юрий Игоревич

Доктор физико-математических наук, ведущий научный сотрудник, Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва, Россия

### Голембиовский Дмитрий Юрьевич

Доктор технических наук, профессор, профессор кафедры исследования операций факультета вычислительной математики и кибернетики, МГУ им. М. В. Ломоносова, г. Москва, Россия

### Елохин Андрей Николаевич

Доктор технических наук, член-корреспондент РАН, действительный член Академии геополитических проблем, первый вице-президент, Ассоциация риск-менеджмента «Русское общество управления рисками», г. Москва, Россия

### Ерешко Феликс Иванович

Доктор технических наук, профессор, заведующий отделом, Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва, Россия

### Колесников Евгений Юрьевич

Доктор технических наук, доцент, профессор Высшей школы техносферной безопасности, СПбПУ им. Петра Великого, г. Санкт-Петербург, Россия

### Котловский Игорь Борисович

Кандидат экономических наук, действительный член Российской академии естествознания, доцент, заведующий кафедрой управления рисками и страхования, МГУ им. М. В. Ломоносова, г. Москва, Россия

## Supervisory Council

### Makhutov Nikolay Andreevich (Chairman)

Corresponding Member of RAS, Doctor of Sciences in Technology, Professor, Chairman of the RAS Commission on Technogenic Safety, Moscow, Russia

### Akimov Valery Aleksandrovich (Deputy Chairman)

Doctor of Sciences in Technology, Professor, Honored Scientist of Russia, Chief Researcher, All-Russian research Institute for Civil Defense and Emergency Situations of EMERCOM of Russia, Moscow, Russia

### Vereshchagin Victor Vladimirovich

Candidate of Sciences in History, Member of the Board of Directors of the International Association of Risk Management Federations (IFRIMA), President of the Russian Risk Management Society (RusRisk), Moscow, Russia

## Editorial Board

### Bykov Andrey Aleksandrovich (Editor-in-Chief)

Doctor of Sciences in Physics and Mathematics, Professor, Honored Scientist of Russia Federation, Full Member of the Russian Risk Management Society, Moscow, Russia

### Porfiriev Boris Nikolayevich (Deputy Editor-in-Chief)

Academician of RAS, Doctor of Sciences in Economics, Professor, Scientific Director, Institute of Economic Forecasting of RAS, Moscow, Russia

### Bashkin Vladimir Nikolaevich (Deputy Editor-in-Chief for Environmental Safety)

Doctor of Sciences in Biology, Professor, Chief Researcher, Institute of Physico-Chemical and Biological Problems of Soil Science RAS, Pushchino, Russia

### Karantina Elena Valerevna (Deputy Editor-in-Chief for Regional and Economic Security)

Doctor of Sciences in Economics, Associate Professor, Corresponding Member of the Russian Academy of Natural Sciences, Head of the Department of Finance and Economic Security, Vyatka State University, Kirov, Russia

### Brodsky Yury Igorevich

Doctor of Sciences in Physics and Mathematics, Leading Researcher, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia

### Golembiovsky Dmitry Yuryevich

Doctor of Sciences in Technology, Professor, Professor Department of operations research Faculty of computational mathematics and cybernetics, MSU named after M. V. Lomonosov, Moscow, Russia

### Elokhin Andrey Nikolaevich

Doctor of Sciences in Technology, Corresponding Member of RANS, Full Member of the Academy of Geopolitical Problems, First Vice President, Risk Management Association "Russian Risk Management Society", Moscow, Russia

### Ereshko Felix Ivanovich

Doctor of Sciences in Technology, Professor, Head of Department, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia

### Kolesnikov Evgeny Yuryevich

Doctor of Sciences in Technology, Associate Professor, Professor of the Higher School of Technosphere safety, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia

### Kotlovsky Igor Borisovich

Candidate of Sciences in Economics, Associate Professor, Full Member of the Russian Academy of Natural Sciences, Head of the Department of Risk Management and Insurance, MSU named after M. V. Lomonosov, Moscow, Russia

**Макашина Ольга Владиленовна**

Доктор экономических наук, профессор, профессор  
Департамента общественных финансов, Финансовый  
университет при Правительстве РФ, г. Москва, Россия

**Мальшев Владлен Платонович**

Доктор химических наук, профессор, заслуженный деятель  
науки РФ, главный научный сотрудник, ФГБУ «Всероссийский  
научно-исследовательский институт по проблемам  
гражданской обороны и чрезвычайных ситуаций МЧС России»  
(ФЦ), г. Москва, Россия

**Мартынюк Василий Филиппович**

Доктор технических наук, доцент, профессор кафедры  
промышленной безопасности и охраны окружающей среды,  
РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва, Россия

**Морозко Нина Иосифовна**

Доктор экономических наук, профессор, профессор кафедры  
«Денежно-кредитные отношения и монетарная политика»,  
Финансовый университет при Правительстве РФ, г. Москва,  
Россия

**Опарин Сергей Геннадиевич**

Член-корреспондент Академии военных наук,  
доктор технических наук, профессор, профессор кафедры  
«Экономика и менеджмент в строительстве»,  
Петербургский государственный университет путей сообщения  
Императора Александра I, г. Санкт-Петербург, Россия

**Помазанов Михаил Вячеславович**

Кандидат физико-математических наук, Руководитель  
подразделения валидации, ПАО Промсвязьбанк, Дирекция  
«Риски», г. Москва, Россия

**Ревич Борис Александрович**

Доктор медицинских наук, профессор, нобелевский лауреат  
в составе Межправительственной группы экспертов  
по изменению климата, руководитель лаборатории  
прогнозирования качества окружающей среды и здоровья  
населения, Институт народнохозяйственного прогнозирования  
РАН, г. Москва, Россия

**Сосунов Игорь Владимирович**

Кандидат технических наук, доцент, заместитель начальника,  
ФГБУ «Всероссийский научно-исследовательский институт по  
проблемам гражданской обороны и чрезвычайных ситуаций  
МЧС России» (ФЦ), г. Москва, Россия

**Фалеев Михаил Иванович**

Кандидат политических наук, помощник начальника отряда,  
ФГКУ «Государственный центральный аэромобильный  
спасательный отряд», г. Жуковский, Россия

**Шевченко Андрей Владимирович**

Доктор технических наук, профессор, главный научный  
сотрудник, ФГБУ «ЦНИИ ИВ» Минобороны России, г. Москва,  
Россия

**Шемякина Татьяна Юрьевна**

Кандидат экономических наук, профессор, заместитель  
заведующего кафедрой, Государственный университет  
управления, г. Москва, Россия

**Makashina Olga Vladilenovna**

Doctor of Sciences in Economics, Professor, Professor Department  
of public Finance, Financial University under the Government of  
the Russian Federation, Moscow, Russia

**Malyshev Vladlen Platonovich**

Doctor of Sciences in Chemistry, Professor, Honored Scientist  
of Russia Federation, Chief Researcher, All-Russian research  
Institute for civil defense and emergency situations of EMERCOM  
of Russia, Moscow, Russia

**Martynyuk Vasily Filippovich**

Doctor of Sciences in Technology, Associate Professor, Professor  
of the Department Industrial Safety and Environmental  
Protection, National University of Oil and Gas "Gubkin University",  
Moscow, Russia

**Morozko Nina Iosifovna**

Doctor of Sciences in Economics, Professor, Professor of the  
Department "Monetary relations and monetary policy", Financial  
University under the Government of the Russian Federation,  
Moscow, Russia

**Oparin Sergey Gennadievich**

Corresponding Member of the Military Sciences Academy,  
Doctor of Sciences in Technology, Full Professor, Professor  
Department of Economics and Management in Construction,  
Emperor Alexander I St. Petersburg State Transport University,  
St. Petersburg, Russia

**Pomazanov Mikhail Vyacheslavovich**

Candidate of Science in Physics and Mathematics, Head of  
Validation Unit, PJSC Promsvyazbank, Management "Risks",  
Moscow, Russia

**Revich Boris Aleksandrovich**

Doctor of Sciences in Medicine, Professor, Nobel Laureate in  
the Intergovernmental Panel on Climate Change, Head of the  
Laboratory of Environmental and Public Health Forecasting,  
Institute of Economic Forecasting of RAS, Moscow, Russia

**Sosunov Igor Vladimirovich**

Candidate of Sciences in Technology, Associate Professor,  
Deputy chief, All-Russian Research Institute for Civil Defense and  
Emergency Situations of EMERCOM of Russia, Moscow, Russia

**Faleev Mihail Ivanovich**

Candidate of Sciences in Politics, Assistant to the Chief of Group,  
Federal Public Treasury Institution "State Central Airmobile  
Rescue Group", Zhukovsky, Russia

**Shevchenko Andrey Vladimirovich**

Doctor of Sciences in Technology, Professor, Chief Researcher,  
Central Research Test Institute of Engineering Troops of the  
Ministry of Defense of the Russian Federation, Moscow, Russia

**Shemyakina Tatyana Yurievna**

Candidate of Sciences in Economics, Professor, Deputy Head  
of the Department, State University of Management, Moscow,  
Russia

# Content

## Editor's Column

- 8 About Modern Military-Political, Global and Regional Risks  
*Andrey A. Bykov, Editor-in-Chief*

## Risk Military-Political

- 12 Possible Directions for Reducing Military-Strategic Risks in the Threat of the Use of Nuclear Weapons  
*Vladlen P. Malyshev, Vasily A. Duganov, Oleg V. Vinogradov, Federal State Budgetary Establishment «All-Russian Scientific Research Institute for Civil Defence and Emergencies of the EMERCOM of Russia» (Federal Science and High Technology Center), Moscow, Russia*

## Global Risks

- 24 Crisis Genesis of Global Risks: Growth Factors and Directions of Anti-Crisis Policy  
*Yuriy A. Krupnov, Sergei N. Sil'vestrov, Financial University under the Government of the Russian Federation, Institute of Economic Policy and Economic Security Problems, Moscow, Russia*

## Information Security

- 34 Risk-Oriented Approach to Assessing the Information and Digital Component of Economic Security of Small Business Entities  
*Elena V. Karanina, Asya V. Kotandzhyan, Vyacheslav L. Korshunov, Vyatka State University, Kirov, Russia*

## Production Safety

- 46 Formation and Development of the «Hazard and Operability Studies» as a Method of Accident Risk Analysis  
*Oleg I. Dronyaev, Vasily Ph. Martynyuk, Gubkin Russian State University of Oil and Gas, Moscow, Russia*

## Ecological Risk

- 54 Management of Environmental Impact on Atmospheric Air by the Oil and Gas Business (on the Example of the Activities of PJSC OC «ROSNEFT» for 2012–2023)  
*Olga P. Trubitsina, Northern (Arctic) Federal University, Arkhangelsk, Russia*  
*Vladimir N. Bashkin, Institute of Physicochemical and Biological Problems in Soil Science RAS, Pushchino, Russia*

## Natural Risk

- 62 Cyclonic Activity of Tropical Cyclones and Some of its Features. Part V. Seismic Response in a Number of Magnitude Ranges to Long-Term Cyclonic Activity of Tropical Cyclones  
*Mikhail I. Yaroshevich, Obninsk, Russia*

## Project Risk

- 68 Analysis of the Processes of Creating IT-Products as Part of the Implementation of IT-Projects  
*Valentin S. Nikolaenko, Tomsk State University of Control Systems and Radioelectronics; Tomsk Polytechnic University; Siberian State Medical University, Tomsk, Russia*

## Financial Risk

- 88 Using the Benford Distribution to Reduce the Risk of Undetected Misstatements of Financial Statements  
*Sergey Y. Krivolapov, Anna V. Komissarova, Daniil A. Khamula, Financial University under the Government of the Russian Federation, Moscow, Russia*

# Содержание

## Колонка редактора

- 8 О современных военно-политических, глобальных и региональных рисках  
*Быков А.А., главный редактор*

## Риск военно-политический

- 12 Возможные направления снижения военно-стратегических рисков при угрозе применения ядерного оружия  
*Мальшиев В.П., Дуганов В.А., Виноградов О.В., Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России (федеральный центр науки и высоких технологий), г. Москва, Россия*

## Глобальные риски

- 24 Кризисогенность глобальных рисков: факторы роста и направления антикризисной политики  
*Крупнов Ю.А., Сильвестров С.Н., Финансовый университет при Правительстве Российской Федерации, Институт экономической политики и проблем экономической безопасности, г. Москва, Россия*

## Информационная безопасность

- 34 Риск-ориентированный подход к оценке информационно-цифровой составляющей экономической безопасности субъектов малого предпринимательства  
*Каранина Е.В., Котанджян А.В., Коришунов В.Л., Вятский государственный университет, г. Киров, Россия*

## Производственная безопасность

- 46 Становление и развитие метода «Анализ опасности и работоспособности» как метода анализа риска аварий  
*Дроняев О.И., Мартынюк В.Ф., РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва, Россия*

## Риск экологический

- 54 Управление экологическим воздействием нефтегазового бизнеса на атмосферный воздух (на примере деятельности ПАО «НК «РОСНЕФТЬ» за 2012–2023 годы)  
*Трубицина О.П., Северный (Арктический) федеральный университет имени М.В. Ломоносова, г. Архангельск, Россия*  
*Башкин В.Н., Институт физико-химических и биологических проблем почвоведения РАН, г. Пущино, Россия*

## Риск природный

- 62 Циклоническая активность тропических циклонов и некоторые ее особенности. Часть V. Сейсмическая реакция в ряде диапазонов магнитуд на многолетнюю циклоническую активность тропических циклонов  
*Ярошевич М.И., г. Обнинск, Россия*

## Риск проектный

- 68 Анализ процессов создания ИТ-продуктов в рамках выполнения ИТ-проектов  
*Николаенко В.С., Томский государственный университет систем управления и радиоэлектроники; Томский политехнический университет; Сибирский государственный медицинский университет, г. Томск, Россия*

## Риск финансовый

- 88 Использование распределения Бенфорда для снижения риска необнаружения искажений финансовой отчетности  
*Криволапов С.Я., Комиссарова А.В., Хамула Д.А., Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия*

<https://elibrary.ru/fnxwfu>

ISSN 1812-5220

© Проблемы анализа риска, 2025

# О современных военно-политических, глобальных и региональных рисках

**Быков А.А.**,  
главный редактор

Для цитирования: Быков А.А. О современных военно-политических, глобальных и региональных рисках // Проблемы анализа риска. 2025. Т. 22. № 1. С. 8–10. — EDN: AWGWCG.

## About Modern Military-Political, Global and Regional Risks

**Andrey A. Bykov**,  
Editor-in-Chief

For citation: Bykov A.A. About modern military-political, global and regional risks // Issues of Risk Analysis. 2025;22(1): 8-10 (In Russ.). — EDN: AWGWCG

Уважаемые читатели!

В этом номере журнала мы представляем разноплановые статьи, не все из которых относятся к главной теме номера «Военно-политические и глобальные риски» и посвящены проблемам управления экологическими и природными рисками, а также рисками производственной и экономической безопасности.

Открывает наш номер в рубрике «Риск военно-политический» статья сотрудников Всероссийского научно-исследовательского института по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России В. П. Малышева, В. А. Дуганова и О. В. Виноградова «Возможные направления снижения военно-стратегических рисков при угрозе применения ядерного оружия». В статье приведен анализ масштаба последствий применения ядерного оружия, а также оценка возможности использования различных мероприятий гражданской обороны для снижения военно-стратегических рисков при угрозе применения ядерного оружия. Авторами на основе проведенного анализа предложены рекомендации

для органов государственной власти и управления гражданской обороны, направленные на минимизацию военно-стратегических рисков в условиях угрозы ядерного конфликта.

В следующей статье, относящейся к главной теме в рубрике «Глобальные риски», мы разместили статью Ю. А. Крупнова и С. Н. Сильвестрова, представляющих Институт экономической политики и проблем экономической безопасности Финансового университета при Правительстве Российской Федерации «Кризисогенность глобальных рисков: факторы роста и направления антикризисной политики». В статье авторы сделали попытку показать, что особенностью развития современных глобальных рисков является рост их т.н. «кризисогенности», что связано в основном с повышением общей международной конфликтности, характеризуемой как глобальная, географически расширяющаяся, бескомпромиссная, трудноразрешимая и имеющая межцивилизационную и геополитическую основу. По мнению авторов, важными предпосылками снижения кризисогенности и успешности

купирования кризисов являются: принадлежность к союзу, сравнимому по потенциалу с противостоящим блоком стран, способность минимизировать сдерживающее влияние оппонентов и выстроить союзную систему ограниченного квазимирового хозяйства с отлаженными потоками товаров и денег, балансом спроса и предложения, системой взаимодополнения и усиления (синергии).

В статье «Риск-ориентированный подход к оценке информационно-цифровой составляющей экономической безопасности субъектов малого предпринимательства» Е. В. Караниной, А. В. Котанджян и В. Л. Коршуновым, представляющим Вятский государственный университет, рассматривается понятие информационно-цифровой составляющей экономической безопасности субъекта предпринимательства. Приводятся основные проблемы, изменение требований к организации защиты с учетом современных реалий, а также возможности идентификации основных рисков. Авторы предлагают механизм оценки уровня информационно-цифровой составляющей экономической безопасности субъекта малого предпринимательства на примере функционирующей компании.

Далее в номере размещены статьи в постоянно присутствующих в журнале рубриках производственной, экологической и природной безопасности. В первой статье «Становление и развитие метода «Анализ опасности и работоспособности» как метода анализа риска аварий» О. И. Дроняева и В. Ф. Мартынюка, представляющих РГУ нефти и газа (НИУ) имени И. М. Губкина рассмотрено становление метода «Анализ опасности и работоспособности» (АОР), который широко известен под английским наименованием «Hazard and operability studies» (HAZOP) с 1960 по 2024 гг. Авторами подчеркивается принципиальное различие задач, связанных с анализом риска аварий и анализом риска достижения целей проекта, которые объединены в канонической версии метода. По мнению авторов, это создает некоторую путаницу в использовании методических документов, созданных для решения одних задач при решении задач совсем другого направления. Продемонстрированы ограничения, возможности и перспективы метода при решении задач анализа риска аварий. Также рассмотрены возможные дополнения метода специальными инструментами или привлечение других методов анализа риска аварий.

В следующей статье «Управление экологическим воздействием нефтегазового бизнеса на атмосферный воздух (на примере деятельности ПАО «НК «РОСНЕФТЬ» за 2012–2023 годы)» О. П. Трубицина и В. Н. Башкин, представляющих Северный (Арктический) федеральный университет имени М. В. Ломоносова и Институт физико-химических и биологических проблем почвоведения РАН, соответственно, рассмотрены вопросы управления воздействием нефтегазового бизнеса на атмосферный воздух. Исследование проводилось на основе данных о валовых и удельных выбросах в атмосферу из утвержденных отчетов в области устойчивого развития компании «Роснефть». Динамика валовых выбросов вредных веществ в целом имеет тенденцию к незначительному снижению при росте показателей валовых выбросов  $SO_2$  и  $NO_x$ . В то же время динамика удельных выбросов  $SO_2$  и  $NO_x$  растет в меньшей степени. По мнению авторов, компании «Роснефть» следует повысить информационную прозрачность в области затрат на мероприятия по минимизации воздействия на атмосферный воздух и стремиться к дальнейшему повышению эффективности реализации Концепции охраны окружающей среды.

В следующей рубрике «Риск природный» размещена пятая часть статьи М. И. Ярошевича, посвященной циклонической активности тропических циклонов и некоторым ее особенностям. Автором рассчитаны многолетние годовые значения циклонической энергии тропических циклонов и годовые значения сейсмической энергии раздельно по землетрясениям нескольких диапазонов магнитуд. Расчеты проведены по обширной циклонической зоне северо-западной части Тихого океана. Автор выявил определенные корреляционные связи между многолетними динамиками годовых значений циклонической энергии и годовых значений сейсмической энергии, а также определил на этой основе характеры тенденций развития многолетних рядов годовых значений циклонической и сейсмической энергии и предложил возможный механизм возможного влияния циклонической активности на сейсмическую активность в двух разных диапазонах магнитуд.

В рубрике «Риск проектный» размещена статья В. С. Николаенко «Анализ процессов создания ИТ-продуктов в рамках выполнения ИТ-проектов», представляющего Томский государственный университет

систем управления и радиоэлектроники. В статье представлены результаты анализа международных сводов знаний управления проектами (PMBOK Guide®, ISO и др.) и национальных стандартов (ГОСТ Р ИСО/МЭК 12207, серия стандартов ИСО/МЭК 15504, ГОСТ Р ИСО 21500, семейство стандартов «Проектный менеджмент»), регламентирующих формализацию процессов создания ИТ-продуктов и процессов управления проектами, в том числе в области ИТ. Итогом проведенного автором анализа стала разработанная процессная модель создания ИТ-продуктов в рамках выполнения ИТ-проектов, включающая в себя 62 подпроцесса. В статье представлены доказательства того, что разработанная процессная модель элиминирует наступление рисков и негативных последствий, связанных с отклонением от базовых планов и существенных условий контрактов.

Завершает наш номер рубрика «Риск финансовый», в которой мы разместили статью С. Я. Криволапова, А. В. Комиссаровой и Д. А. Хамулы, представляющих

Финансовый университет при Правительстве Российской Федерации «Использование распределения Бенфорда для снижения риска необнаружения искажений финансовой отчетности». В статье рассматривается совокупность числовых массивов, каждый из которых содержит данные о финансовой отчетности некоторых компаний, изложена процедура обучения и использования для предсказания классификатора, основанного на проверке близости частот цифры первого разряда и цифры второго разряда теоретическим частотам закона Бенфорда. Результаты кластерного анализа используются для обучения классификатора на основе логистической регрессии, который в дальнейшем применяется для прогнозирования наличия (или отсутствия) искажений в финансовой отчетности, получаемой от новых компаний. Вычисления, проведенные авторами для реальных данных, содержащих сведения о финансовой отчетности компаний, показали работоспособность предложенной процедуры.



ФГБУ ВНИИ ГОЧС  
МЧС России

Журнал  
выпускается  
1 раз в 2 месяца  
в двух форматах



Подписаться на журнал

## Концепция научного журнала основывается на представлении всего спектра исследований риска

На страницах журнала публикуются статьи фундаментального и прикладного характера, как правило, междисциплинарные и многоплановые, посвященные проблемам анализа и управления рисками различного происхождения и характера

Стать автором журнала

Прием статей,  
оформленных  
в соответствии  
с инструкцией  
для авторов

Все статьи  
проходят  
рецензирование  
у одного или двух  
экспертов

Проверка  
присланных  
материалов  
на плагиат

Возможна доработка  
или переработка  
статьи  
по результатам  
рецензирования

Решение  
о публикации  
статьи

Срок рассмотрения статьи на предмет публикации в журнале

45 дней

УДК 351.862  
Научная специальность: 6.1.0  
<https://elibrary.ru/fnxwfu>

ISSN 1812-5220  
© Проблемы анализа риска, 2025

# Возможные направления снижения военно-стратегических рисков при угрозе применения ядерного оружия

**Малышев В.П.\*,  
Дуганов В.А.,  
Виноградов О.В.,**

Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (федеральный центр науки и высоких технологий), 121352, Россия, г. Москва, ул. Давыдовская, д. 7

## Аннотация

Цель: анализ масштаба последствий применения ядерного оружия, а также оценка возможности использования различных мероприятий гражданской обороны для снижения военно-стратегических рисков при угрозе применения ядерного оружия. На основе проведенного анализа выработаны рекомендации для органов государственной власти и управления гражданской обороны, направленные на минимизацию военно-стратегических рисков в условиях угрозы ядерного конфликта.

**Ключевые слова:** поражающие факторы ядерного оружия; масштаб последствий применения ядерного оружия; защищенность населения; мероприятия гражданской обороны; устойчивость функционирования; направления деятельности.

**Для цитирования:** Малышев В.П., Дуганов В.А., Виноградов О.В. Возможные направления снижения военно-стратегических рисков при угрозе применения ядерного оружия // Проблемы анализа риска. 2025. Т. 22. № 1. С. 12–23. — EDN: FNXWFU

**Авторы заявляют об отсутствии конфликта интересов**

# Possible Directions for Reducing Military-Strategic Risks in the Threat of the Use of Nuclear Weapons

Vladlen P. Malyshev\*,  
Vasily A. Duganov,  
Oleg V. Vinogradov,  
Federal State Budgetary  
Establishment «All-Russian  
Scientific Research Institute for  
Civil Defence and Emergencies  
of the EMERCOM of Russia»  
(Federal Science and High  
Technology Center),  
Davydovskaya str., 7, Moscow,  
121352, Russia

## Abstract

Purpose: analysis of the scale of the consequences of the use of nuclear weapons, as well as an assessment of the possibility of using various civil defense measures to reduce military-strategic risks in the threat of the use of nuclear weapons. Based on the analysis, recommendations were developed for state authorities and civil defense departments aimed at minimizing military-strategic risks in the face of a threat of nuclear conflict.

**Keywords:** damaging factors of nuclear weapons; the scale of the consequences of the use of nuclear weapons; protection of the population; civil defense measures; stability of functioning; areas of activity.

**For citation:** Malyshev V.P., Duganov V.A., Vinogradov O.V. Possible directions for reducing military-strategic risks in the threat of the use of nuclear weapons // Issues of Risk Analysis. 2025;22(1):12-23. (In Russ.). — EDN: FNXWFU

The authors declare no conflict of interest

## Содержание

Введение

1. Анализ масштаба последствий применения ядерного оружия
2. Мероприятия гражданской обороны, реализуемые в период холодной войны для повышения защищенности населения и устойчивости объектов и отраслей экономики в условиях угрозы применения ядерного оружия
3. Возможные направления деятельности органов государственной власти и управления гражданской обороны по снижению военно-стратегических рисков при угрозе применения ядерного оружия

Заключение

Список источников

## Введение

Безрассудная политика руководителей стран коллективного Запада по наращиванию дальнобойной огневой мощи вооруженных сил Украины для нанесения неприемлемого ущерба территориям Российской Федерации способствует ядерной эскалации и повышает вероятность возникновения вооруженного конфликта с блоком НАТО. В этом конфликте решающее значение будет иметь не только эффективное применение ядерного оружия по противоборствующей стороне, но и успешные действия по смягчению последствий апокалиптического характера от столь тяжелого военного конфликта.

В период холодной войны с западными странами наша страна уделяла большое внимание повышению защищенности населения и критически важных отраслей экономики от массированного применения ядерного оружия [1]. Был сформирован значительный фонд противорадиационных укрытий и защитных сооружений гражданской обороны, которые позволяли укрыть более 70% городских жителей. Были накоплены средства индивидуальной защиты практически на все население страны.

Особое внимание уделялось проблемам повышения устойчивости функционирования критически важных отраслей экономики от массированного применения ядерного оружия. В 1976 г. Правительство СССР возложило выполнение этой задачи на гражданскую оборону СССР. Для научного обеспечения этой задачи был создан научно-исследовательский институт гражданской обороны, носящий ныне название ВНИИ ГОЧС. В отраслевых и республиканских научно-исследовательских учреждениях были сформированы научные подразделения (секторы, лаборатории), на которые возлагались задачи по проведению научно-исследовательских работ по вопросам повышения устойчивости функционирования отраслей и регионов в военное время с целью выявления узких мест и выработки предложений по их устранению.

Этой научной кооперацией были подготовлены «Общие требования по повышению устойчивости народного хозяйства в военное время», утвержденные постановлением ЦК КПСС и Совета Министров СССР. В этом документе были изложены требования к эффективному размещению производительных сил на территории страны, к подготовке отраслей народного хозяйства и промышленности к работе в условиях

военного времени, а также к выполнению работ по восстановлению народного хозяйства в условиях военного времени и обеспечению устойчивости системы управления народным хозяйством.

В министерствах и ведомствах СССР были также разработаны отраслевые требования. В них были учтены специфические особенности соответствующих отраслей народного хозяйства. Особое внимание уделялось строительству в Сибири и на Дальнем Востоке предприятий, дублирующих продукцию военно-промышленного комплекса и других критически важных отраслей экономики. С целью повышения устойчивости транспортной инфраструктуры было начато строительство Байкало-Амурской магистрали.

Представляется целесообразным творчески переосмыслить накопленный Советским Союзом опыт в области защиты населения и критически важных секторов экономики от ядерной войны с НАТО, основываясь на принципах разумной достаточности, и использовать его для подготовки нашей страны к возможному ядерному конфликту.

## 1. Анализ масштаба последствий применения ядерного оружия

Мощность ядерного оружия определяется общим количеством высвобождаемой при взрыве энергии и характеризуется тротиловым эквивалентом, который численно равен массе такого количества тротила. При ядерном взрыве в воздухе возникает несколько поражающих факторов, основные поражающие факторы представлены в табл. 1 [2, 6].

Ударная волна ядерного взрыва — один из основных поражающих факторов. Она поражает людей, разрушает все сооружения, находящиеся в зоне воздействия. Световое излучение способно вызвать возгорание различных материалов, имущества и сооружений. У людей и животных вызывает ожоги кожи, поражение глаз и временное ослепление. Проникающая радиация, воздействуя на людей, вызывает у них лучевую болезнь. Радиоактивное загрязнение местности и объектов оказывает на людей и животных такое же поражающее действие, как и проникающая радиация. Электромагнитный импульс может повредить аппаратуру управления и связи, нарушать работу электрических устройств, подключенных к наружным линиям.

**Таблица 1. Поражающие факторы современного ядерного оружия**

Table 1. Damaging factors of modern nuclear weapons

Ядерные средства поражения	Поражающий фактор	Характеристика величины воздействия
Авиационные бомбы, крылатые ракеты морского базирования, крылатые ракеты воздушного и наземного базирования, межконтинентальные баллистические ракеты	ударная волна	избыточное давление от 0,1 до 3,0 кгс/см <sup>2</sup>
	световое излучение	световой импульс от 1 до 12 кал/см <sup>2</sup>
	проникающая радиация	доза излучения от 5 до 1000 Зв
	радиоактивное заражение местности	уровни радиации от 1 до 2500 Зв/час
	электромагнитный импульс	энергия импульса от 1 кВт до 100 МВт

По оценкам экспертов [3, 5], поражающие факторы ядерного оружия имеют следующие доли причиняемых последствий (см. рис. 1).

При анализе последствий в очаге поражения рассматривают зоны:

- полного разрушения. Избыточное давление ударной волны в ней превышает 50 кПа, а степень поражения имеет величину не менее 0,9;
- сильного разрушения. Избыточное давление ударной волны составляет 30–50 кПа, а степень поражения имеет величину не менее 0,7;
- среднего разрушения. Избыточное давление ударной волны не более 20 кПа, а степень поражения имеет величину 0,3;
- слабого разрушения. Избыточное давление ударной волны в пределах 10–20 кПа и степень поражения имеет величину не более 0,1.

Основные характеристики зон разрушения (см. табл. 2) [8].

О характере и масштабе последствий свидетельствуют результаты сброса атомных бомб на японские города Хиросима и Нагасаки [4]. На Хиросиму 6 августа 1945 г. вооруженные силы США сбросили атомную бомбу «Малыш», эквивалентную по мощности 13–18 кг тротила. Находившиеся в эпицентре взрыва люди погибли мгновенно, их тела обратились в уголь. Световое излучение оставило силуэты человеческих тел на стенах. В течение нескольких минут 90% людей, находившихся на расстоянии 800 м от эпицентра, погибли. Горючие материалы воспламенялись на расстоянии до 2 км от эпицентра. Количество погибших от воздействия ударной волны и светового излучения взрыва составило от 70 до 80 тыс. чел. К концу 1945 г. от действия радиоактивного заражения и других отложенных



Рис. 1. Доли причиняемых последствий от поражающих факторов ядерного взрыва

Figure 1. Shares of consequences caused by damaging factors of nuclear explosion

**Таблица 2. Основные характеристики зон разрушения**

Table 2. Main characteristics of destruction zones

Наименование зоны	Зона слабых разрушений	Зона средних разрушений	Зона сильных разрушений	Зона полных разрушений
Избыточное давление в зоне, кПа	10–20	20–30	30–50	60–100
Избыточное давление на внешней границе зоны, кПа	10	20	30	свыше 50
Степень разрушения строений, %	10	30	70	90
Вероятность поражения людей	0,1	0,3	0,7	0,9

эффектов взрыва общее количество погибших увеличилось примерно до 145 тыс. чел. По истечении пяти лет общее количество погибших, с учетом умерших от рака и других долгосрочных воздействий взрыва, могло достичь порядка 200 тыс. чел.

9 августа 1945 г. на город Нагасаки была сброшена атомная бомба на основе плутония, известная как «Толстяк», мощность которой составляла от 19 до 21 кт в тротиловом эквиваленте. Атомный взрыв над Нагасаки затронул район площадью примерно 110 км<sup>2</sup>, из которых 22 км<sup>2</sup> приходится на водную поверхность и 84 км<sup>2</sup> было заселено только частично. Согласно отчету префектуры Нагасаки «люди и животные погибли почти мгновенно» на расстоянии до 1 км от эпицентра. Почти все дома в радиусе 2 км были разрушены, а возгорающиеся материалы воспламенялись на расстоянии до 3 км от эпицентра. Из 52 тыс. зданий в Нагасаки 14 тыс. было разрушено полностью и еще 5,4 тыс. — серьезно повреждено. Неповрежденными осталось всего лишь 12% зданий. В городе не возникло полноценного огненного шторма, но наблюдались многочисленные локальные пожары. Количество погибших к концу 1945 г. составило порядка 80 тыс. чел. По истечении пяти лет общее количество погибших, с учетом умерших от рака и других долгосрочных воздействий взрыва, могло достичь 140 тыс. чел. [2]. Представленные данные свидетельствуют, что при применении подобных боеголовок площадь зоны полных, сильных и средних разрушений составляет порядка 25 км<sup>2</sup> и при высокой плотности населения в очаге поражения количество погибших может составить до 80 тыс. чел.

При подготовке к ядерному конфликту военно-политическое руководство США и НАТО уделяет особое внимание планированию применения тактического ядерного оружия, которое размещено в Европе. Наиболее массовым носителем тактического ядерного оружия в Европе является истребитель-бомбардировщик F-16

с радиусом действия 930 км, оснащенный авиабомбой B-61 [9]. B-61 планируется модернизировать в управляемую авиабомбу со сроком эксплуатации до 30 лет. Тактические ядерные боеголовки могут иметь тротильный эквивалент от 1 тыс. до 50 тыс. т.

Тактическое ядерное оружие США размещено в основном в Германии, а также в Бельгии, Италии, Турции и Греции. При перебазировании самолетов-носителей тактического ядерного оружия США и НАТО на передовые аэродромы Польши, Румынии и стран Балтии в зоне досягаемости оказывается вся территория Европейской части России [10]. В качестве стратегического ядерного оружия США располагает 1498 боеголовками, готовыми к применению, кроме этого Великобритания располагает 225 боеголовками, Франция имеет 290 боеголовок. Стратегический запас ядерного оружия США в основном содержит термоядерные боеприпасы.

Источником энергии в термоядерных боеприпасах является реакция термоядерного синтеза атомов дейтерия и трития, которая может протекать при температуре порядка десятков миллионов. Поэтому в качестве детонатора используется ядерный заряд на основе цепной реакции деления атомов урана-235. Эти боеголовки имеют весьма большую мощность в тротиловом эквиваленте, которая составляет от 150 до 500 кт. Радиус поражения R для зон полных и сильных разрушений в зависимости от мощности ядерного боеприпаса q может быть определен по формуле [2]:

$$R = 0,54 q^{0,33} \text{ км}, \quad (1)$$

где q — тротильный эквивалент боеприпаса в кт.

Но за три последних десятилетия ядерный клуб существенно расширился. К США, СССР, Великобритании и Франции добавились Китай, Индия, Пакистан, Израиль и Северная Корея. В настоящее время эти

**Таблица 3. Количество боеголовок ядерного оружия**

Table 3. Number of nuclear weapons warheads

Состояние	Россия	США	Франция	Китай	Англия	Пакистан	Индия	Израиль	Северная Корея
Боеголовки, готовые к пуску	1910	1800	290	270	120	0	0	0	0
Всего	7000	6800	300	295	215	140	130	80	60

страны в общей сложности обладают около 15 тыс. боеголовок. Из них США и Россия располагают 90% боеголовок. Их распределение в различных странах мира (по общему числу и по числу развернутых и готовых к пуску) показано в табл. 3.

США и Россия в случае применения всех готовых к пуску боеголовок могут создать зоны полных и сильных разрушений на территории до 300 тыс. км<sup>2</sup>. Это составляет около 2% территории России и 15% территории США.

По мнению многих военных экспертов, наиболее вероятными целями для ядерного оружия могут стать [3, 7]:

- города с населением от 1 млн чел. и выше, а также столицы республик, областные и краевые административные центры с объектами государственного управления и крупными транспортными узлами;
- объекты электроэнергетики: атомные, тепловые и гидроэлектростанции;
- критически важные предприятия оборонного комплекса и жизнеобеспечения населения.

При ограниченном применении ядерного оружия (до 500 боеголовок) для нанесения ударов по территории страны может сложиться следующая обстановка<sup>1</sup>: общие потери населения в городах, по которым наносятся удары, могут составить до 60%, в том числе: безвозвратных — до 20%, санитарных — до 40%, из них свыше 30% потребуются эвакуация в лечебные учреждения.

Возможные потери экономики могут составить:

- энергетика (потери мощностей) — до 80%;
- железнодорожный транспорт (снижение пропускной способности) — до 60%;
- автомобильный транспорт (снижение объема перевозок) — до 40%;

<sup>1</sup> Разработка методических и организационных основ по переводу гражданской обороны с мирного на военное время: Отчет о НИР «Лавина-2». 2017.

- междугородняя связь общего пользования (потери коммуникационного оборудования и каналообразующей аппаратуры) — до 70%;

- металлургическая промышленность — до 60%;
- нефтеперерабатывающая и нефтехимическая промышленности — до 70%;
- машиностроение — до 40% производственных мощностей.

Вследствие разрушения АЭС могут образоваться обширные зоны отчуждения по типу территории вокруг Чернобыльской АЭС. За счет разрушения гидродинамических объектов могут образоваться значительные площади катастрофического затопления.

Наиболее сложная обстановка прогнозируется в Москве, Санкт-Петербурге, крупных городах, включая столицы республик, краевых и областных центров, расположенных на Европейской части территории Российской Федерации.

## **2. Мероприятия гражданской обороны, реализуемые в период холодной войны для повышения защищенности населения и устойчивости объектов и отраслей экономики в условиях угрозы применения ядерного оружия**

В начале 70-х годов руководством США была взята на вооружение «концепция первого обезоруживающего удара» [7]. Наряду со стратегическими наступательными силами на передний план в качестве средств первого удара выдвигались ракеты средней дальности (1000–5500 км), размещаемые в Западной Европе. Малое подлетное время (10–12 мин.) делало их идеальным средством стремительного удара по выбранным целям. Реально возникла угроза внезапного ядерного нападения на территорию СССР. Одновременно в эти годы в США стала реформироваться гражданская оборона

с учетом национальной стратегии гарантированного выживания в ядерной войне. Сложившаяся обстановка потребовала от руководства страны принять неотложные меры по защите населения и тыловой инфраструктуры.

Условно все мероприятия по защите от ядерного оружия, которые проводились в СССР, можно свести в три группы<sup>2</sup>. В первую группу входили мероприятия, связанные с непосредственным обеспечением защиты населения от современных средств поражения противника. Они касались главным образом подготовки и реализации мероприятий в области инженерной, противорадиационной и противохимической защиты, медико-биологической и противопожарной безопасности, рассредоточения и эвакуации населения, а также инженерно-технических и организационных мер, направленных на повышение эффективности основных методов и средств защиты граждан.

Вторую группу составляли мероприятия, направленные на повышение устойчивости функционирования экономики и уменьшение возможного ущерба народному хозяйству при применении противником ядерного оружия и других средств поражения. Мероприятия предусматривали: рассредоточение производительных сил на территории страны; подготовку отраслей и объектов народного хозяйства к переводу на режим работы в условиях военного времени; дублирование производства важнейших видов продукции; защиту производственного персонала, технической документации и наиболее важных видов оборудования, сырья и готовой продукции; меры по повышению устойчивости работы транспорта, связи, энергетики, управления отраслями и объектами народного хозяйства в военных условиях; меры по повышению автономности функционирования ряда важных экономических районов страны.

В третью группу входили мероприятия по повышению готовности сил и средств гражданской обороны к действиям по ликвидации последствий нападения противника и осуществления одной из наиболее важных и первоочередных задач — проведение спасательных и неотложных аварийно-восстановительных работ в очагах поражения, а также в районах возникших бедствий. В этих целях отработывались вопросы

<sup>2</sup> Постановление ЦК КПСС и Совета Министров СССР «Об утверждении Общих требований по повышению устойчивости», 1979 г.

организации разведки очагов поражения, поиска и оказания медицинской помощи, а также спасения пораженных.

В целях защиты населения развернулось строительство защитных сооружений для укрытия рабочих и служащих объектов народного хозяйства, расположенных в крупных городах, и особо важных объектов вне этих городов<sup>3</sup>. Были разработаны типовые проекты встроенных и отдельно стоящих убежищ<sup>4</sup>. Для защиты в угрожаемый период остального населения спланировано строительство быстровозводимых убежищ и противорадиационных укрытий<sup>5</sup>. Одним из важнейших направлений накопления фонда защитных сооружений являлось задействование такого значительного резерва, как приспособление под них горных выработок и метрополитенов<sup>6</sup>.

В целях планирования эвакуации в максимально сжатые сроки широкое распространение получил комбинированный способ рассредоточения и эвакуации населения. Этот способ заключался в том, что определенные категории населения планировалось вывозить в безопасные районы всеми имеющимися видами транспорта, а для лиц, продолжающих работы, предусматривались места непосредственно в загородном размещении [1].

Практически для всего населения страны предусматривалось создание резерва средств индивидуальной защиты, устанавливалась ответственность руководителей за хранение и своевременную выдачу в случае необходимости их населению. Проводилась работа по приближению мест хранения средств индивидуальной защиты к районам массового проживания населения. Были начаты работы по подготовке загородной зоны к приему эвакуированных, развертыванию в них лечебных учреждений. Значительно активизировалась работа по созданию запасов медицинского и санитарно-хозяйственного имущества,

<sup>3</sup> Постановление Совета Министров СССР «О мерах по дальнейшему совершенствованию гражданской обороны (категоризованный город)», 1978 г.

<sup>4</sup> Директива начальника гражданской обороны СССР «О применении новых типовых проектов быстровозводимых убежищ гражданской обороны на 50 и 100 чел.», 1981 г.

<sup>5</sup> Директива начальника штаба гражданской обороны СССР «О введении современных рекомендаций по приспособлению подвальных помещений под усиленные укрытия», 1984 г.

<sup>6</sup> Постановление Совета Министров СССР «О повышении готовности метрополитенов к защите населения», 1979 г.

медикаментов и оборудования. Существенно увеличилось количество медицинских учреждений и формирований, полностью обеспеченных табельным имуществом [11].

Особое внимание уделялось повышению устойчивости функционирования отраслей и объектов народного хозяйства. Основные направления повышения устойчивости (см. рис. 2).

Для подготовки руководящего состава министерств, ведомств, республик и областей к деятельности по повышению устойчивости функционирования народного хозяйства по инициативе начальника гражданской обороны СССР был создан учебно-экспериментальный комплекс. В нем на основе использования последних достижений научно-технического прогресса области были развернуты экспозиции по вопросам устойчивости в машиностроительном и агропромышленном комплексах, на транспорте, в системах связи и органах управления гражданской обороной [1].

Высокий уровень готовности гражданской обороны СССР к защите населения и экономики страны, безусловно, оказал влияние на стратегическое противостояние двух сверхдержав и способствовал снижению риска возникновения ядерной войны. По взаимной договоренности угроза применения ракет средней дальности, размещаемых в Европе, была устранена.

Однако начавшиеся в нашей стране с середины восьмидесятых годов негативные социально-политические процессы привели к распаду социалистического лагеря, а затем и Советского Союза, что позволило руководству США считать себя победителем в холодной войне и вести переговоры с руководителями нашей страны, как с побежденными.

### 3. Возможные направления деятельности органов государственной власти и управления гражданской обороны по снижению военно-стратегических рисков при угрозе применения ядерного оружия

При подготовке тех или иных предложений по направлениям деятельности органов государственной власти целесообразно исходить из двух постулатов. Первый постулат: предложения должны способствовать росту наших преимуществ в ядерном противостоянии с Западом, которые заключаются в больших размерах территории нашей страны по сравнению со странами Запада и гораздо меньшей плотности населения. Поэтому при реализации «Стратегии территориального развития Российской Федерации» большинство крупных инфраструктурных проектов необходимо размещать на территориях Сибири и Дальнего Востока. В Европейской части территории



Рис. 2. Основные направления повышения устойчивости функционирования отраслей и объектов народного хозяйства

Figure 2. The main directions of increasing the sustainability of the functioning of industries and facilities of the national economy

страны новые промышленные объекты целесообразно размещать в малых городах. Целесообразно в городах-мегаполисах значительно сократить строительство высотных жилых домов, близко расположенных друг к другу, и стимулировать желание многих городских жителей обустроить свое жилье в сельской местности.

Второй постулат: преимущественное развитие должны получить предложения, решающие проблемы комплексной безопасности регионов в условиях мирного и военного времени. Учитывая те потери, которые несет наша страна от климатических бедствий, представляется целесообразным в рамках реализации природоохранных национальных проектов и государственных программ обеспечения комплексной безопасности государства решать проблемы устойчивого развития регионов в условиях военных и климатических угроз. Основные направления деятельности государственных органов по повышению устойчивости регионов к угрозам военного и климатического характера представлены на рис. 3.

Органы управления гражданской обороны и департаменты субъектов Российской Федерации, ответственные за обеспечение комплексной безопасности регионов, должны на основе анализа возможных сценариев военных опасностей с учетом социально-экономических и природно-климатических особенностей регионов обеспечить выполнение следующих задач:

- повышение уровня защищенности населения от современных средств поражения, включая ядерное оружие, за счет подготовки к проведению мероприятий по рассредоточению и эвакуации населения, накоплению необходимого фонда укрытий путем использования заранее подготовленных заглубленных помещений и созданию запасов технических и медицинских средств индивидуальной защиты;

- повышение устойчивости функционирования объектов жизнеобеспечения, энергетики, связи, транспортного обеспечения, организаций здравоохранения за счет повышения защищенности физической стойкости основных элементов объектов, дублирования систем энерго- и водообеспечения, резервирования важных узлов и механизмов, обеспечения надежными средствами пожаротушения, подготовки к аварийно-восстановительным работам;

- повышение готовности сил и средств гражданской обороны, а также сил единой государственной системы предупреждения и ликвидации ЧС к действиям по ликвидации последствий стихийных

бедствий и применения современного оружия за счет повышения уровня технического оснащения, совершенствования форм и способов подготовки, применения современных аварийно-спасательных технологий, широкого использования беспилотных авиационных систем и других робототехнических устройств.

По мнению ряда экспертов [5, 9], эффективное применение мероприятий по рассредоточению и эвакуации населения, накоплению необходимого фонда укрытий снижает риск поражения населения на 25–30%, использование мер повышения защищенности физической стойкости основных элементов объектов, дублирования систем энерго- и водообеспечения, резервирования важных узлов и механизмов снижает риск выхода из строя объектов на 15–20%.

Необходимо также уделить внимание вопросам:

- повышения надежности и своевременности оповещения населения за счет привлечения ресурсов операторов связи и телерадиоканалов;

- создания необходимых материально-технических запасов для жизнеобеспечения населения, оказания гуманитарной помощи и ведения аварийно-спасательных и других неотложных работ;

- подготовки руководящего состава гражданской обороны и населения к действиям в условиях применения ядерного оружия.

Для подготовки руководящего состава органов государственной власти к деятельности по повышению устойчивости функционирования отраслей экономики и регионов страны целесообразно на базе Академии гражданской защиты воссоздать учебно-демонстрационный комплекс на основе использования современных информационных и цифровых технологий.

При подготовке планов гражданской обороны предлагается использовать зональный принцип планирования, учитывающий степень и виды военных опасностей в зависимости от расположения территории субъекта Российской Федерации к границам недружественных стран. Планирование защитных мероприятий в зависимости от зонирования территорий по степени военных угроз было начато еще в 1927 г., когда Совет труда и обороны СССР (СТО) принял постановление «Об организации воздушно-химической обороны территории Союза ССР», в котором территория страны подразделялась на пограничную, угрожаемую зону

## Устойчивое развитие в условиях угроз



Рис. 3. Основные направления деятельности государственных органов по повышению устойчивости регионов к угрозам военного и климатического характера

Figure 3. The main activities of state bodies to increase the resistance of regions to military and climatic threats

и тыл. Был утвержден перечень городов, подлежащих активной противовоздушной обороне [1].

Для зонирования территорий Российской Федерации по степени и видам военных опасностей может быть использован принцип деления территорий по режимам безопасности, изложенный в Указе Президента Российской Федерации от 19.10.2022 № 756.

Для повышения уровня взаимодействия и наращивания возможностей спасательных сил целесообразно завершить процесс интеграции гражданской обороны и единой государственной системы предупреждения и ликвидации ЧС (РСЧС)<sup>7</sup>. Для этого необходимо продолжить доработку единого законопроекта «О гражданской обороне и защите населения от ЧС». Вместе с тем для успешной реализации этого законопроекта необходима масштабная консолидация основных

<sup>7</sup> Концепция интеграции единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций и гражданской обороны, ФГБУ ВНИИ ГОЧС (ФЦ), 2020 г.

подзаконных актов. В рамках выполнения такой работы в первую очередь необходимо разработать новые редакции положений о единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций и о гражданской обороне в Российской Федерации, а также осуществить консолидацию нормативных правовых актов Российской Федерации, регулирующих отношения в области РСЧС и ГО. Предложения по консолидации нормативных правовых документов (см. рис. 4).

### Заключение

Создание единых органов управления и группировки сил, единых запасов финансовых, материальных и иных средств позволит более успешно решать задачи по защите населения и территорий от крупномасштабных угроз мирного и военного характера. В целом демонстрация готовности России к защите населения и сохранению объектов, необходимых для функционирования экономики и выживания населения, от угроз



Рис. 4. Основные направления консолидации нормативных правовых документов в области гражданской обороны и РСЧС

Figure 4. The main directions of consolidation of regulatory legal documents in the field of civil defense and RSES

применения ядерного оружия, как свидетельствует опыт межгосударственного противостояния в годы холодной войны, может снизить уровень военно-стратегических рисков.

## Список источников [References]

1. Владимиров В. А., Левин С. Ф., Медведев В. А. и др. От МПВО к Гражданской защите (Исторический очерк) / под общ. ред. С. К. Шойгу. М.: УРСС. 1998. 336 с. [Vladimirov V. A., Levin S. F., Medvedev V. A. [et al.] From MAAD to Civil Protection (Historical essay) / Edited by S. K. Shoigu. M.: URSS. 1998. 336 p. (In Russ.)]
2. Обеспечение мероприятий и действий сил ликвидации чрезвычайных ситуаций: учебник в 3-х частях: Часть 2. Инженерное обеспечение мероприятий и действий сил ликвидации чрезвычайных ситуаций: в 3-х книгах: Книга 2. Оперативное прогнозирование инженерной обстановки в чрезвычайных ситуациях / Саков Г. П., Цивилев М. П., Поляков И. С. и др.; Под общей редакцией С. К. Шойгу; Факультет Гражданской обороны Военно-инженерной академии. М.: Папирус, 1998. 166 с. Provision of activities and actions of emergency response forces: textbook in 3 parts: Part 2. Engineering support of measures and actions of emergency response forces: in 3 books: Book 2. Operational forecasting of engineering situation in emergency situations / G.P. Sakov, M. P. Tsivilev, I. S. Polyakov et al.; Edited by S. K. Shoigu; Faculty of Civil Defense of the Military Engineering Academy. M.: Papyrus, 1998. 166 p. (In Russ.)]
3. Современное вооружение в войне / Панов В. В., Гайкалов В. И., Голобородов А. Ф. [и др.]; ред. Панов В. В., Прядилов С. М.; Российская академия ракетных и артиллерийских наук, Российская инженерная академия, Секция «Военно-технических проблем. М.: Вооружение. Политика. Конверсия, 1994. 284 с. [Modern weapons in the war / Panov V. V., Gaikalov V. I., Goloborodov A. F. [et al.]; ed. Panov V. V., Pryadilov S. M.; Russian Academy of Missile and Artillery Sciences, Russian Academy of Engineering, Section “Military-technical problems. — M.: Armament. Politics. Conversion, 1994. 284 p. (In Russ.)]
4. Александров И. Атомная бомбардировка Хиросимы и Нагасаки // Военно-исторический журнал. 1962. № 4.

- C. 60–69 [Alexandrov I. Atomic bombing of Hiroshima and Nagasaki // *Military History Journal*. 1962;(4):60–69. (In Russ.)]
5. Андриевский А. И., Андриевский И. А. Оценка военного значения стационарных объектов, расположенных на территории зарубежных стран: монограф. М: Граница. 2018. 288 с. [Andrievsky A. I., Andrievsky I. A. Assessment of the military significance of stationary objects located in foreign countries: monograph. M: Granica. 2018. 288 p. (In Russ.)]
  6. Гражданская оборона: учебник / Под общ. ред. В. А. Пучкова. М.: МЧС России, 2015. 360 с. [Civil defense: textbook / Under the general. ed. V. A. Puchkov. M.: EMERCOM of Russia, 2015. 360 p. (In Russ.)]
  7. Бобылов Ю. Л. Опасность тайной агрессии // Независимое военное обозрение. 2007. № 12 [Bobylov Yu. L. Danger of secret aggression // *Independent military review*. 2007. № 12. (In Russ.)]
  8. Научно-методический труд по планированию и ведению гражданской обороны в федеральных органах исполнительной власти и организациях / МЧС России. М.: ФГБУ ВНИИ ГОЧС (ФЦ). 2017. 164 с. [Scientific and methodological work on planning and conducting civil defense in federal executive bodies and organizations / EMERCOM of Russia. M.: FSBI VNIIGOCHS (FC). 2017. 164 p. (In Russ.)]
  9. Долгин Н. Н. Особенности ведения гражданской обороны в современных условиях / сборник материалов ЦСИ ГЗ МЧС России, 2012. № 7 [Dolgin N. N. Features of civil defense in modern conditions / collection of materials from the Central Research Center of the State Ministry for Emergencies of Russia, 2012. № 7. (In Russ.)]
  10. Основы организации и ведения гражданской обороны в современных условиях / Ю. Л. Воробьев, В. А. Акимов, В. А. Владимиров [и др.]; Под общей редакцией С. К. Шойгу. М.: «Деловой экспресс», 2005. 520 с. ISBN 5-89644-086-3 [Fundamentals of the organization and conduct of civil defense in modern conditions / Yu. L. Vorobyov, V. A. Akimov, V. A. Vladimirov [et al.]; Edited by S. K. Shoigu. M.: “Business Express,” 2005. 520 p. ISBN 5-89644-086-3. (In Russ.)]
  12. Маргулис У. Я. Радиация и защита. М.: Энергоатомиздат. 1999 [Margulis U. Ya. Radiation and protection. Moscow: Energoatomizdat. 1999. (In Russ.)]

## Сведения об авторах

**Малышев Владлен Платонович:** доктор химических наук, профессор, заслуженный деятель науки Российской Федерации, главный научный сотрудник ФГБУ «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (федеральный центр науки и высоких технологий)

Количество публикаций: более 320

Область научных интересов: проблемы обеспечения безопасности в чрезвычайных ситуациях

SPIN-код: 2163–3798

*Контактная информация:*

Адрес: 121352, г. Москва, ул. Давыдовская, д. 7

Vlad1936.malyshev@yandex.ru

**Дуганов Василий Александрович:** кандидат технических наук, начальник 2 научно-исследовательского центра ФГБУ «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (федеральный центр науки и высоких технологий)

Количество публикаций: более 40

Область научных интересов: проблемы обеспечения безопасности в чрезвычайных ситуациях

SPIN-код: 4632–9376

*Контактная информация:*

Адрес: 121352, г. Москва, ул. Давыдовская, д. 7

duganov@vniigochs.ru

**Виноградов Олег Владимирович:** кандидат технических наук, ведущий научный сотрудник научно-исследовательского центра ФГБУ «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (федеральный центр науки и высоких технологий)

Количество публикаций: более 40

Область научных интересов: проблемы обеспечения безопасности в чрезвычайных ситуациях

SPIN-код: 3056-0611

*Контактная информация:*

Адрес: 121352, г. Москва, ул. Давыдовская, д. 7

v1970ov@mail.ru

Статья поступила в редакцию: 16.10.2024

Одобрена после рецензирования: 18.11.2024

Принята к публикации: 02.12.2024

Дата публикации: 28.02.2025

*The article was submitted: 16.10.2024*

*Approved after reviewing: 18.11.2024*

*Accepted for publication: 02.12.2024*

*Date of publication: 28.02.2025*

УДК 332.025  
Научная специальность: 5.2.3  
<https://elibrary.ru/frbtzn>

ISSN 1812-5220  
© Проблемы анализа риска, 2025

# Кризисогенность глобальных рисков: факторы роста и направления антикризисной политики<sup>1</sup>

**Крупнов Ю.А.\*,  
Сильвестров С.Н.,**  
Финансовый университет  
при Правительстве Российской  
Федерации, Институт  
экономической политики  
и проблем экономической  
безопасности,  
125993, Россия, г. Москва,  
Ленинградский проспект,  
д. 49/2

## Аннотация

**Цель.** Рассмотрена проблема эскалации глобальных рисков и повышения уровня их кризисогенности. Проведен анализ факторов кризисогенности и разработаны предложения по направлениям антикризисной политики.

**Методы.** Совокупность глобальных рисков рассматривается в соответствии с постулатами общей теории риска, как управляемого и постоянно действующего атрибута жизнедеятельности человечества. С использованием формально-логического метода разработаны направления антикризисной деятельности.

**Результаты.** Авторами показано, что особенностью развития современных глобальных рисков является рост их кризисогенности. Основным фактором роста является повышение общей международной конфликтности, характеризуемой как глобальная, географически расширяющаяся, бескомпромиссная, трудноразрешимая и имеющая межцивилизационную и геополитическую основу. Региональная специфичность проявления кризисогенности состоит в том, что неизбежные и всеобщие риски не генерируют всеобщие и равноглубокие кризисы, неся одним странам и союзам растущий ущерб, а другим — наилучшие возможности. Установлено, что материализация кризисогенности в реальные разрушительные кризисы во многом зависит от силы или слабости национальных и союзных экономик. Основными направлениями антикризисной политики в отдельных странах и союзах являются повышение способности противостоять санкционному сдерживанию собственного развития и уровня обеспеченности финансовым и человеческим капиталом, а также усиление контроля над потоками материальных и нематериальных ресурсов.

**Заключение.** Важными предпосылками снижения кризисогенности и успешности купирования кризисов являются: принадлежность к союзу, сравнимому по потенциалу с противостоящим блоком стран, способность минимизировать сдерживающее влияние оппонентов и выстроить союзную систему ограниченного квазимирового хозяйства с отлаженными потоками товаров и денег, балансом спроса и предложения, системой взаимодополнения и усиления (синергии).

**Ключевые слова:** геополитическая конфликтность; глобальные риски; кризисогенность; факторы кризисогенности; кризисы; антикризисная политика.

**Для цитирования:** Крупнов Ю.А., Сильвестров С.Н. Кризисогенность глобальных рисков: факторы роста и направления антикризисной политики // Проблемы анализа риска. 2025. Т. 22. № 1. С. 24–33. — EDN: FRBTZN

Авторы заявляют об отсутствии конфликта интересов

<sup>1</sup> Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансового университета при Правительстве РФ.

# Crisis Genesis of Global Risks: Growth Factors and Directions of Anti-Crisis Policy<sup>2</sup>

Yuriy A. Krupnov\*,  
Sergei N. Sil'vestrov,  
Financial University under the  
Government of the Russian  
Federation, Institute of  
Economic Policy and Economic  
Security Problems,  
Leningradsky av., 49/2, Moscow,  
125993, Russia

## Abstract

**Objectives.** The problem of escalation of global risks and increase of their crisis level is considered. The aim of the work is to analyze crisis factors and develop proposals on directions of anti-crisis policy.

**Methods.** The totality of global risks is considered in accordance with the postulates of the general theory of risk, as a controlled and constantly acting attribute of human life. Using the formal-logical method, the directions of anti-crisis activities have been developed.

**Results.** The authors show that the peculiarity of the development of modern global risks is the growth of their crisis potential. The main growth factor is the increase in general international conflict, characterized as global, geographically expanding, uncompromising, difficult to resolve and having an intercivilizational and geopolitical basis. The regional specificity of the manifestation of crisis potential is that inevitable and general risks do not generate general and equally deep crises, bringing growing damage to some countries and unions, and the best opportunities to others. The authors found that the materialization of crisis potential in real destructive crises largely depends on the strength or weakness of national and union economies. The main directions of anti-crisis policy in individual countries and unions are increasing the ability to withstand sanctions restraint of their own development and the level of provision with financial and human capital, as well as strengthening control over the flows of material and intangible resources.

**Conclusion.** An important prerequisite for reducing the crisis potential and successfully managing crises is belonging to a union comparable in potential to opposing blocs of countries, the ability to minimize the restraining influence of opponents and build a union system of a limited quasi-global economy with well-established flows of goods and money, a balance of supply and demand, and a system of mutual complementarity and reinforcement (synergy).

**Keywords:** geopolitical conflict; global risks; crisis potential; crisis factors; crises; anti-crisis policy.

**For citation:** Krupnov Yu.A., Sil'vestrov S.N. Crisis genesis of global risks: growth factors and directions of anti-crisis policy // *Issues of Risk Analysis*. 2025;22(1):24-33. (In Russ.). — EDN: FRBTZN

**The authors declare no conflict of interest**

## Содержание

Введение

1. Глобальные риски и предпосылки их эскалации
2. Глобальные риски как абсолютная нормальность
3. Когда риски перестают быть абсолютной нормальностью
4. Кризисогенность глобальных рисков
5. Неизбежные и всеобщие риски не генерируют всеобщие и равноглубокие кризисы

Заключение

Список источников

<sup>2</sup> The article rests on the results of studies funded through the budget, as part of the State job to the Financial University under the Government of the Russian Federation.

## Введение

Мир вступил в новую эпоху, когда изменяются весь глобальный порядок и совокупность вызовов социально-экономическому развитию и безопасности стран и регионов. Он становится все менее мирным, с более жестокими внешними столкновениями и интенсивными внутренними конфликтами [1, с. 11–12]. Глобальные риски накладываются на внутренние вызовы, обусловленные эскалацией украинского кризиса и ограничением доступа российских компаний на финансовый, технологический и другие рынки. Проблема состоит в том, что острота рисков усугубляется растущим недоверием и подозрительностью между мировыми и региональными державами, конфликтующими странами и союзами. Утрачиваются международное единство и способность сообща отвечать на вызовы. Национальные и блоковые эгоистические интересы берут верх над глобальными. Глобальные риски перестают быть привычной нормальностью, становясь все более кризисогенными. Это требует переосмысления традиционной антикризисной политики, включая антикризисные стратегии и инструменты. Проблема рассматривается применительно к «верхнему уровню управления структурно сложными системами», объектами которого являются государства и их союзы, важнейшие аспекты социально-экономического развития в странах и регионах [2, с. 65].

Целью работы является анализ факторов кризисогенности и разработка предложений по направлениям антикризисной политики. Последовательно рассматриваются совокупность глобальных рисков и положения общей теории риска, как управляемого и постоянно действующего атрибута жизнедеятельности человечества. Выявляются факторы повышения кризисогенности рисков, обосновывается тезис о том, что в современном мире они, возможно, перестают быть абсолютной нормальностью. Ненормальность обусловлена коренными изменениями в международных подходах к управлению рисками и предотвращению их перерастания в разрушительные кризисы. С использованием формально-логического метода разработаны направления политики по снижению уровня кризисогенности в отдельных странах и союзах.

## 1. Глобальные риски и предпосылки их эскалации

Рассмотрим, что включают актуальные и прогнозируемые глобальные риски. Под глобальными рисками обычно понимаются события или состояния, которые при наступлении (возникновении) могут привести к значимым негативным последствиям для человечества, нескольких стран или отраслей [3, с. 36]. Глобальные риски выявляются и оцениваются в пяти основных группах: экономическая, социальная, природная, технологическая и геополитическая. Считается, что на временном горизонте до двух лет негативные события, представляющие критическую угрозу, могут быть идентифицированы с наибольшей вероятностью. По данным экспертов Всемирного экономического форума, в период до 2025 г. преобладают социальные и экологические риски, обусловленные основными геополитическими и геоэкономическими тенденциями (см. табл. 1).

Как видно из таблицы, глобальные риски, оцениваемые и прогнозируемые на разных временных горизонтах, не имеют существенных различий и обусловлены преимущественно «вечными» проблемами в сфере климата, окружающей среды, энергетики, продовольствия и уровня жизни. Сравнение представленных рисков с вызовами прошлого десятилетия не позволило, за небольшими исключениями, выявить значимых различий. При этом радикально изменились комментарии экспертов ВЭФ (см. табл. 1), согласно которым риски усугубляются под влиянием войны в Европе (СВО), санкций, эскалации гонки вооружений, геополитического противостояния, роста общей нестабильности, недоверия и подозрительности в отношениях между мировыми и региональными державами, ужесточения внешних и внутренних конфликтов.

## 2. Глобальные риски как абсолютная нормальность

Несмотря на остроту международной конфликтности, анализ и оценка вероятных неблагоприятных последствий осуществляются в рамках общей теории риска, которая рассматривает их как нормальный, управляемый и постоянно действующий атрибут жизнедеятельности человечества [4, с. 56]. Согласно Н. Луману, любое управленческое решение несет в себе потенциальные

риски (поведенческий подход). Поэтому в обществе не может существовать деятельности, независимой от риска, который «является обратной стороной нормальной формы существования общества» [5]. Любые перемены, особенно в сфере технологического развития, происходящие в мире и обществе, несут предпосылки эскалации рисков (постмодернистский подход) [6]. Глобализация, модернизация производства и общества, а также индустриализация войн являются причинами возникновения рисков [7]. Люди и общества давно воспринимают риск как диалектику опасности и прибыли, как перст судьбы, повороты которой невозможно контролировать (перцептивистский подход) [8, с. 48].

В целом, глобальные риски неизбежны и всеобщы, а также непосредственно связаны с кризисами, которые являются их характерными проявлениями и результатами [9, с. 48]. Кризис является результатом воздействия многих рисков, равно как и пренебрежения ими [10, с. 10]. Это позволяет говорить о кризисогенности глобальных рисков. Влияние, которое они оказывают, носит обычно долгосрочный и устойчивый

характер. Под воздействием складывающейся глобальной конъюнктуры параметры отдельных рисков (вероятность наступления нежелательных последствий и прогнозируемый ущерб) могут меняться, что подтверждается систематически проводимым ранжированием и приоритизацией угроз [11, с. 913–922].

Оценка вышеуказанных параметров в различных странах может не совпадать, так как один и тот же риск оказывает неодинаковое по силе воздействие на возможность достижения национальных интересов в отдельных странах и регионах [12, с. 18–23]. Например, обеспечение населения питьевой водой лишь в некоторых странах является фактором национальной безопасности. Подавляющая часть рисков затрагивает отдельную сферу жизнедеятельности человечества: экономику, политику, социальную сферу, экологию и пр. Отдельные страны пытаются манипулировать реальными и надуманными рисками, фокусируя внимание мирового сообщества на отдельных проблемах и рисках, которые носят национальный характер и не в полной мере соответствуют статусу «глобальные».

**Таблица 1. Основные глобальные риски по версии ВЭФ<sup>3</sup>**

*Table 1. Main global risks according to the WEF*

Период оценки и прогнозов	Основные риски	Комментарий экспертов ВЭФ
2023 г.	1. Кризис энергоснабжения. 2. Рост стоимости жизни. 3. Рост инфляции. 4. Продовольственный кризис. 5. Кибератаки на критически важную инфраструктуру	Риски усугубляются: войной в Европе и санкциями; эскалацией гонки технологических вооружений; промышленной конкуренцией и усилением государственного вмешательства
До 2025 г.	1. Долговой кризис. 2. Неспособность стабилизировать цены. 3. Неспособность смягчить последствия изменения климата. 4. Неспособность адаптироваться к изменению климата. 5. Широкое распространение киберпреступности	Преобладают социальные и экологические риски, обусловленные основными геополитическими и экономическими тенденциями. Более половины экспертов ожидает наступления переломных моментов и постоянных кризисов, ведущих к катастрофическим последствиям в течение следующих десяти лет или постоянной нестабильности. Война на Украине ускоряет эпохальные изменения в мировом порядке
До 2033 г.	1. Неспособность смягчить последствия изменения климата. 2. Неспособность адаптироваться к изменению климата. 3. Стихийные бедствия и экстремальные погодные явления. 4. Утрата биоразнообразия и коллапс экосистемы. 5. Крупномасштабная вынужденная миграция; эрозия социальной сплоченности и социальная поляризация.	Растущее недоверие и подозрительность между мировыми и региональными державами уже привели к изменению приоритетов военных расходов и стагнации механизмов нераспространения. Распространение экономической, технологической и военной мощи среди множества стран и субъектов станет движущей силой глобальной гонки вооружений, грозящей ростом конфликтности

Источник: составлено авторами по материалам ВЭФ

<sup>3</sup> The Global Risks Report 2023 18th Edition. World Economic Forum; 2023 [протитировано 02 августа 2024 г.] // URL: [https://www3.weforum.org/docs/WEF\\_Global\\_Risks\\_Report\\_2023.pdf](https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf)

Другими словами, наличие и эволюцию совокупности глобальных рисков следует рассматривать как абсолютную нормальность. Человечество создало необходимые международные (ООН и пр.) и национальные (советы безопасности, системы стратегирования и пр.) институты и постоянно совершенствует политику снижения рисков и адаптации к ним. За многие годы антикризисная деятельность, подкрепленная научными разработками в риск-менеджменте и опирающаяся на международное единство в подходах к основным угрозам (например, угроза пандемии или мирового ядерного конфликта), превратилась в настоящую рутину и банальность. Более того, человечество научилось предвидеть зарождение и эскалацию рисков, а также предотвращать или минимизировать ущерб благодаря функционированию международных и национальных систем стратегирования и стратегического планирования.

### 3. Когда риски перестают быть абсолютной нормальностью

Между тем, в истории человечества неоднократно происходили мировые войны и другие кризисы, несущие реальную витальную угрозу его существованию. Это случалось потому, что в критические моменты истории мир утрачивал единство, а национальные и блоковые эгоистические интересы брали верх над глобальными. Так было накануне Второй мировой войны, когда риски нарастали стремительно, но в рамках системы стратегирования не были своевременно идентифицированы. В частности, даже после открытого проявления диктатуры Гитлера (путч Рема, еврейские погромы) Великобритания отстаивала идею «равновесия сил» и пакта четырех держав, включая Германию и исключая СССР [13, с. 25].

Отсутствует вышеуказанное международное единство и в современном глобальном риск-менеджменте. Страны Запада стремятся сохранить свою гегемонию и осуществляют действия, направленные на сдерживание развития новых глобальных и региональных конкурентов. Расшатываются общепризнанные нормы и принципы международного права, разрушаются международные правовые институты. Растут геополитическая нестабильность и конфликтность. Межгосударственные противоречия достигли крайне высокого уровня и сопровождаются повышением угрозы широкомасштабного применения

военной силы<sup>4</sup>. Россия, поддерживаемая большинством человечества, втянута в крупный военный конфликт, где на стороне Украины в той или иной форме и степени участвуют едва ли не все страны коллективного Запада.

Следовательно, доминантой и катализатором глобальных рисков стали именно межгосударственные конфликты с потенциалом перерастания в прямое столкновение крупных стран и союзов (блоков). Отстаивая ускользающее доминирование, страны Запада делают ставку на обострение противостояния, используя для достижения собственных целей все имеющиеся силы и средства, включая фашистские и террористические режимы и группировки. Пребывая в состоянии разобщенности и противоборства, страны — лидеры мирового развития и мировое сообщество в целом в значительной степени утратили способность предотвращать и купировать кризисы. Риски перестали быть абсолютными нормальностями.

В целом наибольшую угрозу для России и всего человечества несет набирающий силу системный международный конфликт между Россией, поддерживаемой ее сторонниками в борьбе за установление нового миропорядка, и блоком стран коллективного Запада. В этом состоят определяющие конфликт межгосударственные противоречия и риски, которые демонстрируют состояние крайнего обострения, когда недобросовестные участники конфликта предпринимают открытые действия по достижению своих интересов, используя при этом все доступные средства, включая разжигание вооруженных конфликтов, саботаж, терроризм, гибридные действия в поддержку одной из сторон. Риски международной конфронтации фактически материализовались и требуют перехода к оперативному стратегическому управлению в рамках системы стратегирования.

### 4. Кризисогенность глобальных рисков

Современное состояние международных отношений, когда противостояние сторон сопряжено с угрозой его перерастания в вооруженную борьбу, характеризуется терминологической категорией «международный

<sup>4</sup> Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». Гарант; 2021; [процитировано 12.08.2024] Доступно: <https://base.garant.ru/401425792/?ysclid=m12hhquybd983498878>

**Таблица 2. Идентификация текущего международного кризиса**

Table 2. Identification of the current international crisis

№ п/п	Критерий идентификации	Характеристика кризиса
1	Количество участников	Эволюция от двустороннего к многостороннему и мировому кризису
2	Географическое распространение	Эволюция от регионального к глобальному кризису
3	Время протекания	Длительный и потенциально затяжной кризис
4	Характер используемых средств	Эволюция от гибридных к военным средствам и, возможно, неконвенциональным средствам
5	Характер причин	Цивилизационная, геополитическая, территориальная, обеспечение равной безопасности и пр.
6	Возможность урегулирования	Эволюция от конфликта с ненулевой суммой к конфликту с нулевой суммой

Источник: составлено авторами.

кризис». Выполним его идентификацию с использованием системы критериев (табл. 2).

Как видно из таблицы, текущий кризис, являясь проявлением вышеуказанных рисков, характеризуется как глобальный, географически расширяющийся, бескомпромиссный, глубинный и трудноразрешимый, так как обусловлен международным конфликтом, имеющим межцивилизационную и геополитическую основы. По своему масштабу он охватывает отношения между крупнейшими мировыми державами и имеет потенциал разрешения в пользу одной или нескольких сторон, перерастания в военные действия либо перехода в латентное состояние.

Противостояние сторон характеризуется бескомпромиссной жесточенностью при отстаивании интересов, ценностей и образа жизни. Украина, как непосредственный участник вооруженного конфликта, демонстрирует неосмотрительную решимость в борьбе со значительно более сильным противником, полагаясь на почти неограниченную поддержку стоящей за ней гигантской западной цивилизационной общности. Она гарантирует солидарность и стимулирует решимость участников борьбы. Между тем, достижение полной и безоговорочной победы одной из сторон конфликта представляется труднодостижимым.

Следовательно, витальные глобальные риски предопределили эскалацию международного кризиса, который имеет экономический, военный, международно-дипломатический и другие срезы. Речь идет о «всеобъемлющей совокупности углубляющихся кризисов: локально страновых, региональных, субрегиональных, транснациональных, глобально международных» [14, с. 5–6].

## 5. Неизбежные и всеобщие риски не генерируют всеобщие и равноглубокие кризисы

Действительно, риски в сфере международных отношений означают, что имеется вероятность возникновения и разрастания конфликта и связанного с этим ущерба его сторонам. Однако, согласно теории рисков, риск может материализоваться не только в ущерб, но и в новые возможности. Наиболее существенный ущерб обычно несет слабая сторона, а наилучшие возможности открываются перед превосходящим участником конфликта.

Стремительно растущие международные геополитические риски проецируются на Российскую Федерацию и другие страны и в силу своей кризисогенности создают предпосылки для развития кризисных процессов в сферах производства, торговли, финансов и технологий. Неизбежные и всеобщие риски в сфере международных отношений не генерируют всеобщие и равноглубокие кризисы внутри конфликтующих стран и их союзов. По меткому заключению Л. М. Григорьева: «все страны во время экономических подъемов счастливы почти одинаково, но в ходе кризисов страдают по-разному» [15, с. 5].

Природа и глубина этих кризисов в разных странах существенно различаются. Так, Россия испытывает беспрецедентное прокризисное санкционное давление. Отечественная экономика столкнулась со снижением объема военного, энергетического и сырьевого экспорта. Обострился дефицит квалифицированной рабочей силы. Затруднены международные расчеты и существенно осложнен доступ к современным технологиям и высокотехнологичной продукции. В Китае

не удастся решить проблему снижения темпов экономического роста [16, с. 89]. В Германии отмечается деиндустриализация, крепнет тенденция свертывания производства и банкротства среди компаний энергоемких отраслей [17, с. 70]. Многие страны Запада переживают рецессию [15, с. 6–7], непривычно высокий уровень инфляции и дефицита бюджетов [18, с. 813].

Ввиду становления мировой многополярности национальные власти выстраивают антикризисную политику с учетом окружения и опорой на страны-союзники. Анализ протекания кризисных явлений в большом числе стран [19, с. 45] позволил выявить следующую закономерность: материализация кризисогенности глобальных вызовов в реальные разрушительные кризисы зависит от силы или слабости национальных и союзных экономик, а также от их способности преуспеть в реализации антикризисной политики на следующих основных направлениях.

*Сдерживание и подавление конкурентов.* Основными современными инструментами сдерживания являются военные потенциалы — в оборонной сфере и санкции — в сфере социально-экономического развития. Наиболее показательным примером их использования является сдерживание развития Российской Федерации. Приоритетными целями санкционных запретов стали ограничения экспорта и импорта, повышение издержек в производстве и торговле. Неоднозначность этого инструмента состоит в том, что ввиду взаимосвязанности мирохозяйственных процессов косвенный и вторичный ущерб от ограничений распространяется едва ли не на всех участников этих процессов, включая страны — инициаторы санкций. Еще одной характерной чертой политики сдерживания является эффект затухания сдерживающего влияния, обусловленный развитием адаптационных процессов в подсанкционной стране. Этот эффект проявляется тем отчетливее, чем крупнее подсанкционное национальное хозяйство и выше его доля в мировых и региональных производстве и торговле. Особую важность также имеют ресурсная обеспеченность, готовность проводить активную антисанкционную политику и поддержка дружественных стран.

Российская Федерация в полной мере соответствует вышеуказанным критериям устойчивости к санкционному сдерживанию. Это обусловлено «рациональной антисанкционной и антикризисной политикой», которая характеризуется как «прагматичная, оборонительная и протекционистская» [20, с. 359].

*Привлечение финансового капитала.* Перед лицом растущих глобальных вызовов страны и корпоративные структуры обычно сталкиваются с острой нехваткой финансового капитала. Важным источником финансового капитала являются прямые иностранные инвестиции в финансовый сектор [21, с. 2], которые в условиях эскалации глобальных кризисогенных рисков существенно сокращаются. Одновременно увеличивается потребность в финансах со стороны национальных кредитно-денежных систем, которые решают задачи поддержания стабильности денежного обращения и устойчивости национальной валюты на фоне ускорения перетока международного финансового капитала по направлениям к центрам эмиссии. Дефицит денежных средств делает труднодостижимым экономический рост, замедляет социально-экономическое развитие в целом и тем самым создает предпосылки для развития экономического и финансового кризиса.

*Привлечение человеческого капитала.* В соответствии с постулатами современной теории мобильности [22] значение индивидуальной мобильности все более отчетливо превосходит роль массовых миграционных потоков. Превосходство проявляется не в численности перемещающихся субъектов, а в креативности перемещающихся лиц «креативного класса», вклад которого становится определяющим [23]. Поэтому важными антикризисными факторами становятся доля креативно мыслящих новаторов, а также общая численность населения страны или союза. Уже сегодня на периферии воспроизводственного процесса оказалась трудовая миграция, а на первый план уверенно выходит научная, академическая и технологическая мобильность. Антикризисный потенциал в значительной мере обусловлен человеческим капиталом, который консолидируется в локациях с наилучшими возможностями реализации своего потенциала — центрах привлекательности человеческого капитала [24, с. 43–45].

*Контроль над потоками материальных ресурсов.* Одним из важных условий успешной адаптации к глобальным рискам является удержание контроля над потоками традиционного импорта и экспорта, включая цены на важнейшие виды товарной продукции и платежный баланс текущих операций в целом. Традиционными условиями успешной адаптации являются оптимизация времени движения товаров, минимизация затрат на формирование товарных потоков и повышение качества удовлетворения

спроса. Желательно сохранить и укрепить влияние национальных поставщиков на возможность поддержания глобального товарного предложения на уровне, обеспечивающем прибыльность экспортеров и баланс интересов национальных и иностранных производителей. В условиях санкционного блокирования традиционных направлений товарных потоков антикризисная политика развития должна включать разработку новых логистических каналов товародвижения и «интеграцию региональных логистических каналов в международную транспортно-логистическую систему» [25, с. 172].

## Заключение

Исследование показало, что глобальные риски, оцениваемые и прогнозируемые на разных временных горизонтах, не претерпевают существенных изменений и обусловлены преимущественно «вечными» проблемами в сфере климата и окружающей среды, энергетики, продовольствия и уровня жизни. Согласно постулатам общей теории риска вышеуказанные «вечные» проблемы имеют неизбежный и всеобщий характер. Поэтому их следует рассматривать как абсолютную нормальность, то есть нормальный, управляемый и постоянно действующий атрибут жизнедеятельности человечества. Кризисогенность рисков долго оставалась на приемлемом умеренном уровне благодаря тому, что человечество научилось предвидеть их зарождение и эскалацию, а также минимизировать ущерб благодаря функционированию международных и национальных систем стратегирования.

Современным катализатором глобальных рисков стали межгосударственные конфликты с потенциалом перерастания в прямое столкновение крупных стран и союзов (блоков). Основным фактором роста кризисогенности является повышение общей международной конфликтности, характеризующейся как глобальная, географически расширяющаяся, бескомпромиссная, трудноразрешимая и имеющая межцивилизационную и геополитическую основу. Пребывая в состоянии разобщенности и противоборства, страны — лидеры мирового развития в значительной степени утратили способность предотвращать и локализовать кризисы. Риски перестали быть абсолютными нормальностями.

Выявлена региональная специфичность проявления кризисогенности, которая состоит в том, что неизбежные и всеобщие риски не генерируют всеобщие и равноглубокие кризисы, неся одним странам

и союзам растущий ущерб, а другим — наилучшие возможности. Материализация кризисогенности глобальных вызовов в реальные разрушительные кризисы во многом зависит от факторов силы или слабости национальных и союзных экономик, способности стран проводить адекватную антикризисную политику, предусматривающую активное противостояние агрессивным мерам сдерживания собственного развития, повышение обеспеченности финансовым и человеческим капиталом, а также сохранение контроля над потоками материальных и нематериальных ресурсов.

В целом, важными предпосылками снижения кризисогенности и успешности купирования кризисов являются: принадлежность к союзу, сравнимому по потенциалу с противодействующими блоками стран, способность минимизировать сдерживающее влияние оппонентов и выстроить союзную систему ограниченного квазимирового хозяйства с отлаженными потоками товаров и денег, балансом спроса и предложения, системой взаимодополнения и усиления (синергии).

## Список источников [References]

1. Соколов Ю.И. Риски стратегического планирования в России // Проблемы анализа риска. 2019. Т. 16. № 6. С. 10–25  
<https://doi.org/10.32686/1812-5220-2019-16-6-10-25>  
[Sokolov Yu.I. Risks of strategic planning in Russia // Issues of Risk Analysis. 2019;16(6):10-25. (In Russ.)  
<https://doi.org/10.32686/1812-5220-2019-16-6-10-25>]
2. Соложенцев Е.Д., Карасева Е.И. Верхний уровень управления социально-экономическими системами // Проблемы анализа риска. 2017. Т. 14. № 1. С. 64–73  
<https://doi.org/10.32686/1812-5220-2017-14-1-64-73>  
[Solozhentsev E.D., Karaseva E.I. Top level of management of socioeconomic systems // Issues of Risk Analysis. 2017;14(1):64-73. (In Russ.)  
<https://doi.org/10.32686/1812-5220-2017-14-1-64-73>]
3. Манахова И.В., Кудайкулов М.К. Глобальные риски и технологическая безопасность ЕАЭС // Вестник Кыргызско-Российского Славянского университета. 2022. Т. 22. № 11. С. 34–42  
<https://doi.org/10.36979/1694-500X-2022-22-11-34-42>  
[Manakhova I.V., Kudaikulov M.K. Global risks and technological security of the EAEU] // Vestnik Kyrgyzsko-Rossiiskogo Slavyanskogo universiteta. 2022; 22(11):34-42. (In Russ.)  
<https://doi.org/10.36979/1694-500X-2022-22-11-34-42>]
4. Орлов А.И., Пугач О.В. Подходы к общей теории риска // Управление большими системами: сборник

- трудов. 2012. № 40. С. 49-82 [Orlov A.I., Pugach O.V. Approaches to the general theory of risk // Large-Scale Systems Control. 2012;(40):49-82. (In Russ.)]
5. Luhmann N. Soziologie des risikos. Berlin; New York: Walter de Gruyter. 1991. 252 p.
6. Beck U. Risikogesellschaft auf dem weg in eine andere moderne. Frankfurt: Suhrkarnp. 1986. 391 p.
7. Giddens A. Runaway World. How globalization is reshaping our lives. New York: Routledge. 2000. 124 p.
8. Vildavski A., Dake K. Theories of risk perception: who fears what and why. Risk // Dædalus. 1990;119(4):41-60
9. Акимов В.А., Порфирьев Б.Н. Кризисы и риск: к вопросу взаимосвязи категорий // Проблемы анализа риска. 2004. Т. 1. № 1. С. 38–49 [Akimov V.A., Porfiriyev B.N. Crises and risk: on the issue of the concepts' interrelationship // Issues of Risk Analysis. 2004;1(1):38-49. (In Russ.)]
10. Яницкий О.Н. Социология риска: ключевые идеи // Мир России. Социология. Этнология. 2003. Т. 12. № 1. С. 3–35 [Yanitsky O.N. Sociology of risk: key ideas // Universe of Russia. Sociology. Ethnology. 2003;12(1):3-35. (In Russ.)]
11. Крупнов Ю.А. Ранжирование основных угроз национальной безопасности Российской Федерации // Национальные интересы: приоритеты и безопасность. 2022. Т. 18. № 10(415). С. 1905–1939. <https://doi.org/10.24891/ni.18.10.1905> [Krupnov Yu.A. Ranking of the primary threats to the national security of the Russian Federation // National Interests: Priorities and Security. 2022;18(10):1905-1939. (In Russ.) <https://doi.org/10.24891/ni.18.10.1905>]
12. Крупнов Ю.А., Сильвестров С.Н., Старовойтов В.Г., Лапенкова Н.В. Конкурентный подход к оценке национальной безопасности Российской Федерации // Национальная безопасность / Nota Bene. 2023. № 5. С. 13–35. <https://doi.org/10.7256/2454-0668.2023.5.68816> [Krupnov Yu.A., Silvestrov S.N., Starovoytov V.G., Lapenkova N.V. Competitive approach to assessing the national security of the Russian Federation // National Security / Nota Bene. 2023;(5):13-35. (In Russ.) <https://doi.org/10.7256/2454-0668.2023.5.68816>]
13. Морозова Н.М., Шерлыгина В.В. Великобритания в системе международных отношений накануне Второй мировой войны // Столыпинский вестник. 2020. Т. 2. № 3. С. 25. <https://doi.org/10.24411/2713-1424-2020-10009> [Morozova N.M., Sherlygina V.V. Great Britain in the system of international relations on the eve of the Second World War // Stolypin Annals. 2020;2(3):25. (In Russ.) <https://doi.org/10.24411/2713-1424-2020-10009>]
14. Неймарк М.А. Кризисная геополитика и новый мировой порядок: перспективы России // Обозреватель. 2021. № 8(379). С. 5–16. [https://doi.org/10.48137/2074-2975\\_2021\\_8\\_5](https://doi.org/10.48137/2074-2975_2021_8_5) [Neimark M.A. [Crisis Geopolitics and New World Order: Prospects of Russia // Observer. 2021;(8):5-16. (In Russ.) [https://doi.org/10.48137/2074-2975\\_2021\\_8\\_5](https://doi.org/10.48137/2074-2975_2021_8_5)]
15. Григорьев Л.М., Павлюшина В.А., Музыченко Е.Э. Падение в мировую рецессию 2020... // Вопросы экономики. 2020. № 5. С. 5–24. <https://doi.org/10.32609/0042-8736-2020-5-5-2415> [Grigoriev L.M., Pavlyushina V.A., Muzychenko E.E. The fall into 2020 recession... // Voprosy Ekonomiki. 2020;(5):5-24. (In Russ.) <https://doi.org/10.32609/0042-8736-2020-5-5-2415>]
16. Nie Y., Федорова Д.С. Китай в попытке преодолеть пределы роста // Экономика. Профессия. Бизнес. 2019. № 3. С. 88–93. <https://doi.org/10.14258/epb201939> [Nie Y., Fedorova D.S. China attempts to overcome the limits of growth // Economics Profession Business. 2019(3):88-93. (In Russ.) <https://doi.org/10.14258/epb201939>]
17. Белов В.Б. Итоги 2022 г.: Экономический стандарт Германии на грани деиндустриализации? // Научно-аналитический вестник Института Европы РАН. 2022. № 6 (30). С. 70–84. <https://doi.org/10.15211/vestnikieran620227084> [Belov V.B. Results of 2022: German economy on the verge of deindustrialisation? // Scientific and Analytical Herald of Ie RAS. 2022;6(30):70-84. (In Russ.) <https://doi.org/10.15211/vestnikieran620227084>]
18. Кириченко Э.В. Растущий бюджетный дефицит и государственный долг США: оценки, проблемы, риски // Международная экономика. 2021. № 11. С. 812–825. <https://doi.org/10.33920/vne-04-2111-01> [Kirichenko E.V. Growing budget deficit and national debt: estimates, problems, risks // The World Economics. 2021;(11):812-825. (In Russ.) <https://doi.org/10.33920/vne-04-2111-01>]
19. Смирнов Ф.А. Деконструкция мировой финансово-экономической архитектуры. Часть 4.2 Кризисогенность мирового развития — финансовые кризисы // Новый университет. Серия: Актуальные проблемы гуманитарных и общественных наук. 2015. № 1(46). С. 43–52 [Smirnov F.A. Deconstruction the world financial and economic architecture. Part 4.2 Krizis of the world developments — financial crises // Novyi universitet. Seriya: Aktual'nye problemy gumanitarnykh i obshchestvennykh nauk. 2015;1(46):43-52. (In Russ.)]

20. Манушин Д.В. Антисанкционная и санкционная экономическая политика России 2022–2025. Часть 3: анализ антикризисных мер, управление российскими санкциями и антисанкциями // Russian Journal of Economics and Law. 2024. Т. 18. № 2. С. 332–368.  
<https://doi.org/10.21202/2782-2923.2024.2.332-368>  
[Manushin D.V. Anti-sanctions and sanctions economic policy of Russia 2022–2025. Part 3: analysis of anti-crisis measures, management of Russian sanctions and anti-sanctions // Russian Journal of Economics and Law. 2024;18(2):332-368. (In Russ.)  
<https://doi.org/10.21202/2782-2923.2024.2.332-368>]
21. Кудряшов А.Л. Прямые иностранные инвестиции в финансовую систему России в условиях санкционного давления // Вестник евразийской науки. 2023. Т. 15. № 1. URL: <https://esj.today/PDF/71ECVN123.pdf>  
[Kudryashov A.L. Foreign direct investment in the Russian financial system under sanctions pressure // The Eurasian Scientific Journal. 2023;15(1): URL: <https://esj.today/PDF/71ECVN123.pdf>. (In Russ.)]
22. Urry J. Mobilities. Cambridge, Polity. 2007. 336 p.
23. Florida R. The flight of the creative class. The New Global Competition for Talent. New York, Harper Business, Harper Collins. 2005. 320 p.
24. Ячин С.Е., Купряшкин И.В., Хун М.Л. Перспективы гегемонии в Восточной Азии в свете мир-системного подхода // Мировая экономика и международные отношения. 2020. Т. 64. № 1. С. 35–45.  
<https://doi.org/10.20542/0131-2227-2020-64-1-35-45>  
[Yachin S.E., Kupryashkin I.V., Hong M.L. Perspectives of hegemony in the Eastern Asia in light of the world-system approach // World Economy and International Relations. 2020;64(1):35-45. (In Russ.)  
<https://doi.org/10.20542/0131-2227-2020-64-1-35-45>]
25. Пустынная Е.В. Интеграция региональных логистических каналов в единую транспортно-логистическую систему как условие для эффективного ответа российской экономики на международные вызовы // Вестник Южно-Уральского государственного университета. Серия: Экономика и менеджмент. 2022.

Т. 16. № 4. С. 172–185. <https://doi.org/10.14529/em220418>  
[Pustynnikova E.V. Integration of regional logistics channels into a unified transport and logistics system as a condition for an effective response of the Russian economy to international challenges // Bulletin of the South Ural State University. Series: Economics and Management. 2022;16(4):172-185, (In Russ.)  
<https://doi.org/10.14529/em220418>]

## Сведения об авторах

**Крупнов Юрий Александрович:** доктор экономических наук, доцент, ведущий научный сотрудник, Институт экономической политики и проблем экономической безопасности ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации»

Количество публикаций: 156, в т.ч. 7 монографий и 4 учебных издания

Область научных интересов: национальная безопасность, экономическая политика

ORCID: 0000-0002-9524-3747

SPIN-код: 2384-6160

*Контактная информация:*

Адрес: 125993, г. Москва, Ленинградский проспект, д. 49/2  
[yukrupnov@mail.ru](mailto:yukrupnov@mail.ru)

**Сильвестров Сергей Николаевич:** доктор экономических наук, профессор, директор Института экономической политики и проблем экономической безопасности ФГБОУ ВО Финансовый университет при Правительстве Российской Федерации

Количество публикаций: 302, в т.ч. 27 монографий и 14 учебных изданий

Область научных интересов: национальная безопасность, экономическая политика

ORCID: 0000-0002-7678-1283

SPIN-код: 8987-5771

*Контактная информация:*

Адрес: 125993, г. Москва, Ленинградский проспект, д. 49/2  
[silvestrsn@gmail.com](mailto:silvestrsn@gmail.com)

Статья поступила в редакцию: 15.09.2024

Одобрена после рецензирования: 07.10.2024

Принята к публикации: 18.10.2024

Дата публикации: 28.02.2025

*The article was submitted: 15.09.2024*

*Approved after reviewing: 07.10.2024*

*Accepted for publication: 18.10.2024*

*Date of publication: 28.02.2025*

УДК 338.2  
Научная специальность: 5.2.3  
<https://elibrary.ru/uuyvdk>

ISSN 1812-5220  
© Проблемы анализа риска, 2025

# Риск-ориентированный подход к оценке информационно-цифровой составляющей экономической безопасности субъектов малого предпринимательства

Каранина Е.В.\*,

Котанджян А.В.,

Коршунов В.Л.,

Вятский государственный университет,  
610000, Россия, г. Киров,  
ул. Московская, 36

## Аннотация

В рамках настоящей статьи рассматривается понятие информационно-цифровой составляющей экономической безопасности субъекта предпринимательства. Приводятся основные проблемы подсистемы, изменение требований к организации защиты с учетом современных реалий, а также возможности идентификации основных рисков с учетом риск-ориентированного подхода.

Цель исследования: предложение механизма оценки уровня информационно-цифровой составляющей экономической безопасности субъекта малого предпринимательства.

Задачи исследования: определение и интерпретация самого понятия информационно-цифровой подсистемы экономической безопасности, определение факторов угроз, а также обозначение перечня показателей с пороговыми значениями с последующей математической обработкой полученных данных, на примере реально функционирующей компании.

**Ключевые слова:** экономическая безопасность; информационно-цифровая безопасность; кибератаки; риски; риск-ориентированный подход.

**Для цитирования:** Каранина Е.В., Котанджян А.В., Коршунов В.Л. Риск-ориентированный подход к оценке информационно-цифровой составляющей экономической безопасности субъектов малого предпринимательства // Проблемы анализа риска. 2025. Т. 22. № 1. С. 34–45. — EDN: UUYVDK

**Авторы заявляют об отсутствии конфликта интересов**

# Risk-Oriented Approach to Assessing the Information and Digital Component of Economic Security of Small Business Entities

Elena V. Karanina\*,  
Asya V. Kotandzhyan ,  
Vyacheslav L. Korshunov,  
Vyatka State University,  
Moscow str., 36, Kirov, 610000,  
Russia

## Abstract

This article examines the concept of the information and digital component of economic security of a business entity. The main problems of the subsystem, changes in the requirements for organizing protection taking into account modern realities, as well as the possibilities of identifying the main risks taking into account the risk-oriented approach are given.

The purpose of this article is to propose a mechanism for assessing the level of the information and digital component of economic security of a small business entity.

The objectives are to define and interpret the very concept of the information and digital subsystem of economic security, to determine threat factors, and to designate a list of indicators with threshold values with subsequent mathematical processing of the obtained data using the example of a real operating company.

**Keywords:** economic security; information and digital security; cyber-attacks; risks; risk-oriented approach.

**For citation:** Karanina E.V., Kotandzhyan A.V., Korshunov V.L. Risk-oriented approach to assessing the information and digital component of economic security of small business entities // *Issues of Risk Analysis*. 2025;22(1):34-45. (In Russ.). — EDN: UUYVDK

**The authors declare no conflict of interest**

## Содержание

Введение

1. Понятие и сущность информационно-цифровой составляющей экономической безопасности компаний

2. Методика оценки уровня информационно-цифровой составляющей экономической безопасности субъекта малого предпринимательства

Заключение

Список источников

## Введение

В условиях современной экономики, характеризующейся неопределенностью и нестабильностью, деятельность компаний связана с многочисленными рисками, которые могут привести к серьезным последствиям.

Особенно актуальны в настоящее время угрозы, связанные с распространением кибератак на компании и предприятия отечественного рынка. Также идет проседание систем защиты информации и объектов на фоне ухода из страны западных IT-компаний.

С начала 2023 г. наметилась тенденция к усложнению и разнообразию кибератак. Теперь злоумышленники используют трудно обнаруживаемые вредоносные программы, автоматизированные инструменты и даже искусственный интеллект для подготовки атак. Кроме того, они часто применяют многоэтапные стратегии взлома, привлекая для этого доверенных партнеров<sup>1</sup>.

По результатам опроса, проведенного компанией «Инфосистемы Джет» организации сталкиваются с множеством проблем и рисков, связанных с информационно-цифровой составляющей, а именно:

- дефицит квалифицированных кадров и управление талантами (нехватка специалистов, трудности с поиском и удержанием профессионалов, отсутствие необходимого опыта);
- трудности в модернизации инфраструктуры информационной безопасности при переходе на оборудование и программное обеспечение от российских производителей (отсутствие альтернативных решений);
- проблемы с поддержанием работоспособности существующих зарубежных решений;
- трудности с выделением финансирования и защитой проектов;
- проблемы в организации и управлении процессами информационной безопасности<sup>2</sup>.

Также наблюдается крайне негативная тенденция по увеличению числа утечки информации по вине сотрудников (рис. 1).

<sup>1</sup> Итоги года. Годовой отчет Центра информационной безопасности компании «Инфосистемы Джет» // URL: [https://jetsirt.su/upload/godovoy\\_otchet\\_jet\\_2023.pdf](https://jetsirt.su/upload/godovoy_otchet_jet_2023.pdf) (дата обращения: 15.02.2025).

<sup>2</sup> Итоги года. Годовой отчет Центра информационной безопасности компании «Инфосистемы Джет» // URL: [https://jetsirt.su/upload/godovoy\\_otchet\\_jet\\_2023.pdf](https://jetsirt.su/upload/godovoy_otchet_jet_2023.pdf) (дата обращения: 15.02.2025).

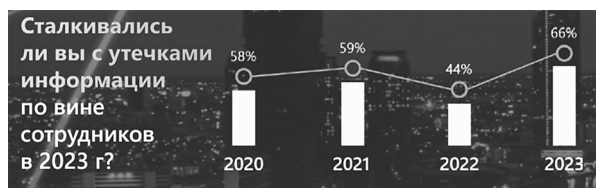


Рис. 1. Динамика количества утечек информации по вине сотрудников среди опрошенных компаний<sup>3</sup>.

Figure 1. Dynamics of the number of information leaks due to the fault of employees among the surveyed companies

При этом ситуация с внедрением средств информационной защиты стабилизируется: процессы налажены, компании хорошо оснащены и даже масштабируют защиту. Прослеживается влияние новых нормативных требований и повышенного общественного внимания к вопросам защиты данных.

Все это требует предложения определенного подхода к понятию информационно-цифровой составляющей экономической безопасности, а также исследования возможных направлений анализа рисков в этой подсистеме.

## 1. Понятие и сущность информационно-цифровой составляющей экономической безопасности компаний

В рамках концепции устойчивого развития, которая широко используется в современном мире, под экономической безопасностью понимается равновесие внутренней структуры открытой системы, включающей в себя социально-экономические и экологические аспекты. Это равновесие позволяет системе стабильно функционировать, воспроизводиться и развиваться. Кроме того, важным аспектом является гармоничное взаимодействие системы с окружающей средой [1].

Исследователи изучают экономическую безопасность на разных уровнях экономической системы, но основное внимание уделяется микроуровню. Здесь все еще есть спорные моменты относительно компонентов экономической безопасности [2]. Однако ряд ученых сходятся во мнении, определяющем отнесение информационной компоненты или составляющей к одной из подсистем экономической

<sup>3</sup> Исследование уровня информационной безопасности в организациях России. Отчет «СёрчИнформ» // URL: <https://ict.moscow/static/pdf/files/godovoe-issledovanie-2023.pdf> (дата обращения: 15.02.2025).

безопасности. При этом глобальные процессы цифровой трансформации предъявляют новые требования к обеспечению информационной безопасности компаний, такие как:

- повышение требований к укреплению информационно-цифровой компоненты хозяйствующих субъектов в целях защиты от киберпреступлений;
- следование основным веяниям технологического прорыва;
- «оцифровка» бизнес-процессов;
- развитие и распространение цифровых каналов продаж.

Так, подобные изменения технологического и финансового характера, предопределившие понятие цифровизации экономического сектора, видоизменяют и понятие информационной безопасности добавлением нового компонента — информационно-цифровую составляющую [3].

Сегодня в условиях перехода к цифровой экономике информация стала ценным активом каждой организации. Одной из важных задач в области защиты активов является обеспечение информационной безопасности. Без регулярного мониторинга информационной безопасности невозможно обеспечить стабильное финансовое положение экономических агентов. В то же время неорганизованный подход к обеспечению информационной безопасности может создать риск потери информационных активов и вызвать финансовую нестабильность организации. Поэтому для снижения рисков каждая организация должна создать отлаженную систему безопасности, которая позволит постоянно управлять уровнем информационной безопасности.

Таким образом, под информационно-цифровой составляющей экономической безопасности субъекта предпринимательства понимается достаточный уровень обеспечения общих принципов информационной безопасности наряду с овладением и внедрением цифровых технологий в соответствии с протекающими бизнес-процессами компании, а также обеспечением цифровой гигиены и цифровой грамотности ее сотрудников [3].

Также под информационной безопасностью компании следует понимать комплекс мер и инструментов, направленных на: обеспечение защиты и безопасности информационных ресурсов, обеспечение достоверности и конфиденциальности информации,

используемой в экономической деятельности, и на предотвращение угроз, связанных с несанкционированным доступом, хищением, подменой и искажением информации. Эти компоненты включают меры по защите персональных данных, меры информационной безопасности для корпоративных систем и меры кибербезопасности [4].

Укреплению позиций цифровой экономики и обеспечению стабильности и безопасности информационно-цифровой составляющей безопасности представителей бизнеса препятствуют следующие риск-факторы:

- компрометация цифровых данных пользователей — сотрудников и клиентов компании;
- внешние атаки на информационно-цифровую платформу;
- технологические риски обеспечения целостности киберзащиты;
- потеря конкурентных преимуществ в гонке «цифровых вооружений»;
- нехватка квалифицированных кадров в сфере обеспечения информационной безопасности и работ ИКТ [5].

В рамках информационно-цифровой безопасности компаний можно рассмотреть два основных типа угроз:

- 1) непреднамеренные — выражаются ошибками в управлении;
- 2) преднамеренные — незаконное получение информации другими лицами.

Причиненные ущербы от таких рисков способны принести различные последствия:

- подрыв деловой репутации организации;
- раскрытие личных данных отдельных лиц, сопряженное с ущербом для них;
- финансовые потери от разглашения охраняемой (конфиденциальной) информации;
- ущерб, связанный с восстановлением нарушенных информационных ресурсов;
- убытки, возникшие в результате невозможности исполнения обязательств перед третьими сторонами;
- моральный и материальный ущерб от нарушения работы всего предприятия [6].

Немаловажным является выявление источников вышеперечисленных угроз, которые, в свою очередь, подразделяются на две категории: внешние и внутренние (рис. 2).



Рис. 2. Внешние и внутренние угрозы информационной безопасности предприятия

Figure 2. External and internal threats to enterprise information security

Поэтому в условиях, когда информационная составляющая экономической безопасности становится все более важной для всех организаций, системы информационной безопасности должны быть оптимизированы, а их мониторинг и оценка — организованы.

Для эффективной организации информационной безопасности необходим анализ угроз и уязвимостей информационной системы, а также оценка связанных с ними рисков. Только после этого можно приступать к выбору и внедрению соответствующих технических мер защиты [7].

Главной целью создания системы информационной безопасности является обеспечение конфиденциальности, целостности и доступности информации.

К созданию своих систем информационной безопасности все компании подходят по-разному. Некоторые формируют собственные организационные структуры и департаменты, опираясь на свой опыт, другие доверяют защиту информации аутсорсинговым

компаниям. В зависимости от сферы деятельности по-разному решаются и проблемы информационной безопасности компании. Для более полного понимания основных принципов построения и поддержки таких систем в российских компаниях рассмотрим методы и способы, которые они применяют для обеспечения информационной безопасности [8].

Максимальная эффективность защиты достигается за счет использования системного подхода. В процессе защиты информационных систем организации принимается ряд мер по предвидению, предотвращению и устранению угроз безопасности.

На практике для обеспечения информационной безопасности используются различные меры. Условно их можно разделить на три группы (рис. 3).

К первой группе относятся материальные средства, представленные оборудованием, техническими устройствами и компьютерной техникой, а также финансовые вложения. Вторая группа обеспечивает нормативно-правовое регулирование процессов,

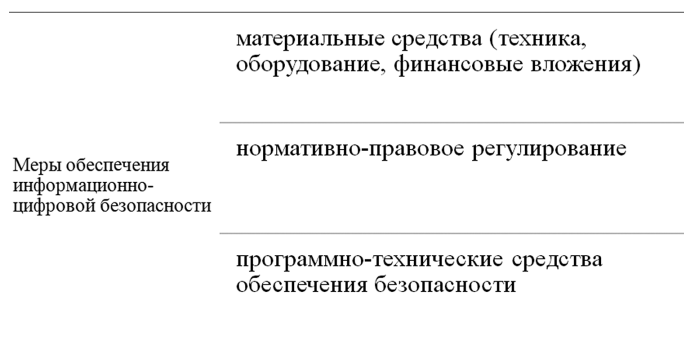


Рис. 3. Направления мер обеспечения информационно-цифровой безопасности

Figure 3. Areas of measures to ensure information and digital security

связанных с информационной безопасностью. Таким образом, в рамках организации существуют различные документы, например, в виде регистрационных, правоустанавливающих и правоудостоверяющих документов, договоров.

В этом контексте третья группа мер направлена на обеспечение технической поддержки информационной безопасности, с целью обеспечения доступности, целостности и конфиденциальности информации. Эти меры включают в себя использование разнообразных технических средств для защиты таких объектов, как: технические устройства и маршрутизаторы; каналы связи и системы удаленного доступа; серверы; программные средства и софт; базы данных, а также различные методы и способы обеспечения безопасности.

Основные принципы, на которых строится работа систем безопасности, включают:

1. Соответствие мер защиты, осуществляемых системой, актуальным угрозам безопасности, принимаемая во внимание различные риски и потенциальные уязвимости.
2. Постепенное создание системы с тщательным планированием и определением этапов, чтобы оптимизировать финансовые затраты и при этом сохранить единую концепцию системы.
3. Защита инвестиций путем использования имеющихся средств и систем защиты информации для построения системы, что позволяет снизить затраты на капиталовложения.
4. Централизованное управление и мониторинг системы безопасности для обеспечения более эффективного контроля и реагирования на возможные угрозы.
5. Учет и эффективная интеграция системы безопасности с существующими процессами управления

информационными технологиями, чтобы создать более гармоничное и согласованное функционирование всей организации.

Таким образом, эти принципы являются фундаментом для создания надежных и эффективных систем безопасности, которые гарантируют сохранность информации и обеспечивают защиту от возможных угроз. С целью предложения механизма диагностики состояния информационно-цифровой составляющей экономической безопасности компании предполагается ориентироваться на вышеуказанные принципы при разработке показателей, оценивающих уровень безопасности этой подсистемы.

## 2. Методика оценки уровня информационно-цифровой безопасности составляющей экономической безопасности субъекта малого предпринимательства

В настоящее время существует достаточное количество публикаций, отражающих различные аспекты экономической безопасности и, в частности, информационной безопасности (например, физические аспекты защиты, контроль доступа, защита конфиденциальной информации и персональных данных, риск недостоверности информации и его влияние на экономическую безопасность), каждая из которых отражает свой подход к проблеме [7, 9]. Тем не менее, можно отметить, что комплексный подход к анализу и оценке информационной составляющей экономической безопасности в большинстве случаев не применяется. В таких случаях предметом исследования часто становится один из аспектов информационной безопасности.

Существует несколько факторов, которые могут объяснить эту проблему:

1. Методы оценки информационных рисков и угроз недостаточно проработаны в связи с быстро изменяющейся ситуацией в области информационной безопасности и появлением новых технологий.

2. Оценка полученных убытков от реализации рисков и угроз является сложной задачей из-за трудностей прогнозирования всех возможных последствий, включая влияние на репутацию организации.

3. События, связанные с нарушением информационной безопасности, и их последствия часто не являются идентичными и стандартизированными, так как они зависят от конкретных субъектов и объектов информационной безопасности.

4. Получение итогового результата в области информационной безопасности зависит от принятия

комплексных решений, поэтому определить конкретные меры, которые максимально повысят уровень информационной безопасности, становится достаточно сложно.

Один из важных этапов разработки системы информационной безопасности организации — это выявление, анализ и оценка рисков информационной безопасности. Верность оценки рисков напрямую влияет на эффективность всей системы информационной безопасности организации.

Если речь идет об оценке информационного компонента экономической безопасности, следует отметить, что показатели информационной безопасности можно разделить на две категории: количественные и стоимостные.

В основе методики лежит сопоставление информационно-цифровых характеристик в виде результата



Рис. 4. Механизм управления и идентификации рисков экономической безопасности компании

Figure 4. Mechanism of management and identification of economic security risks of the company

деятельности компании со среднеотраслевыми показателями (также в учет берутся средние показатели аналогичной подсистемы на региональном уровне). Для построения групповых и интегральных индикаторов оценивания осуществляется перевод показателей типа  $x$  в единую балльную характеристику  $X$ , измеряемую в шкале от 1 до 100 баллов на основе пороговых уровней безопасности  $x^l$  и  $x^h$  ( $x^l < x^h$ ) методом кусочно-линейного масштабирования. Так, для показателя  $x$ , большее значение которого характеризует более высокий уровень безопасности, т.е. для потенциал-формирующего фактора (или коротко — фактора потенциала) используется следующая формула:

$$\begin{cases} \text{если } x < x^l, \text{ то } X = 1, \\ \text{если } x > x^h, \text{ то } X = 100, \\ \text{иначе } X = \frac{x - x^l}{x^h - x^l} \cdot 99 + 1. \end{cases} \quad (1)$$

Значение оценки в один балл означает очень низкий уровень безопасности (за нижним порогом безопасности  $x^l$ ), а в 100 баллов — очень высокий уровень безопасности (за верхним порогом безопасности  $x^h$ ).

Балльная оценка  $1 < X < 34$  означает низкий уровень безопасности;

$34 \leq X < 67$  — средний уровень безопасности;

$67 \leq X < 100$  — высокий уровень безопасности.

Формирование пороговых уровней  $x^l$  и  $x^h$  осуществляется так, чтобы балльная оценка  $X \geq 67$  означала

результат не хуже среднего отраслевого (регионального). В этом контексте оценка уровня экономической безопасности фактически представляет собой анализ конкурентоспособности.

Комплексная оценка информационно-цифровой безопасности формируется на основе системы индикаторов безопасности, имеющей иерархическую структуру, интегральная оценка — на основе обобщенной оценки групповых индикаторов.

Для апробации предложенной методики в качестве объекта анализа была выбрана компания Кировской области, являющаяся представителем малого бизнеса региона, функционирующая на рынке более семи лет. Основным видом деятельности компании является «Торговля оптовой писчебумажными и канцелярскими товарами».

Показатели для оценки состояния информационно-цифровой составляющей выбранного объекта были определены путем письменного опроса руководства компании и анализом финансовой отчетности.

Результаты опроса руководства позволили сделать вывод о грамотном построении бизнес-процессов компании и их цифровизации. Наиболее значимые бизнес-процессы, автоматизированные посредством цифровых платформ представлены на рис. 5.

Исходя из этого, делаем вывод, что основные три направления деятельности компании торговой отрасли: лидогенерация, складской и бухгалтерский учет, а также бизнес-аналитика полностью цифровизированы, бизнес-процессы организованы и прозрачны.

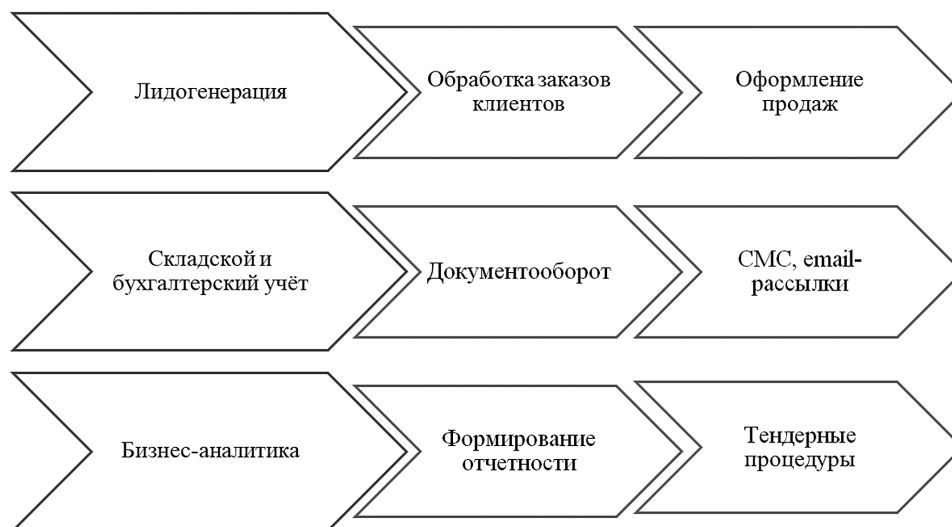


Рис. 5. Направления цифровой трансформации бизнес-процессов рассматриваемой компании

Figure 5. Directions of digital transformation of business processes of the company in question

Тем не менее, одной из уязвимых зон информационно-цифровой подсистемы является отсутствие интегрированной системы, хотя процесс был запланирован на 2025 г.

Оперируя имеющейся информацией о состоянии системы информационной безопасности рассматриваемой компании, представим возможные индикаторы безопасности (табл. 1).

Индикаторы для оценки состояния информационно-цифровой безопасности подразумевают:

1. Темп роста вложений в развитие цифровизации бизнеса отражает изменение расходов на ПО в динамике, где:

$C_{\text{тек.пер.}}$  — сумма вложений в программное обеспечение в текущем периоде;

$C_{\text{пред.пер.}}$  — сумма вложений в программное обеспечение в предыдущем периоде.

2. Коэффициент цифровизации бизнес-процессов компании определяет степень автоматизации с помощью цифровых технологий бизнес-процессов компании, где:

$Ч_{\text{об.}}$  — общее число основных и вспомогательных бизнес-процессов компании;

$Ч_{\text{циф.}}$  — число бизнес-процессов, имеющих цифровые решения.

3. Защищенность корпоративных данных подразумевает степень защищенности критической информации компании, где:

$K_{\text{общ.}}$  — объем информации, разглашение которой может повлечь негативные последствия для предприятия, %;

$K_{\text{заш.}}$  — общий объем защищенной информации.

4. Оценка работы IT-отдела подразумевает анализ качества работы соответствующего персонала, где:

$ЧП_{\text{п}}$  — численность работников, непреднамеренные действия которых привели к утечке информации из-за низкого уровня подготовки персонала к распознаванию угроз безопасности, чел.;

$ЧП_{\text{общ.}}$  — общая численность работников, имеющих доступ к закрытой информации, чел.

Последующий перевод обозначенных индикаторов рассматриваемой компании в балльные значения при помощи формулы 1 дал следующие результаты (табл. 2).

Таким образом, можно сделать вывод, что на текущий момент информационная подсистема экономической безопасности компании находится на должном уровне защищенности. Вложения в развитие цифровизации бизнеса демонстрировали стабильный рост в 2020–2022 г., в 2023 г. наблюдался рост порядка 2%, что не позволило индикатору выйти в безрисковую зону безопасности. Остальные показатели находились в границах значений, соответствующих высокому уровню безопасности.

**Таблица 1. Комплекс индикаторов информационно-цифровой безопасности**

*Table 1. Set of indicators of information and digital security*

Группа показателей	Индикатор	Направление оптимизации	Формула расчета	Пороговые значения $x^l$ и $x^h$ , соответственно
Информационная безопасность	1. Темп роста вложений в развитие цифровизации бизнеса	Максимизация	$\frac{C_{\text{тек.пер.}}}{C_{\text{пред.пер.}}} \times 100 - 100$	5; 10%
	2. Коэффициент цифровизации бизнес-процессов компании	Расчетная величина	$\frac{Ч_{\text{об.}}}{Ч_{\text{циф.}}}$	80; 100%
	3. Защищенность корпоративных данных	Максимизация	$\frac{K_{\text{заш.}}}{K_{\text{общ.}}}$	95; 100%
	4. Оценка работы IT-отдела	Максимизация	$\frac{ЧП_{\text{общ.}} - ЧП_{\text{п}}}{ЧП_{\text{общ.}}}$	95; 100%

**Таблица 2. Интегральная оценка индикаторов информационно-цифровой безопасности компании**  
Table 2. Integrated assessment of information and digital security indicators of the company

Индикаторы безопасности	2019 г.	2020 г.	2021 г.	2022 г.	2023 г.
<b>Интегральная оценка информационной безопасности</b>	75	100	100	100	75
Темп роста вложений в развитие цифровизации бизнеса	1	100	100	100	1
Коэффициент цифровизации бизнес-процессов компании	100	100	100	100	100
Защищенность корпоративных данных	100	100	100	100	100
Оценка работы ИТ-отдела	100	100	100	100	100

## Заключение

Экономическая безопасность субъектов малого бизнеса — это определенное состояние защищенности хозяйственной деятельности компании, которое позволяет ему развиваться и сохранять финансовую стабильность, несмотря на негативное влияние внешних и внутренних факторов. Для того чтобы обеспечить подобное состояние, важно своевременно идентифицировать возможные риски, в том числе в контексте обеспечения цифровой трансформации бизнеса.

Представители малого бизнеса сталкиваются с многочисленными угрозами и рисками в процессе ведения своей деятельности. Существует множество методов для классификации рисков и их типов, а также способов их определения. Относительно рисков информационной подсистемы безопасности следует отметить их постоянное видоизменение и преобразование, а увеличение числа кибератак и развитие технологических возможностей злоумышленников, создает высокие требования к организации системы защиты.

Однако для каждого конкретного представителя малых компаний наиболее эффективным подходом к группировке рисков является их разделение по направлениям деятельности, связка показателей на уровне региона и отдельного субъекта.

Исходя из примера предложенного механизма оценки рисков информационно-цифровой составляющей конкретной компании, можно разработать и адаптировать собственный комплекс индикаторов, их пороговых значений и направлений для оптимизации, учитывая специфику бизнеса и потребности региона.

## Список источников [References]

1. Быков А. А. О современных угрозах, рисках и возможностях // Проблемы анализа риска. 2024. Т. 21. № 1. С. 8–11 [Bykov A. A. About today's threats, risks, and opportunities // Issues of Risk Analysis. 2024;21(1):8–11. (In Russ.)]
2. Соколов А. П. Управление информационной составляющей в системе экономической безопасности предприятия // Вестник Алтайской академии экономики и права. 2024. № 2–2. С. 267–273. <https://doi.org/10.17513/vaael.3271> [Sokolov A. P. Information component management in the system of economic security of the enterprise // Bulletin of the Altai Academy of Economics and Law. 2024;(2–2):267–273. (In Russ.) <https://doi.org/10.17513/vaael.3271>]
3. Каранина Е. В. Цифровые финансы и экосистемы: обеспечение устойчивого и безопасного развития / Е. В. Каранина, А. В. Котанджян. М: Научная библиотека, 2023. 156 с. EDN JZPWMA [Karanina E. V. Digital Finance and Ecosystems: Ensuring Sustainable and Safe Development / E. V. Karanina, A. V. Kotanjyan. M: Scientific Library, 2023. 156 p. (In Russ.) EDN JZPWMA]
4. Котанджян А. В. Киберугрозы и вызовы цифровой трансформации бизнеса / А. В. Котанджян, Д. С. Лутошкина // Студент. Наука. Регион: сборник материалов III региональной антиконференции, Киров, 23 октября 2024 г. Киров: Издательство «Радуга-ИПЕСС», 2024. С. 105–107 [Kotanjyan A. V. Cyber threats and challenges of digital business transformation / A. V. Kotanjyan, D. S. Lutoshkina // Student. Science. Region: collection of materials from the III regional anti-conference, Kirov, October 23, 2024. Kirov: Raduga-PRESS Publishing House, 2024. P. 105–107. (In Russ.)]

5. Лолаева А. С. Информационная безопасность в свете развития цифровой экономики в Российской Федерации // Междисциплинарные исследования: опыт прошлого, возможности настоящего, стратегии будущего: сборник статей III Международной научно-практической конференции, Мельбурн, 20 февраля 2021 года Мельбурн: МЦНИР «Научный взгляд», 2021. С. 90–98. EDN MPYDNN [Lolaeva A. S. Information security in the light of the development of the digital economy in the Russian Federation // Interdisciplinary research: past experience, present opportunities, future strategies: collection of articles III of the International Scientific and Practical Conference, Melbourne, February 20, 2021 Melbourne: ICNIR “Scientific view”, 2021. P. 90–98. (In Russ.) EDN MPYDNN]
6. Никитин А. В. Информационная составляющая экономической безопасности // Современная наука: прогнозы, факты, тенденции развития: Сборник материалов XV Международной научно-практической конференции, посвященной 60-летию Чебоксарского кооперативного института (филиала) Российского университета кооперации, Чебоксары, 31 января 2022 года. Чебоксары: Чебоксарский кооперативный институт (филиал) автономной некоммерческой образовательной организации высшего образования Центросоюза Российской Федерации «Российский университет кооперации», 2022. С. 461–467 [Nikitin A. V. Information component of economic security // Modern science: forecasts, facts, development trends: Collection of materials of the XV International Scientific and Practical Conference dedicated to the 60th anniversary of the Cheboksary Cooperative Institute (branch) of the Russian University of Cooperation, Cheboksary, January 31, 2022. Cheboksary: Cheboksary Cooperative Institute (branch) of the autonomous non-profit educational organization of higher education of the Central Union of the Russian Federation “Russian University of Cooperation,” 2022. P. 461–467. (In Russ.)]
7. Андреева Д. А., Малинин А. М. Комплексная экономическая безопасность социально-экономических систем в контексте перспектив экономического роста // Техничко-технологические проблемы сервиса. 2020. № 2(52). С. 64–69 [Andreeva D. A., Malinin A. M. Integrated economic security of socio-economic systems in the context of economic growth prospects // Technical and Technological Problems of the Service. 2020;(2):64–69. (In Russ.)]
8. Селищев В. А., Чечуга О. В., Наседкин М. Н. Построение системы информационной безопасности предприятия // Известия ТулГУ. Технические науки. 2009. № 1–2. С. 137–144 [Selishchev V. A., Chechuga O. V., Nasedkin M. N. Building an information security system for an enterprise // Izvestia TulSU. Technical sciences. 2009;(1–2):137–144. (In Russ.)]
9. Караулов В. М. Исследование экономической безопасности регионов на основе оценки потенциала и рисков // Проблемы анализа риска. 2023. Т. 20. № 6. С. 10–23. [Karaulov V. M. The study of the economic security of regions based on the assessment of potential and risks // Issues of Risk Analysis. 2023;20(6):10–23. (In Russ.)]
10. Рудакова Т. А., Бондаренко А. С. Инструментарий оценки информационной составляющей экономической безопасности предприятия // Лизинг. 2019. № 6. 47–55 [Rudakova T. A., Bondarenko A. S. Toolkit for assessing information component of economic security of the enterprise // Journal “Leasing”. 2019;(6):47–55. (In Russ.)]

## Сведения об авторах

**Каранина Елена Валерьевна:** доктор экономических наук, профессор, заведующий кафедрой финансов и экономической безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Вятский государственный университет» (ВятГУ)

Количество публикаций: более 450

Область научных интересов: экономическая безопасность региона, оценка рисков, резилиенс-диагностика безопасности и устойчивости региональных экосистем

ResearcherID: L-1395-2016

Scopus Author ID: 57192661919

ORCID: 0000-0002-5439-5912

*Контактная информация:*

Адрес: 610000, г. Киров, ул. Московская, д. 36

Karanina@vyatsu.ru

**Котанджян Ася Валентиновна:** старший преподаватель кафедры финансов и экономической безопасности Вятского государственного университета (ВятГУ)

Количество публикаций: более 100

Область научных интересов: управление рисками, экономическая безопасность, кадровая составляющая экономической безопасности, информационная безопасность

Scopus Author ID: 57216910073

ORCID: 0000-0002-2043-1356

*Контактная информация:*

Адрес: 610000, г. Киров, ул. Свободы, д. 122

usr21823@vyatsu.ru

**Коршунов Вячеслав Леонидович:** аспирант кафедры финансов и экономической безопасности Вятского государственного университета (ВятГУ)

Количество публикаций: более 5

Область научных интересов: стандарты управления рисками и экономической безопасности, информационная безопасность малого бизнеса

ORCID: 0009-0008-1372-6771

*Контактная информация:*

Адрес: 610000, г. Киров, ул. Свободы, д. 122

usr21823@vyatsu.ru

Статья поступила в редакцию: 27.01.2025

Одобрена после рецензирования: 04.02.2025

Принята к публикации: 05.02.2025

Дата публикации: 28.02.2025

*The article was submitted: 27.01.2025*

*Approved after reviewing: 04.02.2025*

*Accepted for publication: 05.02.2025*

*Date of publication: 28.02.2025*

УДК 614.8  
Научная специальность: 2.10.3  
<https://elibrary.ru/ggswyu>

ISSN 1812-5220  
© Проблемы анализа риска, 2025

# Становление и развитие метода «Анализ опасности и работоспособности» как метода анализа риска аварий

**Дроняев О.И.\*,**  
**Мартынюк В.Ф.,**  
РГУ нефти и газа (НИУ)  
имени И.М. Губкина,  
119991, Россия, г. Москва,  
Ленинский пр-кт, д. 65, корп. 1

## Аннотация

Рассмотрено становление метода «Анализ опасности и работоспособности» (АОР), который широко известен под английским наименованием «Hazard and operability studies» (HAZOP), с 1960 по 2024 гг.

Обозначен вклад в развитие метода зарубежных институтов и компаний «Imperial Chemical industries», «Institution of Chemical Engineers», «American Institute of Chemical Engineers», а также Российских государственных надзорных органов и коммерческих организаций. Подчеркивается принципиальное различие задач, связанных с анализом риска аварий и анализом риска достижения целей проекта, которые объединены в канонической версии метода. Это создает некоторую путаницу в использовании методических документов, созданных для решения одних задач при решении задач совсем другого направления. Продемонстрированы ограничения, возможности и перспективы метода при решении задач анализа риска аварий.

Рассмотрены возможные дополнения метода специальными инструментами или привлечение других методов анализа риска аварий.

**Ключевые слова:** метод анализа риска аварий; анализ опасности и работоспособности; АОР; HAZOP.

**Для цитирования:** Дроняев О.И., Мартынюк В.Ф. Становление и развитие метода «Анализ опасности и работоспособности» как метода анализа риска аварий // Проблемы анализа риска. 2025. Т. 22. № 1. С. 46–53. — EDN: GGSWYU

**Авторы заявляют об отсутствии конфликта интересов**

# Formation and Development of the «Hazard and Operability Studies» as a Method of Accident Risk Analysis

Oleg I. Dronyaev\*,  
Vasily Ph. Martynyuk,  
Gubkin Russian State University  
of Oil and Gas,  
Leninsky Prospect, 65, bldg. 1,  
Moscow, 119991, Russia

## Abstract

The formation of the method "Hazard and operability studies" (HAZOP) from 1960 to 2024, is considered.

The contribution to the development of the method of foreign institutes and companies "Imperial Chemical industries", "Institute of Chemical Engineers", "American Institute of Chemical Engineers", as well as Russian state supervisory authorities and commercial organizations is indicated. The fundamental difference between the tasks related to the analysis of the risk of accidents and the analysis of the risk of achieving the project goals, which are combined in the canonical version of the method, is emphasized.

This creates some confusion in the use of methodological documents created to solve some problems when solving problems in a completely different direction. The limitations, possibilities and prospects of the betting method for solving of accident risk analysis problems are demonstrated.

Possible additions to the method with special tools or the use of other methods of accident risk analysis are considered.

---

**Keywords:** accident risk analysis method; Hazard and Operability Studies; HAZOP.

---

**For citation:** Dronyaev O.I., Martynyuk V.Ph. Formation and development of the "Hazard and operability studies" as a method of accident risk analysis // *Issues of Risk Analysis*. 2025;22(1):46-53. (In Russ.). — EDN: GGSWYU

---

**The authors declare no conflict of interest**

## Содержание

Введение

1. Создание метода «Критического анализа» (1960–1970 годы)
2. Синтез метода «Анализ опасности и работоспособности» (1970–2000 годы)
3. Формализация метода «Анализ опасности и работоспособности» в России и за рубежом (2000–2024 годы)
4. Ограничения, возможности и перспективы

Заключение

Список источников

---

## Введение

В настоящее время в России и за рубежом обеспечение и поддержание необходимого уровня производственной безопасности на производственных объектах является ключевой целью как для защищенности жизненно важных интересов личности и общества, сохранения и восстановления окружающей среды, так и для предотвращения потери доходов производства. Для достижения этой цели используются качественные и количественные методы анализа риска.

В перечнях рекомендуемых методов анализа риска аварий<sup>1</sup>, публикациях института инженеров-химиков в Великобритании (Institution of Chemical Engineers, IChemE) [1] и центра безопасности химических процессов (Center for Chemical Process Safety, CCPS) [2], монографии [3] присутствует метод «Анализ опасности и работоспособности» (АОР), который широко известен под английским наименованием «Hazard and operability studies» (HAZOP).

Метод применяется для тщательного систематического анализа опасностей технологического процесса на предмет того, могут ли отклонения от регламентных режимов привести к *нежелательным последствиям*.

Изначально подразумевалось, что этот метод будет направлен на исследование работоспособности различных установок и идентификацию отклонений от ожидаемого в нормальных условиях результата путем идентификации причин отклонений, защит и нежелательных последствий в случае реализации отклонений. Изначальный замысел метода описан Гербертом Лоули в публикации 1974 г. [4]. Для анализа опасностей Герберт Лоули подразумевал применение другого метода — дерево отказов или древовидную логическую схему [4]. Национальный стандарт<sup>2</sup> раскрывает метод в части идентификации потенциальных отклонений от целей проекта. В соответствии с национальным стандартом<sup>3</sup> цель проекта — это диапазон возможных значений характеристик состояния элементов системы, заданный или установленный в соответствии с требованиями проектировщиков. Примерами отклонений

от целей проекта могут быть отклонения в области производства продукции определенного качества и заданного объема в установленные сроки в рамках ограниченных финансовых и трудовых ресурсов.

С другой стороны, методические основы<sup>4</sup> позиционируют метод, как метод анализа опасностей технологических процессов для опасных производственных объектов (ОПО). При анализе опасностей технологических процессов приоритет отдается исследованию нежелательных последствий и их причин для людей и окружающей среды в случае аварии. В ходе анализа с помощью таблиц и технологических схем рассматривается каждый технологический узел по очереди на предмет потенциально опасных отклонений в технологическом процессе, которые формулируются на основании набора заранее установленных ключевых слов, а также составляется перечень потенциальных причин и последствий отклонения существующих мер защиты. По итогам проведенного анализа рабочая группа, состоящая из высококвалифицированных специалистов, основываясь на рабочем опыте и знаниях, экспертно разрабатывает рекомендации (дополнительные меры защиты), направленные на предупреждение возникновения отклонений или на смягчение последствий при их реализации.

В статье представлены становление и развитие метода «Анализ опасности и работоспособности» как метода анализа риска аварий.

## 1. Создание метода «Критического анализа» (1960–1970 гг.)

Основы методологии анализа опасности и работоспособности были разработаны британской компанией «Imperial Chemical industries» (ICI). В 1963 г. подразделение тяжелых органических химикатов (Heavy Organic Chemicals Division, НОС) компании ICI проектировало установку по производству фенола и ацетона кумольным методом. В это время было популярно изучение метода критического анализа «Critical examination». Критический анализ — это формальный метод изучения деятельности и выработки альтернатив путем постановки вопросов: «Что достигнуто?», «Чего еще можно достичь?», «Чего следует достичь?», «Как это

<sup>1</sup> Приказ Ростехнадзора от 03.11.2022 № 387 «Об утверждении Руководства по безопасности «Методические основы анализа опасностей и оценки риска аварий на опасных производственных объектах».

<sup>2</sup> BS EN 61882:2016, Hazard and Operability Studies (HAZOP Studies) –Application guide.

<sup>3</sup> Там же.

<sup>4</sup> Приказ Ростехнадзора от 03.11.2022 № 387 «Об утверждении Руководства по безопасности «Методические основы анализа опасностей и оценки риска аварий на опасных производственных объектах».

достигается?» и так далее. Руководитель проекта решил посмотреть, возможно ли провести критический анализ проекта завода по производству фенола и ацетона, чтобы выявить любые недостатки в проекте и найти наиболее эффективный способ потратить любые дополнительные денежные ресурсы, которые могут быть доступны. Была назначена команда из трех человек: два специалиста по вводу в эксплуатацию и эксперт по критическому анализу. В 1964 г. они встречались три полных дня в неделю в течение четырех месяцев, изучая технологические схемы завода по производству фенола и ацетона и исписывая акры бумаги вопросами и ответами. Они обнаружили множество потенциальных опасностей и эксплуатационных проблем, которые не были предусмотрены проектом, и разработали подход, который узнаваемо напоминал метод HAZOP в том виде, в котором мы его знаем сегодня, хотя и был изменен в ходе более поздних исследований. За несколько месяцев до того, как исследование критического анализа установки по производству фенола и ацетона было проведено в подразделении ICI НОС в Биллингеме, подразделение ICI Mond в Ранкорне провело аналогичное, но гораздо более короткое исследование на техническом заводе. Это заняло у команды из четырех человек 21 час, что составляет сороковую часть времени, затраченного на специальное исследование в подразделении НОС. Данный подход позволил подразделению Mond заявить о себе как о первом в этой области [5].

Позднее подразделение Mond интегрировало HAZOP в шестиэтапную программу изучения опасностей, которая была утверждена во всей ICI и применяется от ранних стадий проектирования до завершения ввода в эксплуатацию [5, 6].

## 2. Синтез метода «Анализ опасности и работоспособности» (1970–2000 гг.)

Метод критического анализа был дополнительно усовершенствован внутри ICI и опубликован Гербертом Лоули в апреле 1974 г. под названием «Исследование работоспособности и анализ опасности» (Operability studies and hazard analysis) [4]. В своей публикации Герберт Лоули продемонстрировал описание двух методов, направленных на повышение безопасности и надежности производственных объектов.

Первый метод под наименованием «Исследование работоспособности» (Operability studies) представляет

классический HAZOP, который используется и по сей день. Этот метод был описан на примере установки димеризации олефинов. Были обозначены значения ключевых слов, формат рабочей таблицы с исследуемыми отклонениями от регламентных режимов и порядок проведения собраний по заполнению и проверке подготовленных рабочих таблиц. Герберт Лоули в своей работе делал акцент на том, что метод построен по принципу «проблема может возникнуть только при наличии отклонения от ожидаемого в нормальных условиях результата», и направлен на идентификацию отклонений, связанных с эксплуатацией установок, надежностью и безопасностью оборудования.

Второй метод под наименованием «Анализ опасности» (Hazard analysis) представляет дерево отказов или древовидную логическую схему, охватывающую события или совпадение случайностей, способных привести к конкретной опасности, которая затем получает количественную оценку в виде определения частоты реализации каждого события (отказа).

Дальнейшее развитие метода Operability studies привело к изменению его названия. Сейчас широко известно наименование «Hazard and operability studies» (HAZOP). В России HAZOP называется «Анализ опасности и работоспособности» (АОР). Стоит отметить, что в основу метода HAZOP заложена методология методов критического анализа «Critical examination», применяемого ICI в 60-х годах, и исследования работоспособности «Operability studies», которое описал Герберт Лоули. Метод анализа опасности «Hazard analysis» на сегодняшний день представляет собой метод анализа дерева отказов (FTA).

После аварии, произошедшей 1 июня 1974 г. на заводе «Нурго» во Фликсборо<sup>5</sup> [7], метод HAZOP стал все более широко применяться для анализа опасностей технологических процессов. Эта авария вызвала большой резонанс в мире, и в 1977 г. ICI совместно с Ассоциацией химической промышленности (Chemical Industries Association, CIA) выпустили первое руководство по методу HAZOP<sup>6</sup>. В руководстве делается акцент на том, что метод направлен на систематическое стимулирование творческого мышления проектировщиков,

<sup>5</sup> Ministry of the Environment - DPPR / SEI / BARPI, Catastrophic explosion of a cyclohexane cloud June 1, 1974 Flixborough United Kingdom, № 5611.

<sup>6</sup> Chemical Industries Association, A Guide to Hazard and Operability Studies, 1977, UK (London).

чтобы они могли идентифицировать потенциальные опасности в проекте, которые могут привести к повреждению оборудования, травмам персонала или убыткам.

Дальнейшее развитие метода связано с работами института инженеров-химиков IChemE и Тревора Ашера Клетца [8, 9], а также с исследованиями американского института инженеров-химиков (American Institute of Chemical Engineers, AIChE) и центра безопасности химических процессов ССРС, который был создан AIChE в 1985 г. после химических катастроф в Севезо, Мехико и Бхопале. В 1985 г. было выпущено первое руководство по процедурам оценки опасности. В нем было представлено подробное описание качественных и количественных методов анализа риска, включая метод HAZOP [10]. Обновленное издание этой работы вышло в 2008 г. [11].

В Российских публикациях и методических указаниях подчеркивается, что метод используется для исследования влияния отклонений технологических параметров от регламентных режимов с точки зрения возникновения опасности и позволяет проводить идентификацию и ранжирование опасностей, а также выявлять неясности и неточности в инструкциях по безопасности, способствуя их дальнейшему совершенствованию.

### 3. Формализация метода «Анализ опасности и работоспособности» в России и за рубежом (2000–2024 гг.)

Первые описания метода «Анализ опасности и работоспособности» в России начали появляться в практическом руководстве по предупреждению крупных аварий [12], в методических указаниях по проведению анализа риска опасных промышленных объектов, утвержденных Госгортехнадзором России 12 июля 1996 г. [13], а также в ряде статей, посвященных оценке риска и анализу деклараций безопасности промышленных объектов [14, 15].

Спустя 22 года после публикации первого руководства<sup>7</sup>, было принято решение о написании нового руководства с использованием передовых практик на основе накопленного опыта за этот период как положительного, так и негативного. В подготовке приняла участие в общей сложности 31 компания,

<sup>7</sup> Chemical Industries Association, A Guide to Hazard and Operability Studies, 1977, UK (London).

и в 2000 г. было опубликовано новое руководство по «Аналізу опасности и работоспособности», как совместный проект IChemE, CIA и Европейского центра безопасности технологических процессов (European Process Safety Centre, далее — EPSC) [16]. Расширенное третье издание этой работы вышло в 2015 г. [17]. Руководство детализировало описание метода в части организации и проведения сессий HAZOP. В публикации IChemE 2022 г. представлено подробное описание деятельности лидера исследования HAZOP [18].

В 2001 г. выходит первый британский стандарт, посвященный «Аналізу опасности и работоспособности»<sup>8</sup>, а в 2016 г. публикуется его обновленная версия<sup>9</sup>.

В России в настоящее время описание метода HAZOP представлено в национальном стандарте ГОСТ Р 27.012-2019<sup>10</sup>, который по сути является переводом британского стандарта<sup>11</sup>. Национальный стандарт раскрывает метод в части идентификации потенциальных отклонений от целей проекта, экспертизы возможных причин и оценки их последствий, что также означает поиск ошибок и неточностей в установленных требованиях проектировщиков для их дальнейшего недопущения на этапе эксплуатации. Использование этого стандарта для анализа риска аварий на производственных объектах малоэффективно ввиду его направленности на достижение целей проекта.

Другое описание метода HAZOP представлено в Руководстве по безопасности, утвержденном приказом Ростехнадзора от 03.11.2022 № 387<sup>12</sup> (Методические основы). Методические основы позиционируют метод, как метод анализа опасностей технологических процессов для опасных производственных объектов (ОПО). В методических основах метод именуется как «Анализ опасности и работоспособности» (АОР). Здесь

<sup>8</sup> BS IEC 61882:2001, Hazard and Operability Studies (HAZOP Studies) – Application guide.

<sup>9</sup> BS EN 61882:2016, Hazard and Operability Studies (HAZOP Studies) – Application guide.

<sup>10</sup> ГОСТ Р 27.012-2019 (МЭК 61882:2016) «Надежность в технике. Анализ опасности и работоспособности (HAZOP)».

<sup>11</sup> BS EN 61882:2016, Hazard and Operability Studies (HAZOP Studies) – Application guide.

<sup>12</sup> Приказ Ростехнадзора от 03.11.2022 № 387 «Об утверждении Руководства по безопасности «Методические основы анализа опасности и оценки риска аварий на опасных производственных объектах».

метод позиционируется как один из методов анализа риска аварий на опасных производственных объектах и практически не применим для анализа возможных отклонений от целей проекта.

Практически в разных документах для решения принципиально различающихся задач даются рекомендации по применению метода, имеющего одинаковое название «Анализ опасности и работоспособности». И хотя общий подход к выявлению отклонений является общим, практическое применение этого подхода к решению разных задач имеет существенные различия и желательно избежать путаницы при выборе рекомендаций.

На сегодняшний день метод HAZOP активно модернизируется и развивается. К примеру, в руководстве 2021 г. представлен метод «Delta HAZOP», предназначенный для проверки и уточнения результатов проведенного исследования классического HAZOP в случае внедрения изменений в проект или эксплуатирующийся объект<sup>13</sup>.

#### 4. Ограничения, возможности и перспективы

Несмотря на то, что метод АОР в действительности является отличным методом, который способен исследовать отклонения технологических параметров от регламентных и разрабатывать меры по их недопущению или смягчению последствий при их реализации, на сегодняшний день существует соблазн позиционировать его как полноценный метод анализа риска аварий, включающий в себя оценку риска. Однако метод АОР не применяется для количественной оценки риска аварий (к примеру, расчет ожидаемого количества погибших в случае аварии), также метод АОР не способен исследовать полный перечень возможных причин аварий и инцидентов. Метод АОР ограничен в анализе работоспособности оборудования, поскольку в рамках метода АОР не осуществляется полноценное исследование опасностей отказов технических устройств — для подобных исследований существуют другие методы, к примеру «Анализ видов и последствий отказов» (Failure modes and effects analysis, FMEA), «Анализ видов, последствий и критичности отказов» (Failure mode, effects, and criticality analysis, FMECA) [19].

<sup>13</sup> IChemE Safety Centre Guidance «Effective revalidation of risk assessments, Delta HAZOP», 2021.

Для проведения полного анализа риска аварий, включающего идентификацию других опасностей и оценку риска, необходимо дополнение метода специальными инструментами или привлечение других методов анализа риска. К примеру, результаты метода АОР можно использовать в методе «Анализ слоев защиты» (LOPA). Метод «Анализ слоев защиты» позволяет обосновать рекомендации, разработанные в ходе проведения собраний метода АОР, с точки зрения снижения вероятности реализации рассматриваемого сценария при внедрении рекомендуемых мер защиты.

#### Заключение

В основу методологии HAZOP заложены характеристики двух методов — критического анализа «Critical examination», применяемого ICI в 60-х годах, и исследования работоспособности «Operability studies», описанного Гербертом Лоули в 1974 г. [4]. «Анализ опасности» (Hazard analysis) описывался Гербертом Лоули как отдельный количественный метод, который в настоящее время сформировался как метод «Анализ дерева отказов».

HAZOP является эффективным инструментом для идентификации опасностей и проблем с работоспособностью, связанных с отклонениями технологического процесса от регламентных режимов работы в части выявления причин отклонений и возможных мер защиты.

Однако метод HAZOP имеет ряд ограничений, что не позволяет позиционировать его как полноценный метод анализа риска аварий, включающий в себя оценку риска.

Для проведения полного анализа риска аварий, включающего идентификацию других опасностей и оценку риска, необходимо дополнение метода специальными инструментами или привлечение других методов анализа риска.

В России на сегодняшний день метод АОР используется для анализа двух разных направлений — работоспособности в соответствии с Национальным стандартом<sup>14</sup> и опасностей в соответствии с Методическими основами<sup>15</sup>.

<sup>14</sup> ГОСТ Р 27.012-2019 (МЭК 61882:2016) «Надежность в технике. Анализ опасности и работоспособности (HAZOP)».

<sup>15</sup> Приказ Ростехнадзора от 03.11.2022 № 387 «Об утверждении Руководства по безопасности «Методические основы анализа опасностей и оценки риска аварий на опасных производственных объектах».

## Список источников [References]

1. F. Crawley, *A Guide to Hazard Identification Methods*, 2nd Edition April 21, 2020, ISBN: 978-0-12-819543-7
2. *Process Safety for Engineers An Introduction* / Center for Chemical Process Safety, 2022, 560 p. ISBN: 978-1-11983-098-6
3. Быков А. А. Методологические и прикладные основы управления рисками предприятия и безопасностью населения и окружающей среды: моногр. / А. А. Быков, В. Э. Зайковский; под общ. ред. чл.-кор. РАН Н. А. Махутова. Изд-во Томск. гос. ун-та систем упр. и радиоэлектроники, 2022. 617 с. ISBN 978-5-86889-954-6 [Bykov A. A. Methodological and applied foundations of enterprise risk management and public and environmental safety: monogr. / A. A. Bykov, V. E. Zaikovsky; by. ed. Corr. Member of RAS N. A. Makhutov. Publishing House Tomsk. State University of Control Systems and Electronics, 2022. 617 p. ISBN 978-5-86889-954-6. (In Russ.)]
4. Lawley H. G. *Operability Studies and Hazard Analysis* // *Chemical Engineering Progress*. 1974;70(4):45–56
5. Kletz T. A. *Hazop — past and future* // *Reliability Engineering and System Safety*. 1997;55(3):263–266
6. Turney R. D. *Designing plants for 1990 and beyond* // *Process Safety and Environmental Protection*. 1990;68:12–16
7. Маршалл В. Основные опасности химических производств: пер. с англ. Г. Б. Барсамьяна и др.; под ред. Б. Б. Чайванова, А. Н. Черноплекова. М.: Мир. 1989. 671 с. ISBN 5-03-000990-6 [Marshall V. The main dangers of chemical production: trans. From English G. B. Barsamyan et al.; ed. B. B. Chaivanov, A. N. Chernoplekov. M.: Mir. 1989. — 671 p. ISBN 5-03-000990-6]
8. Kletz T. A. *HAZOP and HAZAN: notes on the Identification and Assessment of hazards*, Institution of Chemical Engineers, Rugby. 1983. 81 p. ISBN 0-85295-165-5
9. Kletz T. A. *HAZOP and HAZAN* 4th ed Taylor & Francis. 1999. 232 p. ISBN 0-85295-421-2
10. Publication of the Center for Chemical Process Safety of the American Institute of Chemical Engineers and John Wiley & Sons, *Guidelines for Hazard Evaluation Procedures*, 1st Edition, 1985
11. Publication of the Center for Chemical Process Safety of the American Institute of Chemical Engineers and John Wiley & Sons, *Guidelines for Hazard Evaluation Procedures*, 3rd Edition, 2008, ISBN 978-0-471-97815-2
12. *Предупреждение крупных аварий: практическое руководство* / ред. Э. В. Петросянц, пер. с англ. М.; Женева: МП Парог; Междунар. бюро труда. 1992. 256 с. [Prevention of major accidents: a practical guide / ed. E. V. Petrosyants. Trans./from English M. Geneva: MP Parog; International labor bureau. 1992. 256 p.]
13. Дадонов Ю. А., Решетов А. С., Ефименко В. И., Мартынюк В. Ф. и др. РД 08-120-96. Методические указания по проведению анализа риска опасных промышленных объектов: Утв. постановлением Госгортехнадзора России от 12.07.1996 № 29 // *Безопасность труда в промышленности*. 1997. № 2. С. 46–56 [Dadonov Yu. A., Reshetov A. S., Efimenko V. I., Martynyuk V. F. [et al.] RD 08-120-96. Methodological Guidelines for Conducting Risk Analysis of Hazardous Industrial Facilities: Approved by Decree of Gosgortekhnadzor of Russia dated 12.07.1996 No. 29 // *Occupational Safety in Industry*. 1997;(2):46–56. (In Russ.)]
14. Мартынюк В. Ф., Печеркин А. С., Разумов В. П. и др. Анализ деклараций безопасности промышленных объектов Москвы // *Безопасность труда в промышленности*. 1995. № 10. С. 32–38 [Martynyuk V. F., Pecherkin A. S., Razumov V. P. et al. Analysis of safety declarations for industrial facilities in Moscow // *Occupational Safety in Industry*. 1995;(10):32–38. (In Russ.)]
15. Мартынюк В. Ф., Лисанов М. В., Кловач Е. В., Сидоров В. И. Анализ риска и его нормативное обеспечение // *Безопасность труда в промышленности*. 1995. № 11. С. 55–62 [Martynyuk V. F., Lisanov M. V., Klovach E. V., Sidorov V. I. Risk analysis and its regulatory support // *Occupational Safety in Industry*. 1995;(11):55–62. (In Russ.)]
16. F. Crawley, M. Preston and B. Tyler *HAZOP: Guide to Best Practice: Guidelines to Best Practice for the Process and Chemical Industries* / Institution of Chemical Engineers, Rugby, UK. 2000, 108 p. ISBN 0-85295-427-1
17. F. Crawley, B. Tyler *HAZOP Guide to Best Practice: 3rd edit.*, / Elsevier. 2015, 168 p. ISBN: 978-0-323-39460-4
18. Phil Eames *The HAZOP Leader's Handbook: How to Plan and Conduct Successful HAZOP Studies: 1st Edition* / Institution of Chemical Engineers, *Chemical Engineering Process Simulation*. 2022. 262 p. ISBN 978-0-323-91726-1
19. Дроняев О. И., Мартынюк В. Ф. О применении метода «Анализ опасности и работоспособности» при анализе риска аварий на производственных объектах // *Безопасность жизнедеятельности*. 2023. № 11. С. 41–47 [Dronyaev O. I., Martynyuk V. Ph. On the application of the method “HAZARD and operability studies” in the analysis of the risk of accidents at production facilities // *Life Safety*. 2023;(11):41–47. (In Russ.)]

## Сведения об авторах

**Дроняев Олег Игоревич:** аспирант, РГУ нефти и газа (НИУ) имени И. М. Губкина

Количество публикаций: 2

Область научных интересов: управление рисками, системный анализ и моделирование

*Контактная информация:*

Адрес: 119991, г. Москва, проспект Ленинский, д. 65, корп. 1  
oluganato555@gmail.com

**Мартынюк Василий Филиппович:** доктор технических наук, профессор, РГУ нефти и газа (НИУ) имени И. М. Губкина  
Количество публикаций: 150

Область научных интересов: теория горения и взрыва, управление рисками, системный анализ и моделирование, обоснование безопасности машин и оборудования

SPIN-код: 9365-1781

*Контактная информация:*

Адрес: 119991, г. Москва, проспект Ленинский, д. 65, корп. 1  
bio-mart@yandex.ru

---

Статья поступила в редакцию: 06.11.2024

Одобрена после рецензирования: 22.12.2024

Принята к публикации: 22.01.2025

Дата публикации: 28.02.2025

*The article was submitted: 06.11.2024*

*Approved after reviewing: 22.12.2024*

*Accepted for publication: 22.01.2025*

*Date of publication: 28.02.2025*

УДК 502.3  
Научная специальность: 2.10.2  
<https://elibrary.ru/awskpp>

ISSN 1812-5220  
© Проблемы анализа риска, 2025

# Управление экологическим воздействием нефтегазового бизнеса на атмосферный воздух (на примере деятельности ПАО «НК «РОСНЕФТЬ» за 2012–2023 годы)

**Трубицина О.П.,**

Северный (Арктический) федеральный университет имени М.В. Ломоносова, 163002, Россия, г. Архангельск, набережная Северной Двины, 17

**Башкин В.Н.\*,**

Институт физико-химических и биологических проблем почвоведения РАН, 142292, Россия, Московская обл., г. Пущино, ул. Институтская, д. 2-2

## Аннотация

В статье рассмотрены вопросы управления воздействием нефтегазового бизнеса на атмосферный воздух на примере деятельности ПАО «НК «РОСНЕФТЬ» (далее — «Роснефть») за 2012–2023 гг. Исследование проводилось на основе данных о валовых и удельных выбросах в атмосферу из утвержденных отчетов в области устойчивого развития компании «Роснефть». Динамика валовых выбросов вредных веществ в целом имеет тенденцию к незначительному снижению при росте показателей валовых выбросов  $\text{SO}_2$  и  $\text{NO}_x$ . В то же время динамика удельных выбросов  $\text{SO}_2$  и  $\text{NO}_x$  растет в меньшей степени. Компании «Роснефть» следует повысить информационную прозрачность в области затрат на мероприятия по минимизации воздействия на атмосферный воздух и стремиться к дальнейшему повышению эффективности реализации Концепции охраны окружающей среды.

**Ключевые слова:** управление экологическим воздействием; выбросы загрязняющих веществ; атмосферный воздух; нефтегазодобывающая промышленность.

**Для цитирования:** Трубицина О.П., Башкин В.Н. Управление экологическим воздействием нефтегазового бизнеса на атмосферный воздух (на примере деятельности ПАО «НК «РОСНЕФТЬ» за 2012–2023 годы) // Проблемы анализа риска. 2025. Т. 22. № 1. С. 54–61. — EDN: AWSKPP

Авторы заявляют об отсутствии конфликта интересов

# Management of Environmental Impact on Atmospheric Air by the Oil and Gas Business (on the Example of the Activities of PJSC OC «ROSNEFT» for 2012–2023)

**Olga P. Trubitsina,**

Northern (Arctic) Federal University,  
Severnaya Dvina nab., 17,  
Arkhangelsk, 163002, Russia

**Vladimir N. Bashkin\***,

Institute of Physicochemical and Biological Problems in Soil Science RAS,  
Institutskaya str., 2-2,  
Pushchino, Moscow region,  
142290, Russia

## Abstract

The article considers the issues of managing the impact of the oil and gas business on the atmosphere using the example of the activities of PJSC NK ROSNEFT (hereinafter referred to as Rosneft) for 2012–2023. The study was conducted based on data on gross and specific emissions into the atmosphere from the approved reports on sustainable development of Rosneft. The dynamics of gross emissions of harmful substances in general tend to slightly decrease with an increase in the indicators of gross emissions of SO<sub>2</sub> and NO<sub>x</sub>. At the same time, the dynamics of specific emissions of SO<sub>2</sub> and NO<sub>x</sub> grows to a lesser extent. Rosneft should increase information transparency in the area of costs for measures to minimize the impact on the atmosphere and strive to further improve the efficiency of the implementation of the Environmental Protection Concept.

**Keywords:** environmental impact management; emissions of pollutants; atmospheric air; oil and gas industry.

**For citation:** Trubitsina O.P., Bashkin V.N. Management of environmental impact on atmospheric air by the oil and gas business (on the example of the activities of PJSC OC «ROSNEFT» for 2012-2023) // Issues of Risk Analysis. 2025;22(1):54-61. (In Russ.). — EDN: AWSKPP

**The authors declare no conflict of interest**

## Содержание

Введение

1. Стратегия компании «Роснефть»: показатели сокращения выбросов в атмосферу
2. Динамика выбросов вредных веществ в атмосферу от деятельности компании «Роснефть»

Заключение

Список источников

## Введение

В условиях новых экономических и геополитических вызовов в 2023 г. нефтегазовые компании продолжили держать ориентир на устойчивое развитие. Это позволило авторам проанализировать часть целевых показателей стратегии, связанных с таким направлением, как реализация соответствующих стратегических задач и мероприятий, направленных на снижение выбросов в атмосферный воздух. За основу взяты экологические цели компании «Роснефть» и реализация соответствующих показателей, установленных в ее Концепции экологического развития на период до 2035 г. [1].

Исследование проводилось с использованием данных о валовых и удельных выбросах в атмосферный воздух из Отчетов в области устойчивого развития компании «Роснефть» [2–13], которая согласно предыдущим исследованиям авторов [14, 15] занимала лидирующие позиции в рейтинге экологической ответственности (РЭО) в период 2014–2022 гг. как начального, так и финального года реализации рейтинга. При этом анализ распределения ее рейтинговых баллов по трем разделам РЭО выявил наибольшую долю показателей в секторе управления (54%) при наименьшей информационной открытости (16%). Треть показателей принадлежит операционному сектору (30%). Это отличает «Роснефть» от иных компаний-лидеров с примерно равным соотношением долей реализации рейтинговых показателей по разделам [14].

В 2023 г. компания [13] восьмой раз подряд вошла в число лидеров российских фондовых индексов ESG, включая индексы Московской биржи — РСПП «Общественность и открытость» и «Вектор устойчивого развития». Кроме того компания попала в Индекс Московской биржи — RAEX «ESG-сбалансированный», стала лучшей российской нефтегазовой компанией в международном рейтинге World Benchmarking Alliance в области устойчивого развития, предоставила инициативе Глобального договора ООН ежегодный отчет о достигнутом прогрессе с учетом лучших практик.

Анализ выбранной компании интересен еще и тем, что ее хозяйственная деятельность осуществляется, в том числе, в Арктической зоне Российской Федерации (АЗРФ). Управление устойчивым развитием территории можно признать эффективным при балансе затрат на природоохранные мероприятия и сокращении отрицательного воздействия на природную

среду. Так, согласно исследованию эффективности управления устойчивым развитием Арктики [16] выявлена отрицательная зависимость между объемом текущих затрат на охрану окружающей среды в АЗРФ за период 2017–2021 гг. и показателем, характеризующим очистку атмосферы ( $k = -0,92$ ), в отличие от объемов очищенных сточных вод ( $k = 0,68$ ) и повторно использованных и утилизированных отходов ( $k = 0,77$ ). Таким образом, управление экологическим воздействием на атмосферный воздух нельзя считать эффективным и результативным на территории АЗРФ, что ориентирует на исследование этого вопроса в рамках отдельных компаний, осуществляющих свою деятельность в АЗРФ.

Учитывая вышесказанное, представляется актуальным проанализировать динамику выбросов загрязняющих веществ в атмосферный воздух с акцентом на кислотообразующие компоненты, в том числе в рамках реализации показателей Концепции экологического развития до 2035 г. компании «Роснефть».

## 1. Стратегия компании «Роснефть»: показатели сокращения выбросов в атмосферу

Долгосрочные цели компании в области охраны окружающей среды на период до 2035 г. включают минимизацию воздействия на окружающую среду за счет повышения эффективности утилизации отходов, рекультивации земель, очистки сточных вод и сокращения выбросов, а также внедрения и совершенствования принципов «экономики замкнутого цикла».

В рамках раскрытия существенных тем Глобальной инициативой по отчетности GRI-3 экономической результативности и инвестиционной привлекательности в ходе производственной деятельности выбросов в атмосферный воздух «Роснефть» реализует комплекс мер, предусматривающий реализацию инвестиционных проектов с экологическим эффектом, применение наиболее эффективного природоохранного оборудования, проведение инвентаризации источников выбросов и т.д.

Охрана атмосферного воздуха при реализации деятельности компании подразумевает осуществление мониторинга выбросов от производственных объектов и реализацию следующих мероприятий: внедрение системы контроля качества воздуха, установление стационарных постов наблюдений за качеством воздуха

на границах санитарно-защитных зон, оснащение передвижных экологических лабораторий современным оборудованием [13].

Основными показателями в области устойчивого развития с точки зрения выбросов загрязняющих веществ в атмосферу в соответствии с GRI 305–7, призванных помогать организовывать прозрачность и диалог между компаниями и всеми заинтересованными лицами (оксиды азота ( $\text{NO}_x$ ), оксиды серы ( $\text{SO}_x$ ) и другие значительные выбросы в атмосферу), являются:

- валовые выбросы в атмосферу загрязняющих веществ (тыс. т);
- удельные выбросы загрязняющих веществ от нефтегазодобычи (т/тыс. т у.т.);
- удельные выбросы загрязняющих веществ от нефтепереработки и нефтехимии (т/тыс. т у.т.).

Сокращение выбросов в атмосферу, помимо GRI, компания ориентируется на ГД ООН, принцип 9, IPЕСА, ENV-5 [13].

Концепция экологического развития компании на период до 2035 г. [1], принятая 26 февраля 2021 г., устанавливает следующие экологические показатели, связанные с воздействием на атмосферный воздух:

- снижение на 15% общего объема выбросов, не связанных с парниковыми газами;
- снижение на 15% выбросов двуокиси серы и оксидов азота.

Основным источником воздействия на атмосферный воздух от производственной деятельности Компании является утилизация попутного нефтяного газа (ПНГ) на факельных установках [7].

## 2. Динамика выбросов вредных веществ в атмосферу от деятельности компании «Роснефть»

### 2.1. Динамика валовых выбросов вредных веществ в атмосферу

Анализ динамики валовых выбросов вредных веществ в атмосферу за 2012–2023 гг. (рис. 1) позволил выявить спад их объемов, начиная с 2019 г., достигнув уровня 2012 г. в 2023 г. Предполагаем, что на подобную ситуацию косвенно повлияли внешние факторы в виде застоя экономики из-за пандемии коронавируса, пик которого пришелся на 2020 г.

Важно указать на то, что начало исследуемого периода характеризуется существенным ростом валовых выбросов в атмосферу по сравнению с предыдущими годами (2012 г. — 1359 тыс. т, 2010 г. — 925 тыс. т), что связано с быстрым ростом объемов нефтедобычи (2012 г. — 1231 тыс. т, 2010 г. — 783 тыс. т).

Наибольшее значение валовых выбросов приходится на 2017 г. в связи с включением в периметр новых активов, в том числе ПАО АНК «Башнефть», а также с началом активной разработки новых месторождений.

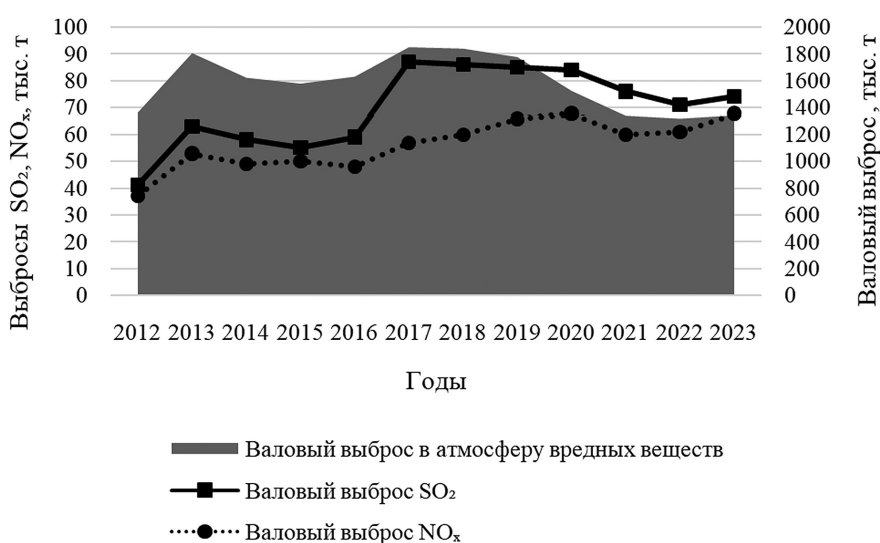


Рис. 1. Динамика валовых выбросов вредных веществ в атмосферу за 2012–2023 гг., тыс. т

Figure 1. Dynamics of gross harmful substances into the atmosphere in 2012–2023, thousand tonnes

Суммарный объем валовых выбросов в атмосферу загрязняющих веществ от производственной деятельности Компании в 2017 г. увеличился на 219 тыс. т. [7].

Таким образом, за исследуемый 12-летний период динамика валовых выбросов вредных веществ в атмосферу характеризуется тенденцией незначительного спада (на 1,6%). Однако динамика валовых выбросов SO<sub>2</sub> и NO<sub>x</sub> имеет устойчивую тенденцию к повышению (на 45% и 46%, соответственно).

При этом в рамках реализации Концепции экологического развития компании до 2035 г. динамика валовых выбросов вредных веществ в 2021–2023 гг. стремится к стабилизации (повышение на 0,2%). Изменение динамики выбросов SO<sub>2</sub> и NO<sub>x</sub> разнонаправлено: спад SO<sub>2</sub> на 2,6% и рост NO<sub>x</sub> на 11%.

### 2.2. Структура валовых выбросов вредных веществ в атмосферу

Структура валовых выбросов вредных веществ в атмосферу, рассчитанная по каждому компоненту как среднearифметическое значение валовых выбросов за 2012–2023 гг. (см. рис. 2).

Условно можно выделить три группы компонентов валовых выбросов в атмосферу, класс опасности которых увеличивается от первой группы к третьей при минимизации вклада в общие выбросы:

1. Макрокомпоненты: оксид углерода, летучие органические соединения (ЛОС), углеводороды (без ЛОС).
2. Мезокомпоненты: твердые вещества, диоксид серы, оксид азота.
3. Микрокомпоненты: бенз(а)пирен и прочие.

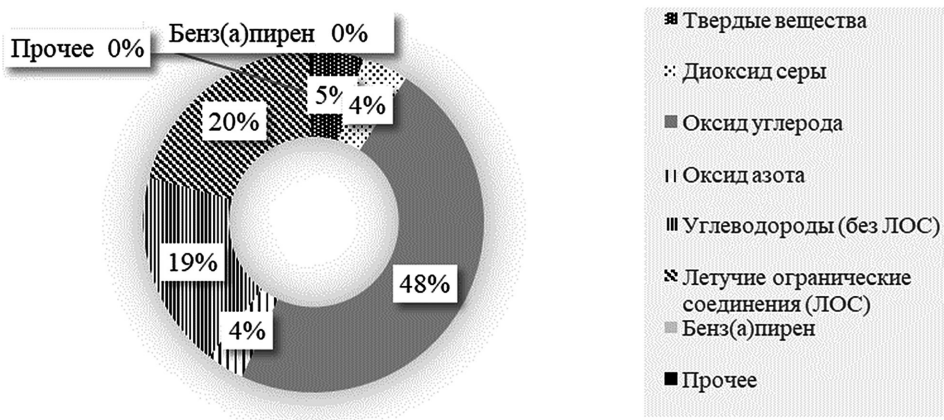


Рис. 2. Структура валовых выбросов в атмосферу вредных веществ за 2012–2023 гг., тыс. т

Figure 2. Structure of gross emissions of harmful substances into the atmosphere in 2012–2023, thousand tonnes

### 2.3. Динамика валовых и удельных выбросов SO<sub>2</sub> и NO<sub>x</sub>

Авторы делают акцент на кислотообразующие соединения в выбросах в атмосферу, провоцирующие закисление осадков и являющиеся предпосылками геоэкологического риска в районах реализации углеводородных проектов, особенно на территории Арктики [3].

Динамика валовых выбросов диоксида серы и оксида азота не всегда соответствует динамике валовых выбросов вредных веществ в целом (рис. 1). При их наименьших значениях в 2012 г. наибольшие значения отмечаются для диоксида серы в 2017 г. (как и валовых выбросов в целом), а для оксида азота — в 2020 г. и 2023 г. В то же время объем кислотообразующих компонентов в валовых выбросах после спада к 2021 г. увеличивается к 2023 г., в отличие от валовых выбросов в целом.

Удельные выбросы диоксида серы и оксида азота на тонну продукции компании характеризуются неравномерными изменениями в течение исследуемого периода (рис. 3). Наименьшие значения показателей обоих газов характерны для 2014–2015 гг., а наибольшие удельные выбросы диоксида серы — для 2017, 2023 гг. и оксида азота — для 2020 г.

Таким образом, динамика удельных выбросов SO<sub>2</sub> за 12-летний исследуемый период демонстрирует тенденцию роста (на 18%), обусловленного повышением показателей в нефтепереработке и нефтехимии (на 20%). При этом нефтегазодобыча характеризуется

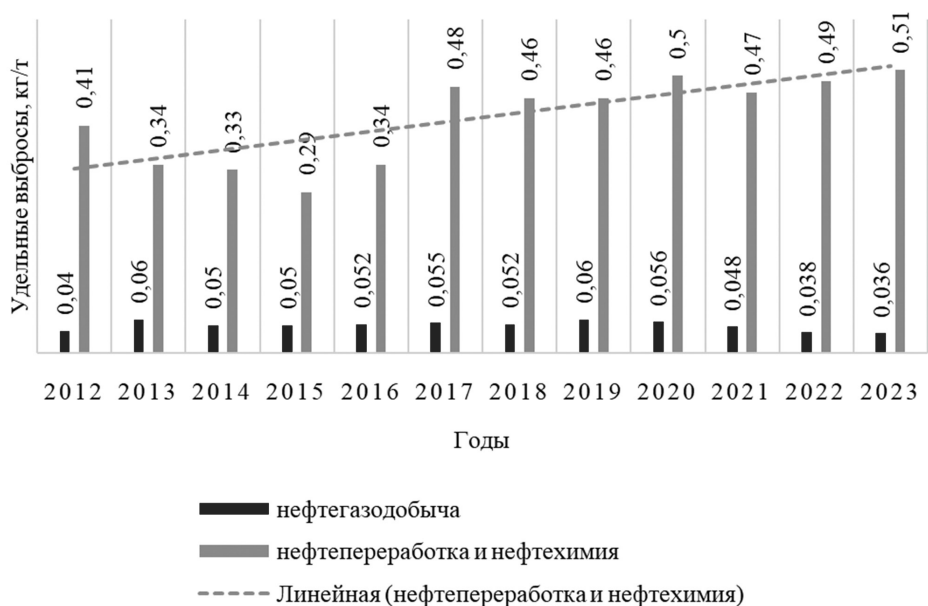


Рис. 3. Динамика удельных выбросов диоксида серы на тонну продукции компании, кг/т

Figure 3. Dynamics of specific sulfur dioxide emissions per ton of the company's products, kg/t

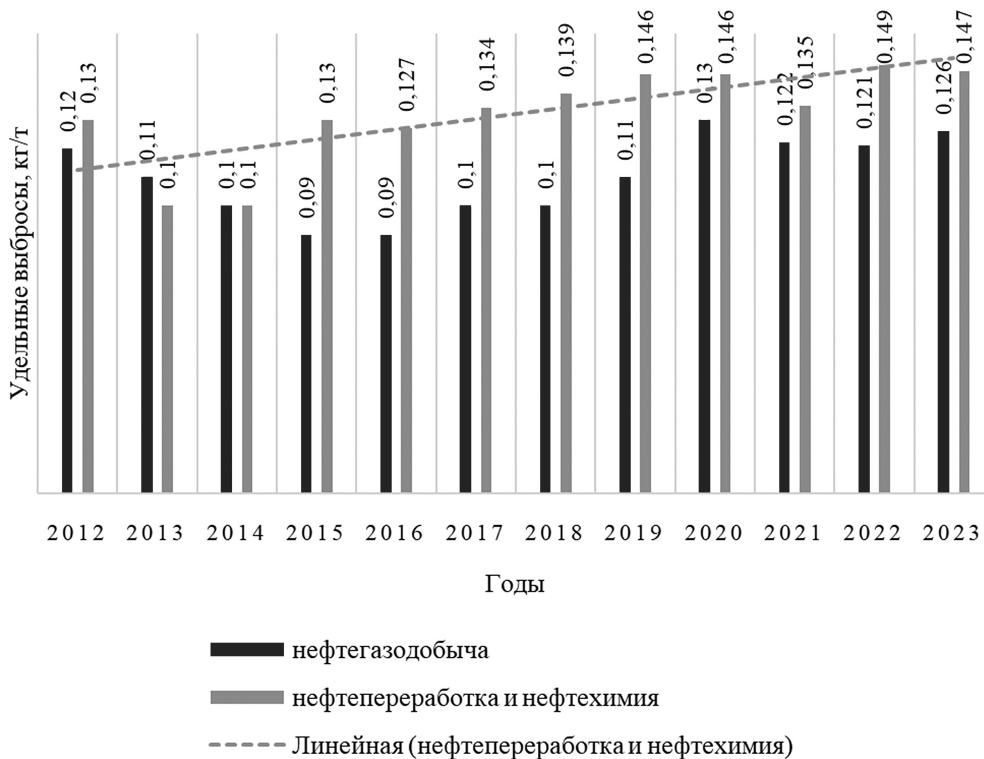


Рис. 4. Динамика удельных выбросов оксида азота на тонну продукции компании, кг/т

Figure 4. Dynamics of specific nitrogen oxide emissions per ton of the company's products, kg/t

**Таблица. Сравнительная характеристика динамики удельных выбросов SO<sub>2</sub> и NO<sub>x</sub> за периоды 2012–2023 гг. и 2021–2023 гг.**

*Table. Comparative characteristics of the dynamics of specific emissions of SO<sub>2</sub> and NO<sub>x</sub> for the periods 2012–2023 and 2021–2023*

Период	Динамика удельных выбросов SO <sub>2</sub> , %			Динамика удельных выбросов NO <sub>x</sub> , %		
	Всего	Нефтегазодобыча	Нефтепереработка и нефтехимия	Всего	Нефтегазодобыча	Нефтепереработка и нефтехимия
2012–2023 гг.	↑ 18%	↓ 10%	↑ 20%	↑ 8%	↓ 5%	↑ 12%
2021–2023 гг.	↑ 5%	↓ 25%	↑ 9%	↑ 6%	↓ 3%	↑ 8%

тенденцией спада (на 10%), обусловленной более трех последних лет реализацией Инвестиционной газовой программы, которая направлена на повышение уровня полезного использования ПНГ [13]. Динамика удельных выбросов NO<sub>x</sub> также показывает тенденцию к повышению (на 8%) за счет роста показателей в нефтепереработке и нефтехимии (на 12%). Показатели нефтегазодобычи отражают тенденцию спада (на 5%).

В годы реализации Концепции экологического развития до 2035 г. в период 2021–2023 гг. количественные показатели сократились, но направления динамики по сравнению с периодом 2012–2023 гг. не изменились (см. табл.).

### Заключение

1. Компания «Роснефть» занимает лидирующие позиции в рейтингах в области устойчивого развития.

2. За исследуемый период при незначительном спаде валовых выбросов вредных веществ в атмосферу от реализации углеводородных проектов компании выявлен рост валовых выбросов SO<sub>2</sub> и NO<sub>x</sub>. При этом в период реализации Концепции экологического развития компании до 2035 г. валовые выбросы SO<sub>2</sub> и NO<sub>x</sub> демонстрируют тенденцию спада и сокращения роста, соответственно.

3. Удельные выбросы SO<sub>2</sub> и NO<sub>x</sub> растут за счет показателей в нефтепереработке и нефтехимии на фоне их снижения в нефтегазодобыче.

4. Компании «Роснефть» следует повышать информационную открытость в области затрат на мероприятия по минимизации воздействия на атмосферный воздух и стремиться далее усиливать эффективность реализации Концепции экологического развития на период до 2035 г., особенно на территории АЗРФ.

### Список источников [References]

1. Концепция экологического развития на период до 2035 года [Электронный ресурс] URL: <https://www.rosneft.ru/Development/HealthSafetyandEnvironment/ecology/> [Rosneft's Environmental vision 2035 [Electronic resource] URL: <https://www.rosneft.ru/Development/HealthSafetyandEnvironment/ecology/> (In Russ.)]
2. Отчет ОАО «НК «Роснефть» в области устойчивого развития за 2012 год. Москва, 2012. 122 с. [Rosneft Sustainability Report 2012. Moscow, 2012. 122 p. (In Russ.)]
3. Отчет ОАО «НК «Роснефть» в области устойчивого развития. 2013. Москва, 2013. 141 с. [Rosneft Sustainability Report 2013. Moscow, 2013. 141 p. (In Russ.)]
4. Отчет ОАО «НК «Роснефть» в области устойчивого развития. 2014. Москва, 2014. 142 с. [Rosneft Sustainability Report 2014. Moscow, 2014. 142 p. (In Russ.)]
5. Роснефть. Отчет в области устойчивого развития за 2015 год. Москва, 2015. 140 с. [Rosneft Sustainability Report 2015. Moscow, 2015. 140 p. (In Russ.)]
6. Роснефть. Отчет в области устойчивого развития. 2016. Москва, 2016. 140 с. [Rosneft Sustainability Report 2016. Moscow, 2016. 140 p. (In Russ.)]
7. Роснефть. Отчет в области устойчивого развития за 2017 год. Москва, 2017. 152 с. [Rosneft Sustainability Report 2017. Moscow, 2017. 152 p. (In Russ.)]
8. ПАО «НК «Роснефть». Отчет в области устойчивого развития. 2018. Москва, 2018. 153 с. [Rosneft Sustainability Report 2018. Moscow, 2018. 153 p. (In Russ.)]
9. Отчет в области устойчивого развития. ПАО «НК «Роснефть». 2019. Москва, 2019. 233 с. [Rosneft Sustainability Report 2019. Moscow, 2019. 233 p. (In Russ.)]
10. Отчет в области устойчивого развития. ПАО «НК «Роснефть». 2020. Москва, 2020. 240 с. [Rosneft Sustainability Report 2020. Moscow, 2020. 240 p. (In Russ.)]

11. Отчет в области устойчивого развития. ПАО «НК «Роснефть». 2021. Москва, 2021. 256 с. [Rosneft Sustainability Report 2021. Moscow, 2021. 256 p. (In Russ.)]
12. ПАО «НК «Роснефть». Отчет в области устойчивого развития. 2022. Москва, 2022. 239 с. [Rosneft Sustainability Report 2022. Moscow, 2022. 239 p. (In Russ.)]
13. ПАО «НК «Роснефть». Отчет в области устойчивого развития 2023. Москва, 2023. 265 с. [Rosneft Sustainability Report 2023. Moscow, 2023. 265 p. (In Russ.)]
14. Трубицина О.П., Башкин В. Н. Экологическая ответственность нефтегазового бизнеса в Арктике: рейтинговый анализ за 2014–2022 годы // Проблемы анализа риска. 2023. Т. 20. № 6. С. 24–33.  
<https://doi.org/10.32686/1812-5220-2023-20-6-24-33>  
[Trubitsina O. P., Bashkin V. N. Environmental responsibility of the oil and gas business in the Arctic: rating analysis for 2014–2022 // Issues of Risk Analysis. 2023;20(6):24–33 (In Russ.).  
<https://doi.org/10.32686/1812-5220-2023-20-6-24-33>]
15. Bashkin V.N., Trubitsina O.P. Geocological and geopolitical risks for oil and gas industry in the Arctic: challenges v/v threats. Springer, ser. Environmental Pollution 2022, 29. 171 p. ISBN 978-3-030-95909-8 ISBN 978-3-030-95910-4 (eBook) <https://doi.org/10.1007/978-3-030-95910-4>
16. Самарина В.П., Скуфьина Т. П. Новые возможности и новые риски устойчивого развития российской Арктики в условиях климатических изменений // Арктика и Север. 2024. № 55. С. 72–96. <https://doi.org/10.37482/issn2221-2698.2024.55.72> [Samarina V. P., Skufina T. P. New opportunities and new risks for sustainable development of the in Russian Arctic in the context of Climate Change // Arctic and North. 2024;(55):72–96. (In Russ.)  
<https://doi.org/10.37482/issn2221-2698.2024.55.72>]

## Сведения об авторах

**Трубицина Ольга Петровна:** кандидат географических наук, доцент, доцент Федерального государственного автономного образовательного учреждения высшего образования «Северный (Арктический) федеральный университет имени М. В. Ломоносова» (САФУ имени М. В. Ломоносова)

Количество публикаций: более 100

Область научных интересов: геоэкологические риски, Арктика, нефтегазовая промышленность, экологический рейтинг, социальная ответственность бизнеса

Scopus Author ID: 57191332613

ORCID: 0000-0001-9847-9328

SPIN-код: 2534-2914

*Контактная информация:*

Адрес: 163002, г. Архангельск, набережная Северной Двины, 17  
test79@yandex.ru

**Башкин Владимир Николаевич:** доктор биологических наук, профессор, главный научный сотрудник Федерального государственного бюджетного учреждения науки Институт физико-химических и биологических проблем почвоведения РАН

Количество публикаций: более 400

Область научных интересов: геоэкологические риски, газовая промышленность, биогеохимия

ResearcherID: J 4621-2018

Scopus Author ID: 7005340339

SPIN-код: 2345-6161

*Контактная информация:*

Адрес: 142292, Московская обл., г. Пущино, ул. Институтская, д. 2-1, ИФХБПП РАН  
vladimirbashkin@yandex.ru

---

Статья поступила в редакцию: 25.11.2024

Одобрена после рецензирования: 12.12.2024

Принята к публикации: 19.12.2024

Дата публикации: 28.02.2025

*The article was submitted: 25.11.2024*

*Approved after reviewing: 12.12.2024*

*Accepted for publication: 19.12.2024*

*Date of publication: 28.02.2025*

УДК 550.341:551.515  
Научная специальность: 1.6.21  
<https://elibrary.ru/wwxyqq>

# Циклоническая активность тропических циклонов и некоторые ее особенности. Часть V. Сейсмическая реакция в ряде диапазонов магнитуд на многолетнюю циклоническую активность тропических ЦИКЛОНОВ

ISSN 1812-5220  
© Проблемы анализа риска, 2025

Ярошевич М.И.,  
Россия, г. Обнинск

## Аннотация

Рассчитаны многолетние годовые значения циклонической энергии тропических циклонов и годовые значения сейсмической энергии отдельно по землетрясениям нескольких диапазонов магнитуд. Расчеты проведены по обширной циклонической зоне северо-западной части Тихого океана. Выявлены определенные корреляционные связи между многолетними динамиками годовых значений циклонической энергии и годовых значений сейсмической энергии. Выявлены характеры тенденций развития многолетних рядов годовых значений циклонической и сейсмической энергии. На основании полученных результатов предложен гипотетический механизм возможного влияния циклонической активности на сейсмическую активность в двух разных диапазонах магнитуд.

**Ключевые слова:** тропические циклоны; энергия тропических циклонов; зона действия тропических циклонов; диапазоны магнитуд землетрясений; энергия землетрясений.

**Для цитирования:** Ярошевич М.И. Циклоническая активность тропических циклонов и некоторые ее особенности. Часть V. Сейсмическая реакция в ряде диапазонов магнитуд на многолетнюю циклоническую активность тропических циклонов // Проблемы анализа риска. 2025. Т. 22. № 1. С. 62–67. — EDN: WWXYQQ

Автор заявляет об отсутствии конфликта интересов.

# Cyclonic Activity of Tropical Cyclones and Some of its Features.

## Part V.

### Seismic Response in a Number of Magnitude Ranges to Long-Term Cyclonic Activity of Tropical Cyclones

Mikhail I. Yaroshevich,  
Obninsk, Russia

#### Abstract

Long-term annual values of the cyclonic energy of tropical cyclones and annual values of seismic energy were calculated separately for earthquakes of several magnitude ranges. Calculations were carried out over a vast cyclonic zone in the northwestern part of the Pacific Ocean. Certain correlations have been identified between long-term dynamics of annual values of cyclonic energy and annual values of seismic energy. The patterns of development trends in long-term series of annual values of cyclonic and seismic energies have been identified. Based on the results obtained, a hypothetical mechanism for the possible influence of cyclonic activity on seismic activity in two different magnitude ranges is proposed.

**Keywords:** tropical cyclones; tropical cyclone energy; tropical cyclone action area; earthquake magnitude ranges; earthquake energy.

**For citation:** Yaroshevich M.I. Some regularities of burst cyclone activity of tropical cyclones. Part V. Seismic response in a number of magnitude ranges to long-term cyclonic activity of tropical cyclones // *Issues of Risk Analysis*. 2024;22(1):62–67. (In Russ.). — EDN: WWXYQQ

**The author declares no conflict of interest.**

#### Содержание

Введение  
1. Расчетные эксперименты  
2. Обсуждения  
Заключение  
Список источников

## Введение

Северо-западная часть Тихого океана — зона очень высокой сейсмической и циклонической активности тропических циклонов. Здесь ежегодно возникает примерно 1000–1200 землетрясений разного уровня энергии и ежемесячно в среднем 30 тропических циклонов, из которых около половины — тайфуны (максимальная скорость ветра  $V_m \geq 33\text{ м/с}$ ). Среднесуточная энергия тайфуна оценивается величиной  $10^{18}$  Дж [1]. Таким образом, тайфун в среднем суммарно за время своего действия излучает энергию порядка  $10^{19}$  Дж. Это огромная энергия, соответствующая суммарной энергии почти 900 землетрясений магнитудой  $M = 7.5$ .

По меньшей мере, для рассматриваемого района достаточно свидетельств того, что тропические циклоны являются одним из факторов, влияющих на сейсмическую ситуацию в зоне действия тропических циклонов [2, 3, 7, 8]. Ранее были получены результаты расчетных экспериментов, в целом иллюстрирующие общий характер влияния циклонического фактора на общую сейсмичность в зоне высокой циклонической активности [7].

В представленной статье предпринята попытка несколько детальнее выявить влияние циклонической активности на сейсмическую активность в зависимости от рассматриваемого диапазона магнитуд и удаленностей гипоцентров землетрясений.

## 1. Расчетные эксперименты

Здесь исходной информацией в расчетных экспериментах служат тропические циклоны и землетрясения, произошедшие в обширной циклонической зоне северо-западной части Тихого океана ( $[(5-45)^\circ\text{N} - (115-175)^\circ\text{E}]$ ) в течение 1980–2015 гг.

Расчетными единицами в эксперименте являются годовые значения циклонической энергии ( $E_c$ ) и годовые значения сейсмической энергии ( $E_s$ ). Годовые значения сейсмической энергии рассматриваемых диапазонов магнитуд рассчитываются по данным сейсмологических бюллетеней «Геофизической службы РАН». Годовые значения циклонической энергии рассчитываются по неоднократно описанной модели [5, 6].

Циклоническая энергия по модели рассчитывается каждые 12 ч по Гринвичу по всей площади рассматриваемой циклонической зоны. Зона

поделена равномерно на несколько десятков равных квадратов размером  $5^\circ \times 5^\circ$ . Для каждого из этих квадратов рассчитывается суммарная энергия всех действующих в этот момент времени циклонов, в зависимости от расстояния до соответствующего циклона и максимальной скорости ветра циклона в это время. Сумма всех суперпозиций энергии квадратов и задает значение циклонической энергии в данный момент времени по всей площади. В году рассчитывается 730–732 таких значения, сумма которых в итоге и представляет соответствующее годовое значение циклонической энергии ( $E_c$ ). Сглаженная многолетняя динамика циклонической энергии за 1980–2015 гг. представлена на графике (см. рис. 1).

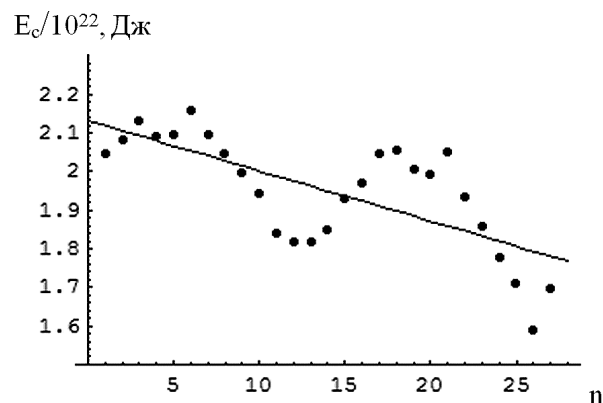


Рис. 1. Динамика сглаженных годовых значений циклонической энергии тропических циклонов, произошедших в 1980–2015 гг. (Сглаживание по 10 последовательным значениям;  $n$  — количество лет)

Figure 1. Dynamics of smoothed annual values of cyclonic energy of tropical cyclones that occurred in 1980–2015 (smoothing by 10 consecutive values;  $n$  = number of years)

Динамика характеризуется относительно многолетними усилениями и ослаблениями циклонической энергии и тенденцией к общему с годами ослаблению энергии. Динамика представлена регрессионным соотношением  $E_c / 10^{22} \text{ Дж} = 2.131 - 0.013 \times n$ .

Многолетняя динамика годовых значений сейсмической энергии, рассчитанных по всем землетрясениям всех магнитуд при условии, что глубина гипоцентров всех землетрясений  $H \leq 33$  км, показана на рис. 2. В этом случае наблюдается тенденция к общему нарастанию с годами сейсмической активности ( $E_s / 10^{17}$

Дж =  $1.038 + 0.11 \times n$ ). Коэффициент корреляции между динамикой циклонической энергии (рис. 1) и динамикой сейсмической энергии (рис. 2):  $r = -0.83^1$ .

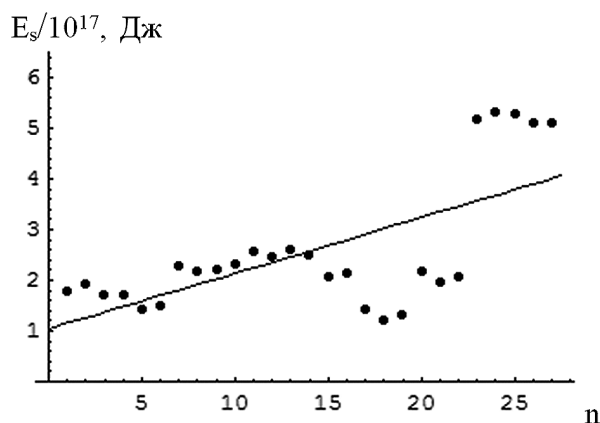


Рис. 2. Динамика сглаженных годовых значений сейсмической энергии за 1980–2015 гг. Расчеты по всем землетрясениям всех магнитуд и по значениям  $H \leq 33$  км. (Сглаживание по 10 последовательным значениям;  $n$  — количество лет)

Figure 2. Dynamics of smoothed annual values of seismic energy for 1980–2015. Calculations for all earthquakes all magnitudes and  $H$  values  $\leq 33$  km. (Smoothing by 10 consecutive values;  $n$  = number of years)

В следующем расчетном эксперименте рассматривались землетрясения диапазоном  $M \geq 6$ , но в двух вариантах: в одном только землетрясения с  $H \leq 33$  км, в другом — землетрясения с любыми значениями  $H$ . Результаты этого эксперимента приведены на рис. 3.

И здесь в обоих случаях в течение 1980–2015 гг. отмечено общее стремление к нарастанию сейсмической активности:  $E_s/10^{16}$  Дж =  $0.978 + 0.109 \times n$  (рис. 3а) и  $E_s/10^{16}$  Дж =  $6.165 + 0.086 \times n$  (рис. 3б). Существенно в этом варианте расчетов различаются коэффициенты корреляции между многолетними динамиками циклонической и сейсмической энергии. В случае, когда рассматриваются землетрясения с  $M \geq 6$  и ограниченные  $H \leq 33$  км, коэффициент корреляции  $r = -0.83$ , в случае же этого же диапазона землетрясения, но не ограниченные значением  $H$ ,  $r = -0.14$ . Это важное различие, на которое будет обращено внимание ниже.

<sup>1</sup> Учитывая уровень точности определения параметров тропических циклонов и землетрясений и расчетов соответствующих энергий, как кажется, коэффициент корреляции  $-0.83$  является достаточно высокой и достаточно достоверной оценкой соотношений динамик, приведенных на рис. 1, 2.

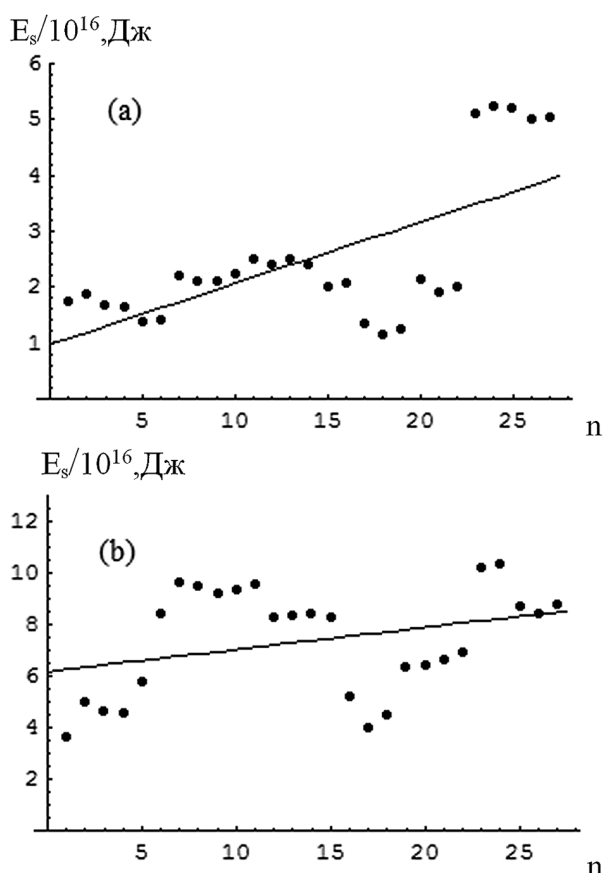


Рис. 3. Динамика сглаженных годовых значений сейсмической энергии за 1980–2015 гг.: (а) — все землетрясения  $M \geq 6$  с  $H \leq 33$  км; (б) — все землетрясения  $M \geq 6$  и неограниченно по значениям  $H$ .

Figure 3. Dynamics of smoothed annual values of seismic energy for 1980–2015 (a) — all earthquakes  $M \geq 6$  with  $H \leq 33$  km; (b) — all earthquakes  $M \geq 6$  and unlimited values of  $H$ .

В еще одном расчетном эксперименте определялась сглаженная многолетняя динамика сейсмической активности, рассчитанная по всем землетрясениям  $M \geq 7$  и по всем значениям  $H$  (см. рис. 4). Здесь общее многолетнее нарастание сейсмичности отражено регрессионным соотношением  $E_s/10^{16}$  Дж =  $5.136 + 0.075 \times n$ . В этом случае коэффициент корреляции между многолетними динамиками циклонической и сейсмической энергии  $r = -0.476$ .

Такой характер и уровень корреляции между многолетними динамиками циклонической и сейсмической энергии, вероятно, можно объяснить определенным своеобразным сочетанием сильных землетрясений ( $M \geq 7$ ), гипоцентры которых расположены и на глубинах  $H \leq 33$  км, и на глубинах  $H > 33$  км.

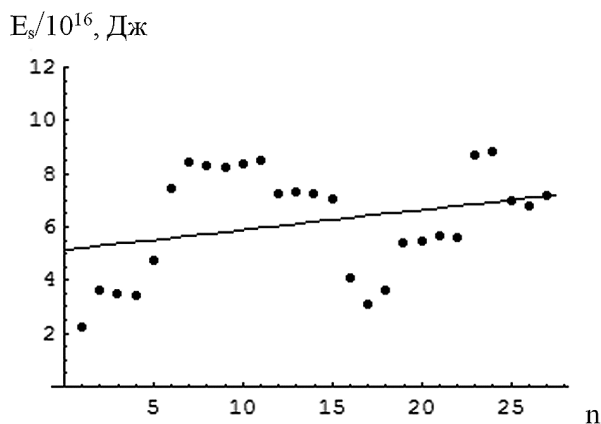


Рис. 4. Динамика сглаженных годовых значений сейсмической энергии за 1980–2015 гг. Все землетрясения  $M \geq 7$  по всем значениям  $N$

Figure 4. Dynamics of smoothed annual values of seismic energy for 1980–2015. All earthquakes  $M \geq 7$  for all values  $N$

## 2. Обсуждения

Вначале обратим внимание на случаи, когда многолетние ряды циклонической и сейсмической энергии связаны относительно высоким, по абсолютной величине, отрицательным коэффициентом корреляции (рис. 2 и рис. 3а). Эта ситуация свидетельствует о том, что при нескольких годах непрерывной сильной циклонической активности сейсмическая активность относительно низкая. И наоборот, при слабой циклонической активности сейсмическая активность относительно высокая. Казалось бы, логично предположить, что при сильной циклонической активности в твердые слои Земли «накачивается» и большая энергия, тем самым возбуждается большая сейсмичность. Сейчас, как кажется, объяснить эту парадоксальность можно лишь механизмом гипотетического характера.

Земная кора насыщена большим числом зон напряженностей. Напряженности по своей силе непрерывно меняются и непрерывно мигрируют. Если в результате миграции несколько зон напряженности объединяется, то может произойти среднее или сильное землетрясение. Для этого, правда, необходимо время, иногда довольно длительное.

Тропические циклоны обладают не только большой энергией, но и занимают большие площади. Кроме того, очень часто циклоны действуют группами. Таким образом, в периоды высокой циклонической активности в земную кору накачивается огромная энергия

на относительно большой площади. Предполагается, что эта энергия «накадывается» на определенное число средних или слабых напряженностей, увеличивая уровень их напряженности. В этой ситуации из-за необычно сильного и быстрого действия циклонической энергии быстрее сейсмически «срабатывают» возросшие напряженности и гасится, возможно значительно, миграция напряженностей. В итоге провоцируется увеличение числа слабых землетрясений, например, землетрясений с  $M \leq 4$  и снижается вероятность возникновения сильных землетрясений. Как бы при этом реально не возросло количество слабых землетрясений ( $M \leq 4 - M < 5$ ), оно относительно мало отразится на величине суммарной годовой сейсмической энергии<sup>2</sup>.

На этапах же низкой циклонической активности поступающая в земную кору энергия, видимо, недостаточна для эффективного воздействия на зоны напряженности. В этом случае зоны напряженности имеют больше возможностей для развития и их слияния, что может привести к сильным землетрясениям, а значит, к усилению сейсмической активности.

В проведенных расчетных экспериментах выявлена еще одна важная особенность: высокое, по абсолютной величине, значение отрицательных коэффициентов корреляции достигается только при рассмотрении землетрясений с  $N \leq 33$  км. Это хорошо иллюстрируется на рис. 3. Этот результат может свидетельствовать о том, что тропические циклоны могут воздействовать на сейсмичность только в неглубоких твердых слоях земли, что и физически достаточно логично.

<sup>2</sup> Для сопоставления напомним, что энергия одного землетрясения с  $M = 7$  равна суммарной энергии более 31000 землетрясений с  $M = 4$ . Здесь не представлена статистика землетрясений с  $M \leq 4$ . Это связано с состоянием информации о таких землетрясениях. В Сейсмологическом бюллетене «Геофизической службы РАН» эти землетрясения представлены следующим образом: до 1978 г. ежегодно 0 таких землетрясений; с 1979 по 2000 г. по несколько землетрясений в год, иногда 20 – 30 землетрясения в год и с 2001 по 2015 г. от 94 до 900 землетрясений в год. Из этого следует, что приведенная статистика землетрясений с  $M \leq 4$  не может объективно быть использована в нашем расчетном эксперименте. В реальности, в рассматриваемой зоне, конечно, не могут быть годы, когда не было землетрясений, или были единицы таких землетрясений. Можно предположить, что, скорее всего, ежегодно в рассматриваемой зоне возникало по несколько сот землетрясений с  $M \leq 4$ . Отсутствие в Сейсмологическом бюллетене данных или отсутствие полных данных о землетрясениях с  $M \leq 4$ , вероятно связано с техническими возможностями типовых сейсмографов, используемых в те годы. Возможно, амплитудно-частотные характеристики этих сейсмографов не позволяли достаточно достоверно выявлять признаки землетрясений с  $M \leq 4$ .

## Заключение

Приведенные результаты позволяют, предположительно, в качестве варианта, представить механизм особого воздействия многолетнего ряда годовых значений циклонической энергии на аналогичные ряды годовых значений сейсмической энергии в нескольких диапазонах магнитуд.

По рассматриваемым годам и циклонической зоне выявлены признаки тенденции многолетнего общего нарастания сейсмической энергии при многолетнем общем ослаблении циклонической энергии.

## Список источников [References]

1. Голицын Г. С. Статистика и энергетика тропических циклонов // Доклады Академии Наук. 1997. Т. 354. № 4. С. 535–538 [Golitsyn G. S. Statistics and energy of tropical cyclones // Reports of the Academy of Sciences. 1997. T. 354. № 4. С. 535–538. (In Russ.)]
2. Островский А. А., Рыкунов Л. Н. Экспериментальное изучение донного сейсмического шума в океане при прохождении циклона // Океанология. 1982. Т. XXII. № 6. С. 975–979 [Ostrovsky A. A., Rykunov L. N. Experimental study of bottom seismic noise in the ocean during the passage of a cyclone // Oceanology. 1982. T. XXII. № 6. P. 975–979. (In Russ.)]
3. Соболев Г. А., Закржевская Н. А., Соболев Д. Г. К вопросу о влиянии циклонов на сейсмичность // Вулканология и сейсмология. 2012. № 2. С. 27–38 [Sobolev G. A., Zakrzhevskaya N. A., Sobolev D. G. The effects of cyclones on seismicity // Vulkanologiya i Seismologiya. 2012;(2):27–38. (In Russ.)]
4. Табулевич В. Н. Комплексные исследования микросейсмических колебаний. Новосибирск: Наука. 1986. 151 с. [Tabulevich V. N. Comprehensive studies of microseismic oscillations. Novosibirsk: Nauka. 1986. 151 p. (In Russ.)]
5. Ярошевич М. И. О некоторых взаимосвязях в динамике активности тропических циклонов // Известия РАН. Физика атмосферы и океана. 2011. Т. 47. № 4. С. 547–551 [Yaroshevich M. I. On some relationships in the dynamics of tropical cyclone activity // Izvestia RAS. Atmospheric and ocean physics. 2011;47(4):547–551. (In Russ.)]
6. Ярошевич М. И. Динамика сезонных значений суммарных интенсивностей тропических циклонов // ДАН. 2007. Т. 413. № 4. С. 549–552 [Yaroshevich M. I. Dynamics of seasonal values of the total intensities of tropical cyclones // DAN. 2007;413(4):549–552. (In Russ.)]
7. Ярошевич М. И. О некоторых особенностях сейсмичности в зоне действия тропических циклонов // Динамические процессы в геосферах. 2024. Т. 16. № 1. С. 25–31 [Yaroshevich M. I. On some features of seismicity in the zone of action of tropical cyclones // Dynamic processes in the geospheres. 2024;16(1):25–31. (In Russ.)]
8. Bowen S. P., Richard J., Macini J. D., et al. Microseism and infrasound generation by cyclones. J. Acoust. Soc. Am. 2003. Vol. 113 (5). P. 2562–2573.

## Сведения об авторе

**Ярошевич Михаил Иосифович:** кандидат технических наук

Количество публикаций: более 140

Область научных интересов: исследование тропических циклонов

Контактная информация:

myarosh32@gmail.com

Статья поступила в редакцию: 16.08.2024

Одобрена после рецензирования: 30.08.2024

Принята к публикации: 18.09.2024

Дата публикации: 28.02.2025

*The article was submitted: 16.08.2024*

*Approved after reviewing: 30.08.2024*

*Accepted for publication: 18.09.2024*

*Date of publication: 28.02.2025*

УДК 338.984  
Научная специальность: 5.2.6  
<https://elibrary.ru/dqsxbs>

ISSN 1812-5220  
© Проблемы анализа риска, 2025

# Анализ процессов создания ИТ-продуктов в рамках выполнения ИТ-проектов<sup>1</sup>

**Николаенко В.С.,**

Томский государственный университет систем управления и радиоэлектроники, 634050, Россия, г. Томск, пр. Ленина, 40

Томский политехнический университет, 634050, Россия, г. Томск, пр. Ленина, 30

Сибирский государственный медицинский университет, 634050, Россия, г. Томск, Московский тракт, 2

## Аннотация

В статье представлены результаты анализа международных сводов знаний управления проектами (PMBOK Guide®, ISO и др.) и национальных стандартов (ГОСТ Р ИСО/МЭК 12207, серия стандартов ИСО/МЭК 15504, ГОСТ Р ИСО 21500, семейство стандартов «Проектный менеджмент»), регламентирующих формализацию процессов создания ИТ-продуктов и процессов управления проектами, в том числе в области ИТ. Выбор этой области исследования обусловлен низкой долей успешно завершённых ИТ-проектов, а также значительным материальным ущербом, который получают ИТ-субъекты в результате неисполнения существенных условий контрактов.

Цель статьи: проведение анализа процессов, реализуемых во время фаз жизненного цикла ИТ-проекта, процессов, распределённых по предметным группам, и процессов контроллинга ИТ-проекта.

Итогом проведенного анализа стала разработанная процессная модель создания ИТ-продуктов в рамках выполнения ИТ-проектов, включающая в себя 62 подпроцесса. В статье представлены доказательства того, что разработанная процессная модель элиминирует наступление рисков и негативных последствий, связанных с отклонением от базовых планов и существенных условий контрактов.

**Ключевые слова:** управление проектами; управление процессами; ИТ-продукт; ИТ-проект; ИТ-субъект; риск; универсальный риск; процессная модель.

**Для цитирования:** Николаенко В.С. Анализ процессов создания ИТ-продуктов в рамках выполнения ИТ-проектов // Проблемы анализа риска. 2025. Т. 22. № 1. С. 68–87. — EDN: DQSXBS

**Автор заявляет об отсутствии конфликта интересов**

<sup>1</sup> Работа выполнена в рамках государственного задания «Наука», проект FEWM-2023-0013.

# Analysis of the Processes of Creating IT-Products as Part of the Implementation of IT-Projects<sup>2</sup>

**Valentin S. Nikolaenko,**

Tomsk State University  
of Control Systems  
and Radioelectronics,  
Lenin Ave., 40, Tomsk, 634050,  
Russia

Tomsk Polytechnic University,  
Lenin Ave., 30, Tomsk, 634050,  
Russia

Siberian State Medical  
University,  
Moscow Tract, 2, Tomsk,  
634050, Russia

**Abstract**

The article presents the results of an analysis of project management' international codes of knowledge (PMBOK Guide®, ISO, etc.) and national standards (GOST ISO 9000, GOST R ISO/IEC 21827, GOST R ISO/IEC 33001, GOST R 54869, GOST R ISO/IEC 15504-1, etc.), which regulate the formalization of processes in IT-projects. This area of research is chosen due to the low proportion of successfully completed IT-projects, as well as the significant material damage that IT-organizations suffer as a result of missed targets in IT-projects. In this regard, the purpose of the article is to develop a toolkit for the maturity assessment of processes in IT-projects, aimed at increasing the chances of successfully achieving the goals of IT-projects, and also eliminating possible negative consequences in cases of deviations from original plans and contract terms. To achieve this goal, the cascade model phases of the life cycle of creating IT-products were analyzed in accordance with national standards GOST R 57102 and GOST R 59793, the life cycle model of an IT-project was proposed, which includes 6 phases (starting an IT-project, defining requirements for an IT-product, planning an IT-project, creating an IT-product, testing an IT-product, and finishing an IT-project), IT-project processes, that implemented during the life cycle phases and distributed by subject groups and performed in controlling, were identified, a reference model of IT-project processes was created, which includes 62 interconnected and interdependent processes.

**Keywords:** project management; process management; IT-product; IT-project; IT-subject; risk; universal risk; process model.

**For citation:** Nikolaenko V.S. Analysis of the processes of creating IT-products as part of the implementation of IT-projects // *Issues of Risk Analysis*. 2025;22(1):68-87. (In Russ.). — EDN: DQSXBS

**The author declares no conflict of interest**

**Содержание**

Введение

1. Анализ национальных стандартов, закрепляющих положения о процессах создания ИТ-продуктов и управления ИТ-проектами

2. Модель 62 подпроцессов создания ИТ-продуктов в рамках выполнения ИТ-проектов

Заключение

Список источников

<sup>2</sup> The work was carried out within the framework of the state task «Science», project FEWM-2023-0013.

## Введение

Исследование бизнес-деятельности 495 ИТ-субъектов Томской области (ОКВЭД код 62), проведенное в рамках научно-исследовательского гранта РФФИ № 16-36-00031 «мол.а», позволило установить, что во время создания ИТ-продуктов в рамках выполнения ИТ-проектов может материализоваться порядка 105 универсальных рисков [1]. Под универсальными рисками понимаются вероятные события, актуальные для ИТ-проектов (спринты, фазы жизненного цикла, контракты и др.), независимо от их масштаба, сложности, длительности (краткосрочные, среднесрочные, долгосрочные), типов (ПО, мобильное приложение, ИС и др.), концепции создания ИТ-продуктов (Waterfall, Agile) и численности участников. Анализ идентифицированных универсальных рисков показал, что одним из механизмов их элиминирования является высокая степень освоения ИТ-субъектами положений о процессах создания ИТ-продуктов и управления ИТ-проектами, которые закреплены в основополагающих национальных стандартах [2, 3]. К таким стандартам относятся ГОСТ Р ИСО/МЭК 12207<sup>3</sup>, серия стандартов ИСО/МЭК 15504<sup>4</sup>, ГОСТ Р ИСО 21500<sup>5</sup> и семейство стандартов «Проектный менеджмент»<sup>6</sup>.

На основании вышесказанного целью представленной статьи является проведение анализа процессов создания ИТ-продуктов в рамках выполнения ИТ-проектов.

<sup>3</sup> ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. М.: Стандартинформ, 2010. 105 с.

<sup>4</sup> ГОСТ Р ИСО/МЭК 15504-1-2009. Информационные технологии. Оценка процессов. Часть 1. Концепция и словарь. М.: Стандартинформ, 2017. 20 с.; ГОСТ Р ИСО/МЭК 15504-2-2009. Информационные технологии. Оценка процессов. Часть 2. Проведение оценки. М.: Стандартинформ, 2017. 16 с.

<sup>5</sup> ГОСТ Р ИСО 21500-2014. Руководство по проектному менеджменту. М.: Стандартинформ, 2015. 46 с.

<sup>6</sup> ГОСТ Р 56716-2015. Проектный менеджмент. Техника сетевого планирования. Общие положения и терминология. М.: Стандартинформ, 2020. 20 с.; ГОСТ Р 56715.1-2015. Проектный менеджмент. Системы проектного менеджмента. Часть 1. Основные положения. М.: Стандартинформ, 2017. 11 с.; ГОСТ Р 56715.2-2015. Проектный менеджмент. Системы проектного менеджмента. Часть 2. Процессы и процессная модель. М.: Стандартинформ, 2016. 42 с.; ГОСТ Р 56715.3-2015. Проектный менеджмент. Системы проектного менеджмента. Часть 3. Методы. М.: Стандартинформ, 2016. 11 с.; ГОСТ Р 56715.5-2015. Проектный менеджмент. Системы проектного менеджмента. Часть 5. Термины и определения. М.: Стандартинформ, 2020. 12 с.; ГОСТ Р МЭК 61160-2015. Проектный менеджмент. Документальный анализ проекта. М.: Стандартинформ, 2016. 28 с.

## 1. Анализ национальных стандартов, закрепляющих положения о процессах создания ИТ-продуктов и управления ИТ-проектами

Национальный стандарт ГОСТ Р ИСО/МЭК 12207 описывает специальные процессы, которые должны быть реализованы на стороне ИТ-субъекта, если он намерен создавать, поставлять и успешно эксплуатировать ИТ-продукты. Для раскрытия особенностей применения этого стандарта раскроем суть и содержание понятия «процесс» подробнее.

Согласно ГОСТ ISO 9000<sup>7</sup>, ГОСТ Р ИСО/МЭК 21827<sup>8</sup>, ГОСТ Р ИСО/МЭК 33001<sup>9</sup>, ГОСТ Р 54869<sup>10</sup> и ГОСТ Р ИСО/МЭК 15504–1 под «процессом» необходимо понимать совокупность действий, которые направлены на достижение определенной цели, где вход процесса — это объекты, необходимые для нормальной работы процесса (информация, ресурсы, регламенты и др.), а выход процесса — это результаты достижения цели процесса.

В научной литературе также можно встретить и другие толкования понятия «процесс». Например, О. Вишняков в своих трудах [4] определяет процесс как повторяющуюся, упорядоченную цепочку действий, которая создает значимый результат для заказчика, пользователя, клиента, потребителя и др. Более развернутое определение можно встретить в работах Ю. Т. Шестопаля, Н. Ю. Дорофеева, Н. Ю. Шестопал и Э. А. Андреевой. Под «процессом» ученые понимают устойчивую, целенаправленную совокупность взаимосвязанных видов деятельности, которая по определенной технологии преобразует входы и выходы, где вход — это ресурс, который необходим процессу, а выход — это результат (продукт) выполнения процесса [5].

Рассмотренные выше определения и требования по документированию процессов, закреплённые

<sup>7</sup> ГОСТ ISO 9000-2011. Системы менеджмента качества. Основные положения и словарь. М.: Стандартинформ, 2020. 28 с.

<sup>8</sup> ГОСТ Р ИСО/МЭК 21827-2010. Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса. М.: Стандартинформ, 2015. 188 с.

<sup>9</sup> ГОСТ Р ИСО/МЭК 33001-2017. Информационные технологии. Оценка процесса. Понятия и терминология. М.: Стандартинформ, 2017. 16 с.

<sup>10</sup> ГОСТ Р 54869-2011. Проектный менеджмент. Требования к управлению проектом. М.: Стандартинформ, 2019. 8 с.

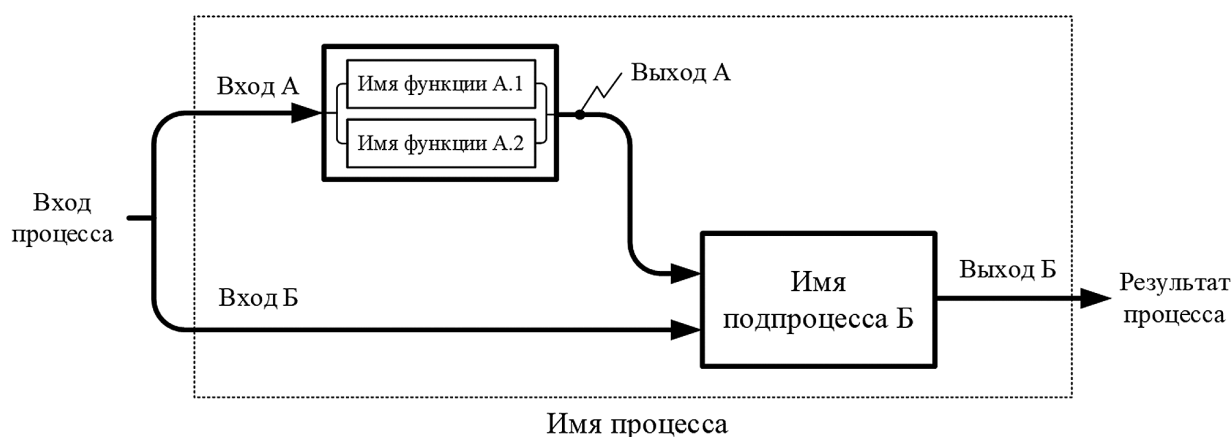


Рис. 1. Пример графического представления процесса

Figure 1. Example of a graphical representation of a process

в стандарте ГОСТ Р 57098<sup>11</sup>, позволяют заключить, что процесс включает в себя такие элементы, как цель, реализуемые действия, функции и их последовательность, потребляемые ресурсы (вход процесса), результат (выход процесса), риски и др. Пример графического изображения процесса согласно ГОСТ Р 57098 представлен на рис. 1.

Анализ положений, закрепленных в ГОСТ Р ИСО/МЭК 12207, показал, что стандарт описывает цели, желаемые результаты, входы и выходы 43 процессов жизненного цикла ИТ-продукта, которые объединены в семь групп.

Несмотря на исчерпывающую совокупность процессов, необходимых для создания ИТ-продуктов, применение ГОСТ Р ИСО/МЭК 12207 имеет ряд ограничений, о которых необходимо упомянуть. Во-первых, в стандарте не детализируются процессы нижнего уровня (подпроцессы) и функции, закрепляющие конкретные методы и процедуры по достижению результатов, что значительно снижает вероятность получения высококачественных ИТ-продуктов. Важно отметить, что определение и формализация подпроцессов дают возможность не только определить состав обязательных функций, но и позволяют установить их последовательность и связи между ними. Отсутствие того либо иного подпроцесса оказывает значительное влияние на вероятность успешного достижения целей проекта [6]. В качестве подтверждения

достаточно упомянуть об экспресс-оценке универсальных рисков и их превентивном элиминировании. Во-вторых, стандарт не декларирует требования к проектной документации в части названий, форматов, содержания, носителей для записей и др. Решения о необходимости создания проектных документов стандарт оставляет за пользователем. По мнению автора настоящей статьи, оставление без внимания этого вопроса является существенным недостатком, т.к. выявленные комплаенс-особенности создания ИТ-продуктов показали, что процессы выполнения спринтов, фаз жизненного цикла ИТ-проектов и (или) контрактов требуют обязательного документального сопровождения. Например, в части обеспечения перехода права собственности и исключительного права на ИТ-продукт от правообладателя к приобретателю права, создания ИТ-продукта в рамках служебного задания и др. В-третьих, стандарт не устанавливает применение конкретной модели жизненного цикла (ЖЦ) ИТ-продукта. Ответственность за возможные последствия, связанные с выбором той либо иной модели ЖЦ, согласно положениям стандарта возлагается на заинтересованные стороны. Такое обстоятельство также является существенным недостатком, т.к. проведенное исследование показало, что для создания ИТ-продуктов необходимо применять модель ЖЦ ИТ-проекта, включающую в себя квантификацию ЖЦ на шесть фаз: начало ИТ-проекта, определение требований к ИТ-продукту, планирование ИТ-проекта, создание ИТ-продукта, тестирование ИТ-продукта и окончание ИТ-проекта.

<sup>11</sup> ГОСТ Р 57098-2016/ISO/IEC TR 24774: 2010. Системная и программная инженерия. Управление жизненным циклом. Руководство для описания процесса. М.: Стандартинформ, 2018. 14 с.

**Серия стандартов ИСО/МЭК 15504** предлагает использовать процессную модель, состоящую из 60 процессов — 10 процессов соглашения, 13 процессов организационного обеспечения, 7 процессов проекта, 13 технических процессов, 6 процессов реализации ПС, 8 процессов поддержки ПС и 3 процесса повторного применения ПС. Согласно ГОСТ Р ИСО/МЭК 15504-5<sup>12</sup> под «процессной моделью» понимается модель, состоящая из логической последовательности процессов, выполнение которых гарантирует получение желаемого результата. Несмотря на исчерпывающее описание процессов, представленных в серии стандартов ИСО/МЭК 15504, проведенный анализ показал, что предлагаемая процессная модель не объясняет последовательность выполнения действий, оставляя решение о выборе процессов и определение последовательности их выполнения за пользователями. Стандарты не содержат информации о возможных проблемах, которые могут материализоваться в ходе выполнения процессов, о мерах, элиминирующих эти проблемы, а также о метриках, которые бы показывали результативность и эффективность выполнения процессов. Кроме того предлагаемая модель не содержит процессов анализа проблем, выявления лучших практик, стандартизации и распространения полученного опыта среди заинтересованных сторон и работников ИТ-субъекта. Отсутствие подобных процессов на стороне ИТ-субъекта создает угрозу утраты выученных уроков, что в будущих проектах может привести к повторному появлению ранее решенных проблем.

**ГОСТ Р ИСО 21500** распределяет 39 процессов проектного менеджмента на управленческие (инициация, планирование, исполнение, контроль и завершение) и предметные группы (интеграция, заинтересованные стороны, содержание, ресурсы, сроки, стоимость, риски, качество, закупки и коммуникации). Согласно условиям, закрепленным в разд. 4, требования ГОСТ Р ИСО 21500 носят рекомендательный характер, т.к. количество процессов и их последовательность зависят от области, в которой выполняются проектные работы. Например, если используются заемные средства (кредиты), то в проект должны быть добавлены процессы, связанные с финансами. Если проектные

работы могут оказать негативное влияние на жизнь и здоровье человека, то в проект необходимо включить процессы по технике безопасности и охране здоровья. Если оказывается негативное влияние на окружающую среду, то в проект необходимо включить процессы, связанные с экологической безопасностью, и др.

Кроме того в ГОСТ Р ИСО 21500 отмечается, что количество процессов и их последовательность также зависят от зрелости субъекта и накопленного им опыта. В качестве примера следует привести РМВОК® Guide, где:

- в первом издании (1996 г.) было зафиксировано 9 предметных групп и 37 процессов;
- во втором (2000 г.) — 9 предметных групп и 39 процессов;
- в третьем (2004 г.) — 9 предметных групп и 44 процесса;
- в четвертом (2008 г.)<sup>13</sup> — 9 предметных групп и 47 процессов
- в пятом (2013 г.)<sup>14</sup> — 10 предметных групп и 47 процессов;
- в шестом (2017 г.)<sup>15</sup> — 10 предметных групп и 49 процессов.

Среди ключевых недостатков ГОСТ Р ИСО 21500 необходимо отметить, что представленные процессы дают только общее представление о возможном количестве и последовательности выполнения работ.

Несмотря на расширенный перечень процессов проектного менеджмента (61 наименование) аналогичные недостатки были также выявлены при анализе **семейства стандартов «Проектный менеджмент»**. Однако это семейство стандартов закрепляет важное положение, которое заключается в декомпозиции процесса выполнения проекта на совокупность подпроцессов с последующим объединением их в самостоятельные группы. Например, согласно требованиям ГОСТ Р 54869 и Р 50.1.028<sup>16</sup> процесс выполнения проекта включает в себя пять процессов более низкого уровня: процесс инициации проекта; процесс планирования проекта; процесс организации и исполнения проекта; процесс контроллинга проекта; процесс

<sup>12</sup> ГОСТ Р ИСО/МЭК 15504-5-2009. Информационные технологии. Оценка процессов. Ч. 5. Образец модели оценки процессов жизненного цикла программного обеспечения. М.: Стандартинформ, 2016. 158 с.

<sup>13</sup> Project management body of knowledge. Guide 4th edition (РМВОК-4). Project Management Institute (PMI), 2008. 506 p.

<sup>14</sup> Project management body of knowledge. Guide 5th edition (РМВОК-5). Project Management Institute (PMI), 2013. 616 p.

<sup>15</sup> Project management body of knowledge. Guide 6th edition (РМВОК-6). Project Management Institute (PMI), 2017. 756 p.

<sup>16</sup> Р 50.1.028-2001. Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования. М.: ГОССТАНДАРТ РОССИИ, 2003. 50 с.

завершения проекта. Говоря же о наличии подпроцессов следует обратиться к разд. 5 ГОСТ Р 54869, где отмечается, что наличие, количество, повторяемость и последовательность процессов, подпроцессов и функций в первую очередь зависят от масштаба, сложности и длительности работ проекта. Например, если ИТ-продукт создается согласно концепции Agile, то процесс организации и исполнения проекта в части формирования бюджета может выполняться частично либо вовсе отсутствовать.

Таким образом, на основании проведенного анализа основополагающих национальных стандартов автором настоящей статьи предлагается распределить процессы создания ИТ-продуктов в рамках выполнения ИТ-проектов на три группы: процессы, реализуемые во время фаз жизненного цикла ИТ-проекта; процессы, распределенные по предметным группам; процессы контроллинга ИТ-проекта. Рассмотрим обозначенные группы процессов подробнее.

*Процессы, реализуемые во время фаз жизненного цикла ИТ-проекта.* Результаты проведенного исследования показали, что для каждой фазы модели ЖЦ ИТ-проекта характерно выполнение определенного процесса с получением конкретного результата. Например, по итогу завершения процесса начала ИТ-проекта между заказчиком и ИТ-субъектом должен быть заключен контракт на создание ИТ-продукта. Анализ судебной практики показал, что некачественное, частичное выполнение либо полное невыполнение этого процесса влечет тяжкие последствия.

В качестве примера наступления нежелательного исхода для заинтересованных сторон, которые спонтанно инициировали запуск ИТ-проекта, можно привести дело № А67-4580/2016<sup>17</sup>, в котором между сторонами отсутствовали документальные соглашения, подтверждающие заключение контракта. Однако в ходе разбирательства было установлено, что требующие исполнения гражданско-правовые обязательства все же возникли.

Похожая ситуация произошла в деле № А67-3471/2010<sup>18</sup>, где подписание актов сдачи-приемки оказанных услуг по техническому обслуживанию и обновлению баз данных ИСС «Кодекс»

послужило доказательством того, что между сторонами возникли определенные обязательства.

Другим примером тяжких комплаенс-последствий для заинтересованных сторон является дело № А45-15497/2020<sup>19</sup>. Согласно материалам, при эксплуатации мобильного приложения «Boom Boom» заказчик выявил большое количество программных недостатков и потребовал от ИТ-субъекта переделать работу. ИТ-субъект не согласился с предъявленной претензией и отказал в удовлетворении этого требования. Для определения характера недостатков суд был вынужден провести экспертизу, которая установила, что результат выполненных работ частично соответствует условиям контракта, является некачественным и требует устранения выявленных дефектов. Размер причиненного ущерба составил 340,8 тыс. руб.

Нередки случаи, когда заинтересованные стороны после завершения ИТ-проектов запрещают своим бывшим контрагентам и работникам использовать ИТ-продукты. В качестве примера следует привести дело № А53-23110/22<sup>20</sup>, где истец попросил суд запретить ответчику использовать ИТ-продукт «LabWagon». Другим примером является дело № А40-90889/21-134-529<sup>21</sup>, где истец требовал запретить использование его ИТ-продукта, изъять все материальные носители с копиями ИТ-продукта и взыскать компенсацию за нарушение исключительных прав в размере 5 млн руб.

С учетом вышесказанного автором статьи предлагается использовать процессную модель, в которой разработка технического задания, базового плана проекта и ИТ-продукта ведется в рамках отдельных процессов и оформляется отдельными дополнительными соглашениями к контракту (рис. 2).

Цели, действия и результаты процессов процессной модели создания ИТ-продуктов в рамках выполнения ИТ-проектов представлены в табл. 1.

<sup>17</sup> Решение Арбитражного суда Томской области по делу от 10.10.2016 № А67-4580/2016 [Электронный ресурс]. URL: <https://clck.ru/m5nMz> (дата обращения: 31.01.2024).

<sup>18</sup> Решение Арбитражного суда Томской области по делу от 28.06.2010 № А67-3471/2010 [Электронный ресурс]. URL: <https://clck.ru/m4kbL> (дата обращения: 31.01.2024).

<sup>19</sup> Решение Арбитражного суда Новосибирской области по делу от 24.03.2022 № А45-15497/2020 [Электронный ресурс]. URL: <https://clck.ru/36d7VV> (дата обращения: 31.01.2024).

<sup>20</sup> Решение Арбитражного суда Ростовской области по делу от 07.06.2023 № А53-23110/22 [Электронный ресурс]. URL: <https://clck.ru/36c8y> (дата обращения: 31.01.2024).

<sup>21</sup> Решение Арбитражного суда города Москвы по делу от 05.10.2023 № А40-90889/21-134-529 [Электронный ресурс]. URL: <https://clck.ru/36cmjw> (дата обращения: 31.01.2024).

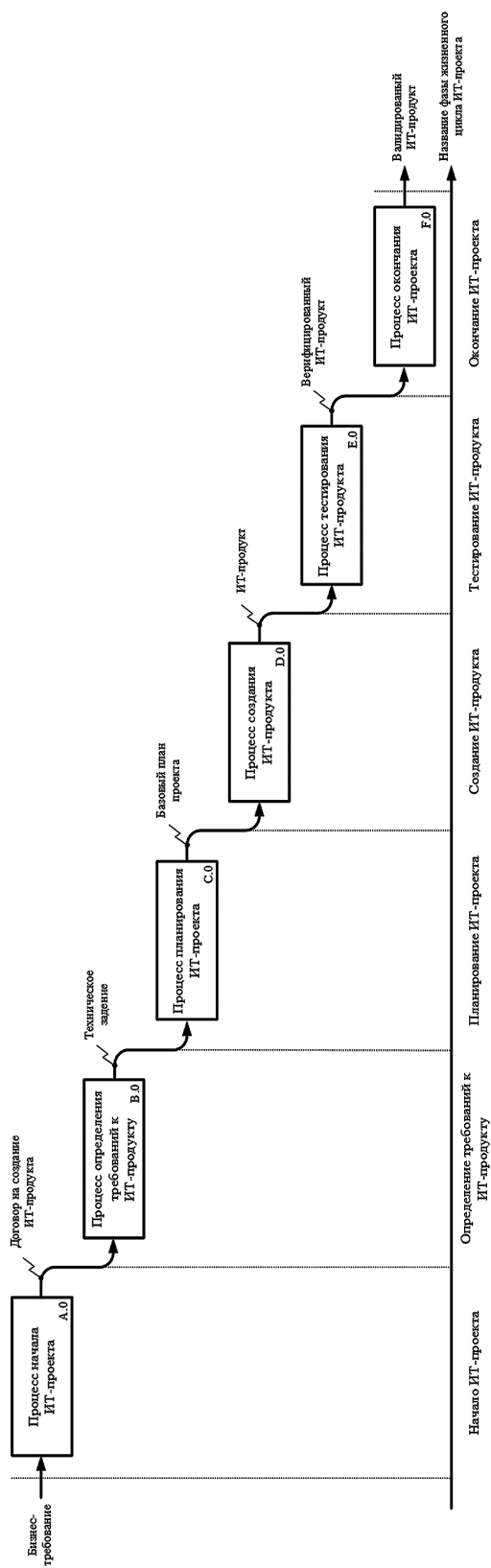


Рис. 2. Процессная модель создания ИТ-продуктов в рамках выполнения ИТ-проектов  
 Figure 2. IT Project IT product creation process model

Требуется отметить, что основным преимуществом предлагаемого решения является превентивное воздействие на универсальные риски, связанные с отклонением от существенных условий контракта, за счет высокой точности определения дат окончания спринтов, фаз жизненного цикла ИТ-проекта и контрактов, количества необходимых ресурсов, а также объемов бюджетов. Кроме того предлагаемое решение уменьшает вероятность наступления риска получения материального и репутационного урона из-за досрочного прекращения проектных работ.

Процессы ИТ-проекта, распределенные по предметным группам. Процессы, относящиеся к функциональным областям управления проектами, согласно ГОСТ Р ИСО 21500 должны быть дифференцированы на предметные группы. Предметная группа — это выделенная область проекта, определяемая ее требованиями к знаниям [13]. В частности, управление рисками в проекте является отдельным знаниевым домом, который регулируется собственным семейством стандартов ГОСТ Р ИСО 31000<sup>22</sup> [14], управление качеством — ГОСТ ISO 9000, управление закупками и интеграцией — нормами действующего гражданского законодательства<sup>23</sup> и др. В литературе также можно встретить синонимы понятия «предметная группа». Например, А. А. Дульзон в своих трудах предметные группы управления проектами называет «функциями управления» [15]. В своде лучших практик управления проектами PMBOK® Guide используется понятие «области знаний», которыми руководитель проекта должен обладать для успешного завершения проекта [16]. В ряде национальных стандартов, например ГОСТ Р 54869, предметные группы управления проектами именуют как «области управления».

На основании проведенного анализа положений основополагающих национальных стандартов предлагается процессы создания ИТ-продуктов в рамках выполнения ИТ-проектов распределить на десять предметных групп, таких как: интеграция; заинтересованные стороны; содержание; ресурсы; сроки; стоимость; риски; качество; закупки; коммуникации. Результаты распределения процессов ИТ-проектов по предметным группам представлены в табл. 2.

<sup>22</sup> ISO 31000:2009. «Risk Management – Principles and Guidelines». 2013. 34 p.

<sup>23</sup> Гражданский кодекс Российской Федерации (ГК РФ). Комментарий к последним изменениям. М.: АБАК, 2019. 752 с.

**Таблица 1. Цели, действия и результаты процессов процессной модели создания ИТ-продуктов в рамках выполнения ИТ-проектов**

Table 1. Goals, actions and results of the processes of the IT Product creation process model in the framework of IT Projects

№	Название процесса	Комментарий
1	Процесс начала ИТ-проекта	Процесс направлен на достижение договоренности между заказчиком и ИТ-субъектом, где ИТ-субъект по заданию заказчика обязуется создать ИТ-продукт, а заказчик обязуется принять его и произвести оплату [7]. Материальным воплощением договоренности является заключенный контракт
2	Процесс определения требований к ИТ-продукту	Процесс направлен на идентификацию функциональных, пользовательских и бизнес-требований, которые предъявляют заинтересованные стороны к разрабатываемому ИТ-продукту [8]. В рамках процесса осуществляются сбор, обработка и утверждение требований, разработка ТЗ, формирование содержания ИТ-продукта, а также определяется необходимый и достаточный объем работ, который необходим для достижения целей ИТ-проекта [9]. Результатом выполнения процесса является ТЗ
3	Процесс планирования ИТ-проекта	Процесс направлен на разработку базового плана проекта, в котором фиксируются существенные условия сделки и цели ИТ-проекта [10]. В частности, организационная структура проекта, перечень ресурсов, даты начала и окончания ИТ-проекта и его этапов, бюджет проекта, возможные риски и меры воздействия на них. По завершении процесса разрабатывается базовый план проекта
4	Процесс создания ИТ-продукта	Процесс направлен на создание ИТ-продукта согласно заявленным функциональным, пользовательским и бизнес-требованиями, которые предъявляют заинтересованные стороны к разрабатываемому ИТ-продукту [11]. По завершении процесса создается желаемый ИТ-продукт
5	Процесс тестирования ИТ-продукта	Процесс направлен на установление соответствия между функциональными, пользовательскими и бизнес-требованиями, которые предъявляют заинтересованные стороны к созданному ИТ-продукту. Результатом выполнения процесса является верифицированный ИТ-продукт
6	Процесс окончания ИТ-проекта	Процесс направлен на организацию передачи и перехода прав собственности созданного ИТ-продукта от ИТ-субъекта к заказчику [12]. Результатом выполнения процесса является валидированный ИТ-продукт

**Таблица 2. Процессы ИТ-проекта, распределенные по предметным группам**

Table 2. IT project processes divided into subject groups

№	Название процесса	Комментарий
1	Интеграция	Процессы, направленные на выявление, определение, комбинирование, объединение, координацию действий, необходимых для завершения работ проекта [17]. Для этих процессов характерны: заключение контрактов и дополнительных соглашений к ним; обеспечение инфраструктурой, необходимой для выполнения работ проекта; стандартизация лучших практик управления проектом; разработка методических рекомендаций
2	Заинтересованные стороны	Процессы, направленные на: выявление всех заинтересованных сторон и выстраивание диалога и отношений с ними [18]. Для таких процессов характерно определение состава заинтересованных сторон и требований к ИТ-продукту [19]
3	Содержание	Процессы, направленные на определение и включение в проект только тех работ и результатов, которые необходимы для успешного достижения целей проекта [20]. Для этих процессов характерны: непосредственная разработка ТЗ и его валидирование; разработка ИСР; разработка базового плана и его валидирование; создание, доработка и валидирование ИТ-продукта
4	Ресурсы	Процессы, направленные на обеспечение проекта трудовыми, материальными, информационными и иными ресурсами, необходимыми для успешного достижения целей проекта. Для этих процессов характерно обеспечение ресурсами для разработки ТЗ, базового плана проекта и создания ИТ-продукта
5	Сроки	Процессы, направленные на создание календарного плана-графика проекта, отслеживание его выполнения и обеспечение своевременного завершения [21]. Для этих процессов характерно определение последовательности работ; оценка длительности работ и разработка календарного плана-графика проекта

Окончание табл. 2

№	Название процесса	Комментарий
6	Стоимость	Процессы, направленные на формирование бюджета проекта, отслеживание его выполнения и обеспечение своевременного завершения. Для таких процессов характерны проведение оценки длительности стоимости работ и разработка бюджета проекта
7	Риски	Процессы, направленные на оценку рисков и инициацию мер воздействия для наиболее опасных и значимых рисков [22]. Для этих процессов характерна оценка рисков с последующей разработкой и проведением мер воздействия на них
8	Качество	Процессы, направленные на планирование и обеспечение качества. Для этих процессов характерны: определение критериев качества, обеспечение качества и верифицирование ИТ-продукта
9	Закупки	Процессы, направленные на планирование снабжения, приобретение или получение результатов, услуг и (или) товаров у субподрядчиков [23]. Для этих процессов характерны: заключение контрактов с субподрядчиками и выполнение работ субподрядчиками
10	Коммуникации	Процессы, направленные на планирование и управление коммуникациями, а также на распространение информации, относящейся к проекту. Для этих процессов характерны: определение форм коммуникаций; распространение актуальной, точной и достоверной информации

Процессы контроллинга ИТ-проекта. Результативное и эффективное выполнение процессов в ИТ-проектах невозможно без процессов контроллинга [24]. Контроллинг в ИТ-проектах представляет собой замкнутую систему информационной, аналитической, методологической и инструментальной поддержки, которая направлена на определение текущего состояния проекта, сравнение текущего состояния с целевыми показателями, прогнозирование дальнейшего развития проекта и определение запросов на изменения [25].

Цель контроллинга совпадает с целью ИТ-проекта — создать ИТ-продукт в назначенный срок и в границах утвержденного бюджета [26]. Для дости-

жения запланированных целей ИТ-проекта во время контроллинга осуществляются взаимодействие с заинтересованными сторонами, управление их ожиданиями, сбор и протоколирование запросов на изменения, а также внесение изменений в контракты, дополнительные соглашения к ним, технические задания, базовые планы проектов либо ИТ-продуктов. Внесение изменений является ключевым процессом контроллинга, который приводит к изменению существенных условий, в связи с чем рекомендуется в тексте контракта заблаговременно описывать механизм внесения изменений. Подробное описание процессов контроллинга представлено ниже (см. табл. 3).

Таблица 3. Процессы контроллинга ИТ-проекта

Table 3. IT Project Controlling Processes

№	Название процесса	Комментарий
1	Управление содержанием проекта	Процесс, направленный на: определение текущего состояния содержания ИТ-продукта и объема работ ИТ-проекта, сравнение текущего состояния содержания ИТ-продукта и объема работ ИТ-проекта с целевыми показателями, прогнозирование дальнейшего развития ИТ-проекта, определение запросов на изменение содержания ИТ-продукта и объема работ проекта, а также на осуществление корректирующих действий
2	Управление ресурсом проекта	Процесс, направленный на определение текущего состояния ресурсов, сравнение текущего состояния ресурсов с целевыми показателями, прогнозирование дальнейшего развития ИТ-проекта, определение запросов на изменение ресурсов, а также на осуществление корректирующих действий

Окончание табл. 3

№	Название процесса	Комментарий
3	Управление сроками проекта	Процесс, направленный на: определение текущего состояния календарного плана-графика, сравнение текущего состояния календарного плана-графика проекта с целевыми показателями, прогнозирование дальнейшего развития ИТ-проекта, определение запросов на изменение календарного плана-графика проекта, а также на осуществление корректирующих действий
4	Управление стоимостью проекта	Процесс, направленный на: определение текущего состояния бюджета ИТ-проекта, сравнение текущего состояния бюджета с утвержденными целевыми показателями, прогнозирование дальнейшего развития ИТ-проекта, определение запросов на изменение бюджета ИТ-проекта, а также на осуществление корректирующих действий
5	Управление рисками проекта	Процесс, направленный на: определение текущего состояния рисков ИТ-проекта, сравнение текущего состояния рисков с утвержденными целевыми показателями, прогнозирование дальнейшего развития ИТ-проекта, задействование мер принятия рисков
6	Управление качеством проекта	Процесс, направленный на: определение текущего состояния качества ИТ-продукта, сравнение текущего состояния ИТ-продукта с утвержденными целевыми показателями, прогнозирование дальнейшего развития проекта, отправление результатов выполненных работ на доработку при установлении отклонений от требований и стандартов, а также на осуществление корректирующих действий
7	Управление закупками проекта	Процесс получения регулярных отчетов от субподрядчиков о ходе исполнения обязательств
8	Управление коммуникациями проекта	Процесс устранения проблем во время информационного взаимодействия между заинтересованными сторонами и участниками ИТ-проекта
9	Управление изменениями проекта	Процесс, направленный на: регистрацию запросов на изменения, проведение оценок сроков, а также человеческих и материальных ресурсов, которые необходимы для реализации запрашиваемых изменений, фиксирование наступивших проблем и предпринятых мер по их устранению в журнале проблем
10	Управление ожиданиями заинтересованных сторон	Процесс, направленный на: проведение переговоров по поиску оптимальных решений, которые помогут выйти из сложившихся обстоятельств, выработку оптимальных решений и внесение изменений в базовый план ИТ-проекта [27]
11	Внесение изменений	Процесс, направленный на внесение изменений в контракты, дополнительные соглашения, техническое задание, базовый план проекта и (или) ИТ-продукт

## 2. Модель 62 подпроцессов создания ИТ-продуктов в рамках выполнения ИТ-проектов

На основании проведенного анализа основополагающих национальных стандартов, разработанной процессной модели, а также предложенного распределения процессов автор представленной статьи разработал модель, состоящую из 62 подпроцессов создания ИТ-продуктов в рамках выполнения ИТ-проектов (рис. 3).

Разработанная модель представляет собой замкнутую последовательность подпроцессов, распределенных по фазам жизненного цикла и предметным группам, где каждый подпроцесс направлен на получение конкретного измеримого результата(–ов). Замкнутость

последовательности подпроцессов указывает на их непрерывность, взаимосвязь и взаимозависимость. Это обстоятельство подчеркивает важность и значимость каждого подпроцесса. Например, если будут отсутствовать такие процессы, как «В.5 Валидирование ТЗ», «С.13 Валидирование базового плана проекта» и (или) «Е.1 Валидирование ИТ-продукта», то может возникнуть проблема, связанная с тем, что заказчик выявит недостатки ИТ-продукта во время его эксплуатации [28]. Кроме того анализ разработанной модели показал, что самым трудоемким является процесс планирования ИТ-проекта, где нарушение последовательности выполнения подпроцессов создает угрозу получения недостоверных значений в базовом плане проекта и искажения существенных условий контракта.

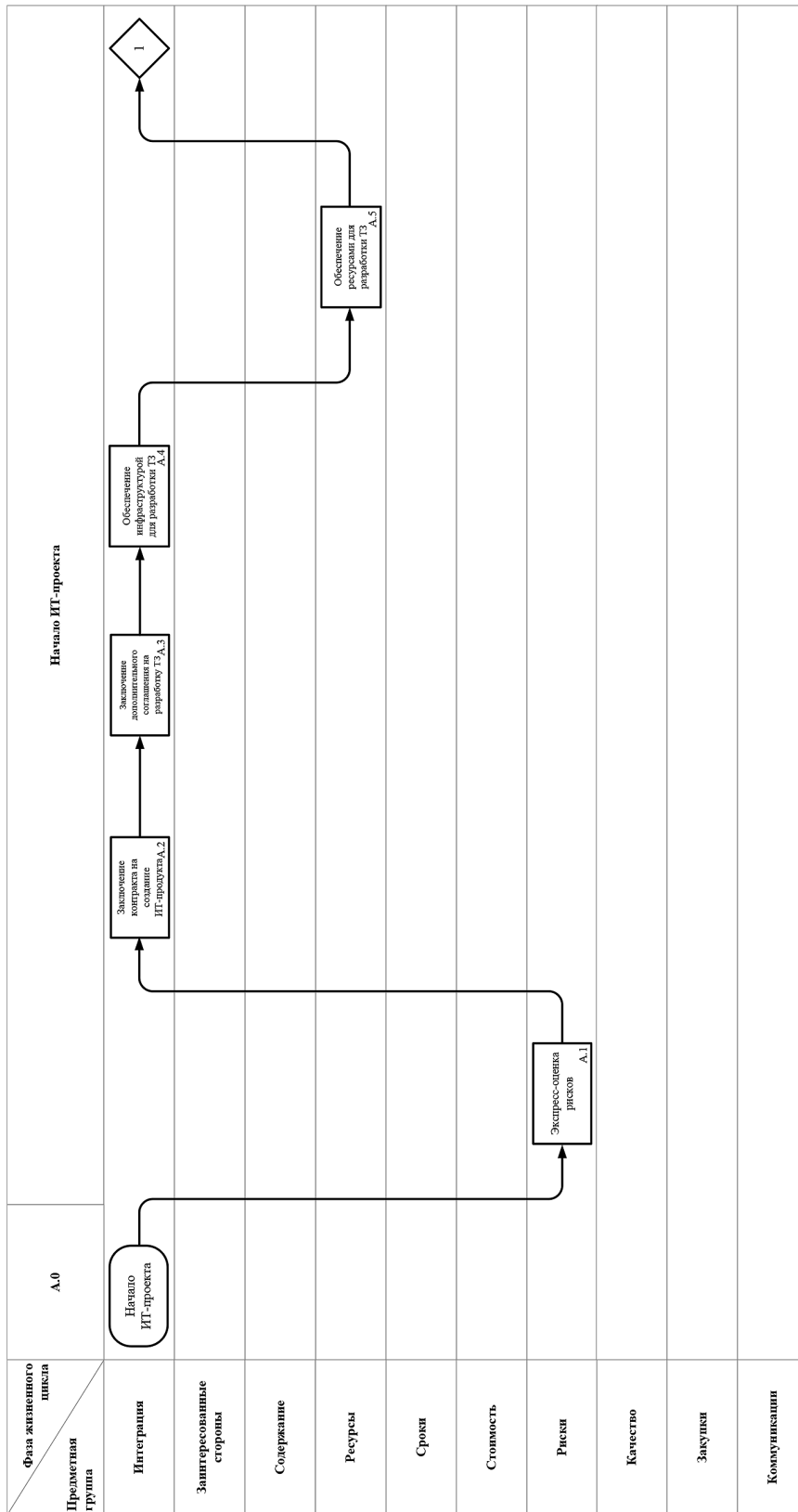


Рис. 3. А.0 — Подпроцессы фазы жизненного цикла «начало ИТ-проекта»  
 Fig. 3. A.0 — Sub-processes of the life cycle phase "the beginning of the IT Project"

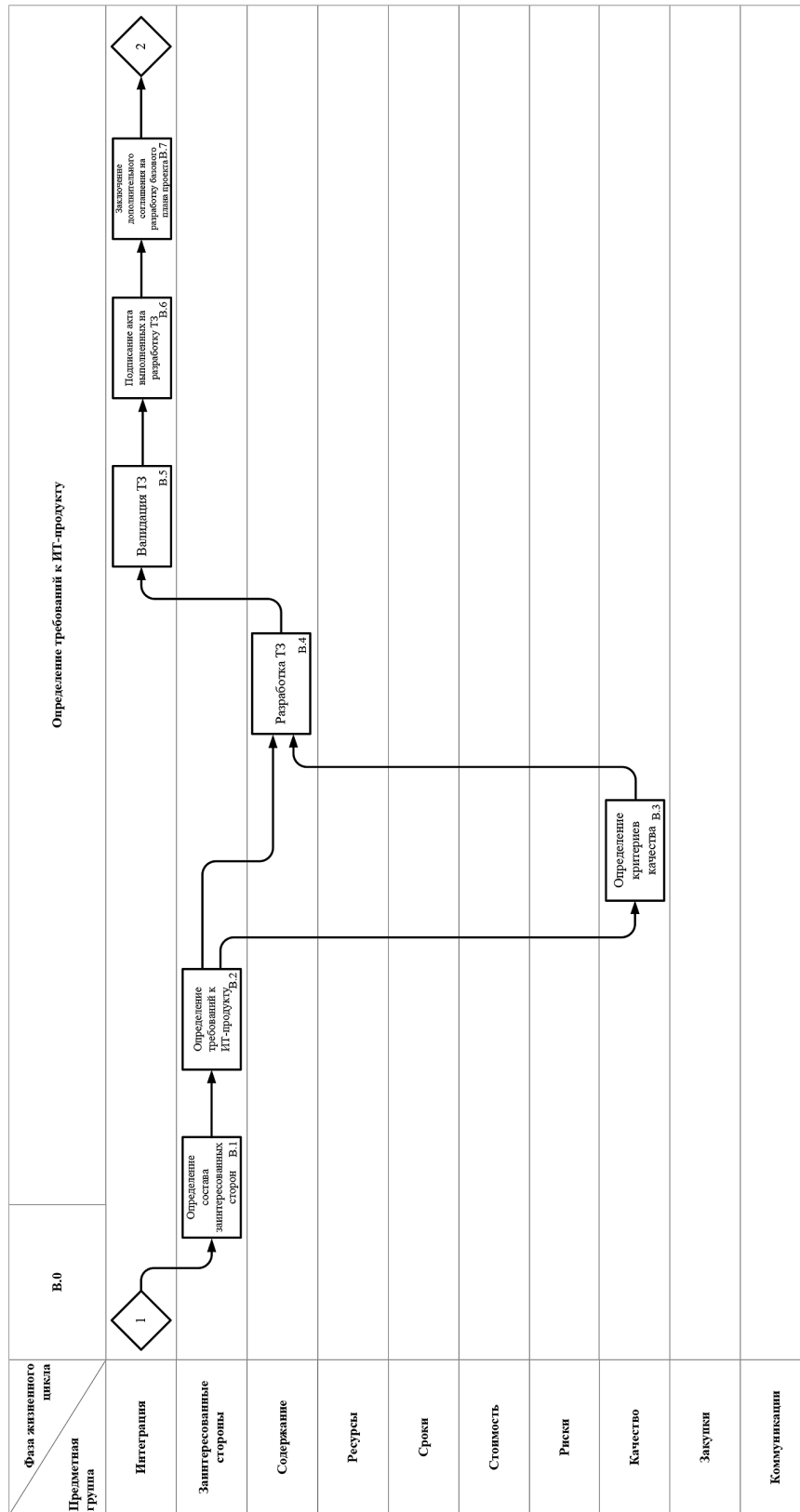


Рис. 3. В.0 — Подпроцессы фазы жизненного цикла «определение требований к ИТ-продукту»

Figure 3. В.0 — IT Product Requirements Lifecycle Phase Sub-Processes



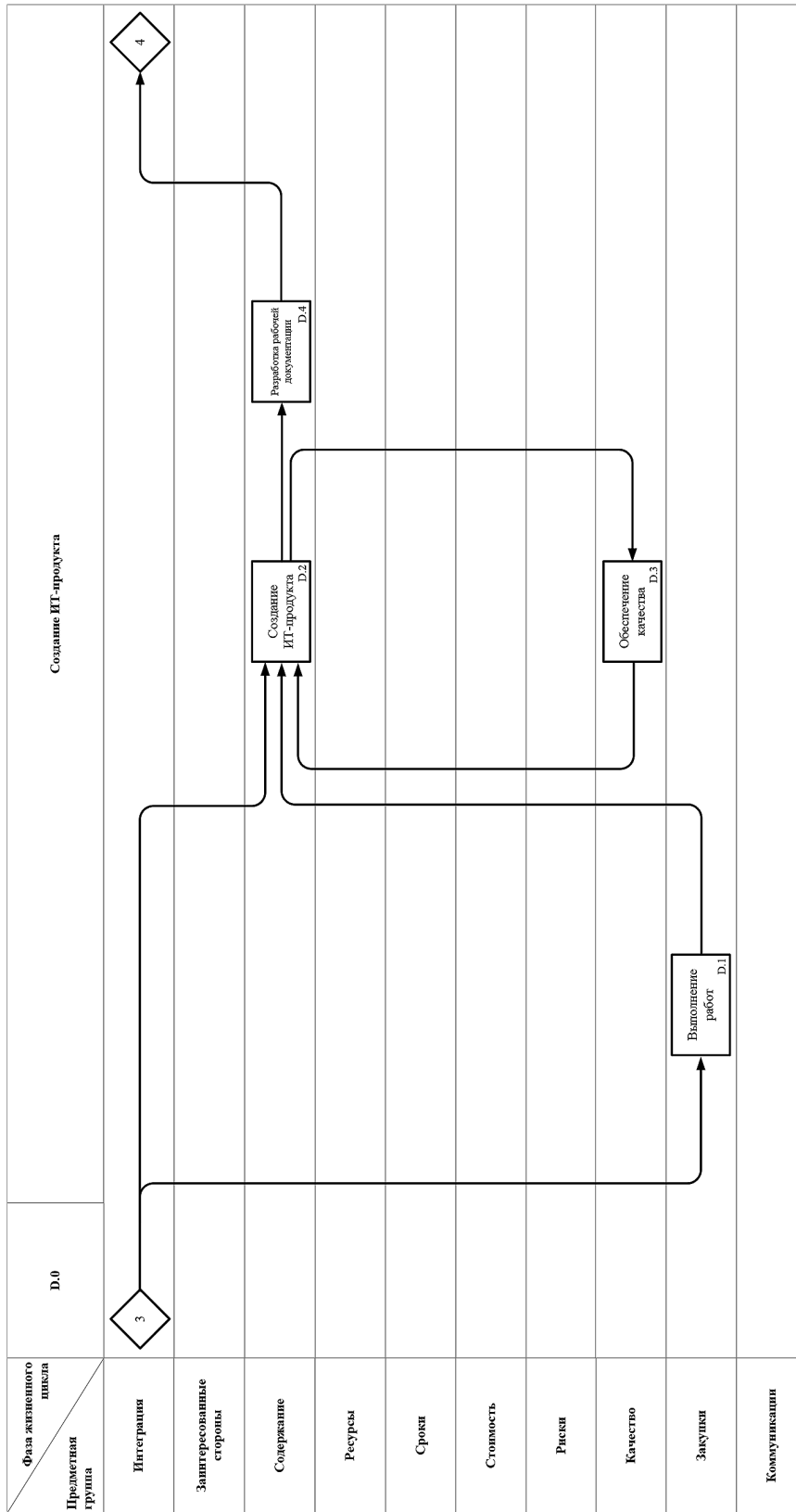


Рис. 3. D.0 — Подпроцессы фазы жизненного цикла «создание ИТ-продукта»  
 Figure 3. D.0 — Subprocesses of IT Product Creation Lifecycle Phase

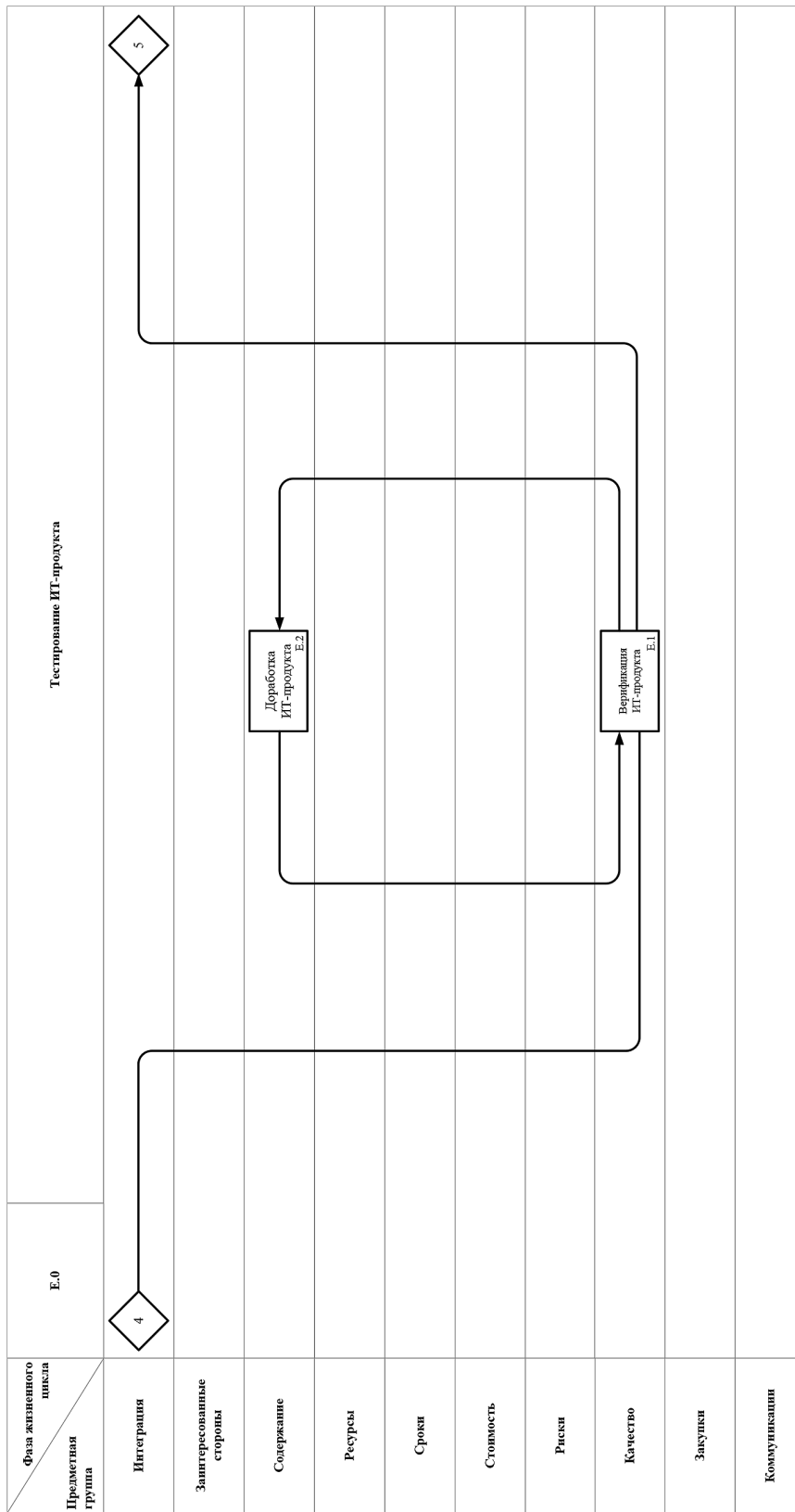


Рис. 3. E.0 — Подпроцессы фазы жизненного цикла «тестирование ИТ-продукта»

Figure 3. E.0 — IT Product Testing Lifecycle Sub-Processes

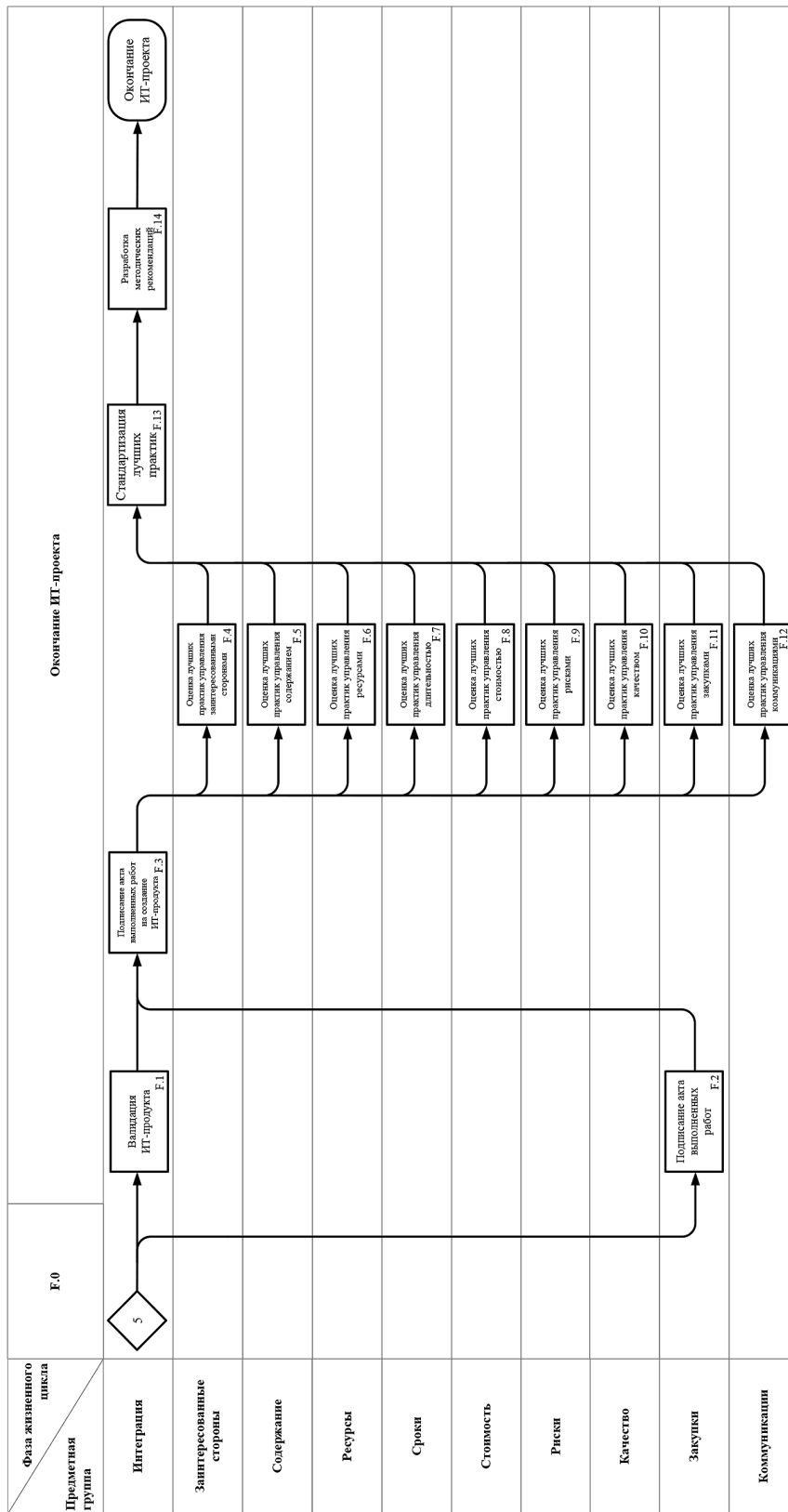


Рис. 3. F.0 — Подпроцессы фазы жизненного цикла «окончание ИТ-проекта»  
 Figure 3. F.0 — Sub-Processes of the End of IT Project Life Cycle Phase

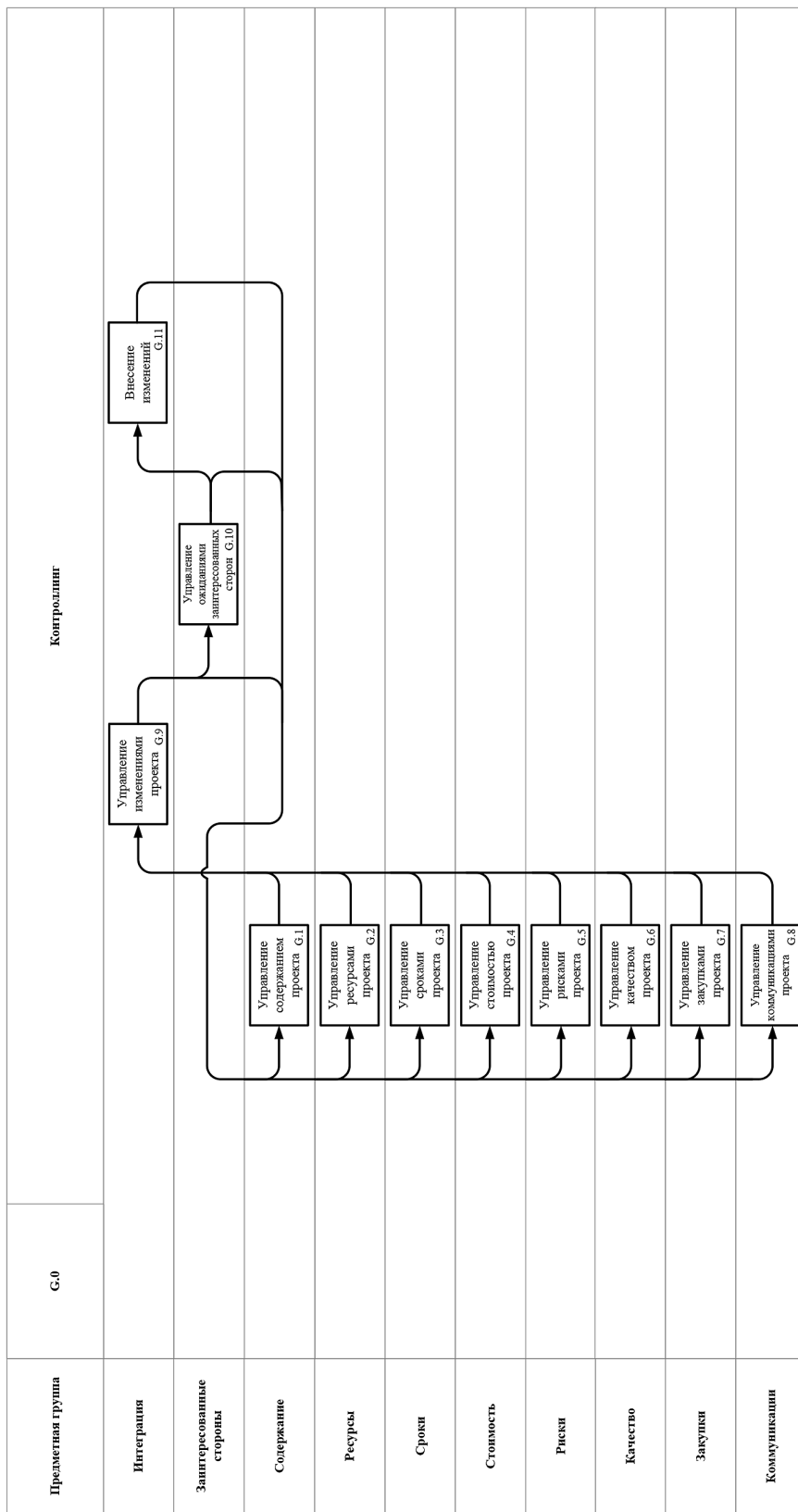


Рис. 3. G.0 — Подпроцессы контроллинга ИТ-проекта

Figure 3. G.0 — IT Project Controlling Sub-Processes

## Заключение

На основании проведенного анализа основополагающих национальных стандартов, декларирующих создание ИТ-продуктов в рамках выполнения ИТ-проектов, была разработана процессная модель создания ИТ-продуктов в рамках выполнения ИТ-проектов, где подготовка технического задания, базового плана проекта и ИТ-продукта ведется в рамках отдельных процессов и оформляется отдельными дополнительными соглашениями к контракту. Процессы модели коррелируют с фазами усовершенствованной модели жизненного цикла ИТ-проекта, что позволяет определить ключевые результаты процессов. Выявление ключевых результатов процессов позволяет оценить трудовые, материальные и финансовые ресурсы, которые необходимы для их создания, определить метрики качества, идентифицировать возможные риски и заблаговременно реализовать предупреждающие меры воздействия на них.

Процессная модель универсальна, поэтому подходит для Waterfall и Agile [29, 30]. Универсальность возможна за счет выделения процесса создания ИТ-продукта в отдельную фазу жизненного цикла ИТ-проекта «создание ИТ-продукта», где решение о способе создания ИТ-продукта ИТ-субъект определяет самостоятельно.

Модель соответствует требованиям, закрепленным в основополагающих национальных стандартах (ГОСТ Р ИСО/МЭК 12207, серия стандартов ИСО/МЭК 15504, ГОСТ Р ИСО 21500 и семейство стандартов «Проектный менеджмент»), дополняя их в части распределения процессов создания ИТ-продуктов в рамках выполнения ИТ-проектов на следующие группы: процессы, реализуемые во время фаз жизненного цикла ИТ-проекта; процессы, распределенные по предметным группам и процессы контроллинга ИТ-проекта.

Основным преимуществом разработанной процессной модели создания ИТ-продуктов в рамках выполнения ИТ-проектов перед другими моделями является возможность превентивного воздействия на риски, связанные с получением материального и (или) репутационного урона из-за досрочного прекращения работ либо отклонения от существенных условий контракта.

Кроме того была разработана модель подпроцессов создания ИТ-продуктов в рамках выполнения ИТ-проектов, включающая в себя замкнутую последовательность 62 подпроцессов, распределенных по фазам жизненного цикла ИТ-проекта и предметным группам, где каждый подпроцесс направлен на получение конкретного измеримого результата. Выявленные результаты подпроцессов позволяют оценить трудовые, материальные и финансовые ресурсы, определить метрики качества, идентифицировать возможные риски и заблаговременно реализовать превентивные меры воздействия на них.

Благодаря выявлению 62 подпроцессов удалось не только идентифицировать их результаты, потребляемые трудовые, материальные и финансовые ресурсы, метрики, риски, превентивные меры воздействия, но и определить обязательные разделы для ключевых проектных документов. Например, было установлено, что базовый план проекта должен включать в себя следующие разделы: иерархическая структура работ (ИСР), календарный план-график, диаграмма сети проекта, бюджет проекта, перечень ресурсов, организационная структура проекта, реестр рисков, меры воздействия на риски и реестр заинтересованных сторон. Некачественное, частичное выполнение либо невыполнение этого условия создает угрозу получения недостоверных значений в базовом плане проекта и искажает существенные условия контракта.

## Список источников [References]

1. Николаенко В. С. Негативные и позитивные риски в ИТ-проектах // Вестник Московского университета. Серия 21: Управление (государство и общество). 2018. № 3. С. 91–124 [Nikolaenko V.S. Negative and positive risks in IT-projects // Moscow University Bulletin. Series 21. Public Administration. 2018;(3):91–124. (In Russ.)]
2. Nikolaenko, Valentin, and Anatoly Sidorov. 2023. Analysis of 105 IT project Risks. Journal of Risk and Financial Management 16: 33. <https://doi.org/10.3390/jrfm16010033>
3. Filippov A., Romanov A., Skalkin A., Stroeva J., Yarushkina N. Approach to formalizing software projects for solving design automation and project management tasks // Software. 2023;2(1):133–162. <https://doi.org/10.3390/software2010006>
4. Вишняков О. Преимущество повторяемости: практическое руководство по бизнес-процессам: процессы и их

- описание / О. Вишняков. СПб. – М. – Минск: Питер, 2022. 302 с. ISBN 978-5-4461-1991-2 [Vishnyakov O. The advantage of repeatability: a practical guide to business processes: processes and their description / O. Vishnyakov. St. Petersburg Moscow Minsk: Peter, 2022. 302 с. ISBN 978-5-4461-1991-2. (In Russ.)]
5. Шестопал Ю. Т., Дорофеев Н. Ю., Шестопал Н. Ю., Андреева Э. А. Управление качеством: учебное пособие, М.: ИНФРА-М. 2019. 331 с. [Shestopal Yu. T., Dorofeev N. Yu., Shestopal N. Yu., Andreeva E. A. Quality management: training manual, M.: INFRA-M. 2019. 331 p. (In Russ.)]
  6. Kuhail M. A., Lauesen S. User Story Quality in Practice: A Case Study // *Software*. 2022;1(3):223-243. <https://doi.org/10.3390/software1030010>
  7. Mazur K., Saleh M., Hornung M. Integrating Life Cycle Assessment in Conceptual Aircraft Design: A Comparative Tool Analysis // *Aerospace*. 2024;11(1):101. <https://doi.org/10.3390/aerospace11010101>
  8. Truong B. Q., Nguyen-Duc A., Van N. T. C. A Quantitative review of the research on business process management in digital transformation: a bibliometric approach // *Software*. 2023;2(3):377-399. <https://doi.org/10.3390/software2030018>
  9. Zhao Z., Zhang L., Lian X., Gao X., Lv H., Shi L. Req Gen: Keywords-driven software requirements generation // *Mathematics*. 2023;11(2):332. <https://doi.org/10.3390/math11020332>
  10. Kiemel S., Rietdorf C., Schutzbach M., Mieke R. How to Simplify Life Cycle Assessment for Industrial Applications — A Comprehensive Review // *Sustainability*. 2022;14(23): 15704. <https://doi.org/10.3390/su142315704>
  11. Gładysz B., Kuchta D. Sustainable metrics in project financial risk management // *Sustainability*. 2022;14 (21):14247. <https://doi.org/10.3390/su142114247>
  12. O'Neill D. The way forward: A strategy for harmonizing agile and CMMI // *CrossTalk*. 2016;29(4):4–9
  13. Alasmari E., Martinez-Vazquez P., Baniotopoulos C. A Systematic literature review of the adoption of building information modelling (bim) on life cycle cost (LCC) // *Buildings*. 2022;12(11):1829. <https://doi.org/10.3390/buildings12111829>
  14. Gonzalez-Granadillo G., Menesidou S. A., Papamartzivanos D., Romeu R., Navarro-Llobet D., Okoh C., Nifakos S., Xenakis C., Panaousis E. Automated Cyber and Privacy Risk Management Toolkit // *Sensors*. 2021;21(16):5493. <https://doi.org/10.3390/s21165493>
  15. Дульзон А. А. Управление проектами: учебно-методическое пособие для вузов / А. А. Дульзон; М-во образования и науки Российской Федерации, Национальный исследовательский Томский политехнический ун-т. Томск: Изд-во Томского политехнического ун-та, 2013. 111 с.; ISBN 978-5-4387-0203-0 [Dulzon A. A. Project management: educational and methodological manual for universities / A. A. Dulzon; Ministry of Education and Science of the Russian Federation, National Research Tomsk Polytechnic University.— Tomsk: Publishing House of Tomsk Polytechnic University, 2013. 111 p., ISBN 978-5-4387-0203-0 (In Russ.)]
  16. Barahmand Z., Eikeland M. S. Life cycle assessment under uncertainty: a scoping review // *World*. 2022;3(3):692–717. <https://doi.org/10.3390/world3030039>
  17. Balaji S., Sundararajan Murugaiyan M. Waterfall Vs V-Model Vs Agile: a comparative on SDLC // *International Journal of Information Technology and Business Management*. 2012; 2(1):26–30.
  18. Biable S. E., Garcia N. M., Midekso D., Pombo N. Ethical issues in software requirements engineering // *Software*. 2022;1(1):31–52. <https://doi.org/10.3390/software1010003>
  19. Combéfis S. Automated code assessment for education: review, classification and perspectives on techniques and tools // *Software*. 2022;1(1):3–30. <https://doi.org/10.3390/software1010002>
  20. Agh H., Ramsin R. A Model-driven approach for software process line engineering // *Software*. 2023;2(1):21–70. <https://doi.org/10.3390/software2010003>
  21. Sahu R., Choudhari B. R., Yadav S. Usages of six sigma in library services // *Conference: Library as a Medium of Communication*. 2022. P. 1–4
  22. Kim I., Kim S., Kim H., Shin D. Mission-based cybersecurity test and evaluation of weapon systems in association with risk management framework // *Symmetry*. 2022;14(11):2361. <https://doi.org/10.3390/sym14112361>
  23. Hu K., Zhu J., Ding Y., Bai X., Huang J. Smart contract engineering // *Electronics*. 2020;9(12):2042. <https://doi.org/10.3390/electronics9122042>
  24. Полубелова М. В., Пьянкова К. А. Контроллинг: определение, цели и задачи // *Учет, анализ и аудит: проблемы теории и практики*. 2018. № 21. С. 133–137 [Polubelova M. V., Ryankova K. A. Controlling: definition, goals and tasks // *Accounting, Analysis and Audit: Problems of Theory and Practice*. 2018;(21):133–137. (In Russ.)]
  25. Просвинова Е. В. Контроллинг как система эффективного управления затратами // *Экономика и бизнес: теория и практика*. 2018. № 11-2. С. 58–60.

- <https://doi.org/10.24411/2411-0450-2018-10151>  
[Prosvirova E. V. Controlling as an effective cost management system // Economy and Business: Theory and Practice. 2018;(11–2):58–60. (In Russ.)  
<https://doi.org/10.24411/2411-0450-2018-10151>]
26. Демина И. Д. Формирование концепции контроллинга, как научной и учебной дисциплины // Инновационное развитие экономики. 2017. № 1(37). С. 151–156 [Demina I. D. Formation of the concept of controlling as a scientific and educational discipline // Innovative development of the economy. 2017;(1):151–156. (In Russ.)]
27. Wakimoto M., Morisaki S. A Metric for questions and discussions identifying concerns in software reviews // Software. 2022;1(3):364–380.  
<https://doi.org/10.3390/software1030016>
28. Menezes T. A. Review to find elicitation methods for business process automation software // Software. 2023;2(2):177–196.  
<https://doi.org/10.3390/software2020008>
29. Huss M., Herber D. R., Borky J. M. Comparing measured agile software development metrics using an agile model-based software engineering approach versus scrum only // Software. 2023;2(3):310–331.  
<https://doi.org/10.3390/software2030015>

30. Guerrero-Ulloa G., Rodríguez-Domínguez C., Hornos M. J. Agile methodologies applied to the development of internet of things (IoT)-Based systems: a review // Sensors. 2023;23(2):790. <https://doi.org/10.3390/s23020790>

## Сведения об авторе

**Николаенко Валентин Сергеевич:** кандидат экономических наук, доцент кафедры автоматизации обработки информации Томского государственного университета систем управления и радиоэлектроники, доцент Бизнес-школы Томского политехнического университета, доцент кафедры экономики, социологии, политологии и права Сибирского государственного медицинского университета

Количество публикаций: более 60

Область научных интересов: риск-менеджмент, национальная безопасность, экономическая безопасность, информационное право и защита интеллектуальной собственности, гражданское право, управление проектами

ORCID: 0000-0002-1990-4443

SPIN-код: 9301-1835

*Контактная информация:*

Адрес: 634050, г. Томск, пр. Ленина, 40

[valentin.s.nikolaenko@tusur.ru](mailto:valentin.s.nikolaenko@tusur.ru)

---

Статья поступила в редакцию: 16.08.2024

Одобрена после рецензирования: 27.09.2024

Принята к публикации: 01.10.2024

Дата публикации: 28.02.2025

*The article was submitted:* 16.08.2024

*Approved after reviewing:* 27.09.2024

*Accepted for publication:* 01.10.2024

*Date of publication:* 28.02.2025

УДК 519.213:51-77  
Научная специальность: 1.1.4; 5.2.4  
<https://elibrary.ru/lbxgrw>

ISSN 1812-5220  
© Проблемы анализа риска, 2025

# Использование распределения Бенфорда для снижения риска необнаружения искажений финансовой отчетности

**Криволапов С.Я.\*,  
Комиссарова А.В.,  
Хамула Д.А.,**

Финансовый университет  
при Правительстве  
Российской Федерации,  
125167, Россия, г. Москва,  
Ленинградский пр-т, д. 49

## Аннотация

Рассматривается совокупность числовых массивов, каждый из которых содержит данные о финансовой отчетности некоторых компаний. Для каждого массива определяются частоты появления каждой из возможных цифр в первом разряде и во втором разряде элементов массива. Несколькими способами вычисляются «расстояния» от полученных эмпирических частот до теоретических частот закона Бенфорда. На множестве точек, координатами которых являются вычисленные расстояния, осуществляется кластерный анализ, разбивающий массивы на две группы, характеризующиеся различной степенью «близости» к закону Бенфорда. Результаты кластерного анализа используются для обучения классификатора на основе логистической регрессии, который в дальнейшем применяется для прогнозирования наличия (или отсутствия) искажений в финансовой отчетности, получаемой от новых компаний.

**Ключевые слова:** закон Бенфорда; фальсификация отчетности; кластерный анализ; логистическая регрессия.

**Для цитирования:** Криволапов С.Я., Комиссарова А.В., Хамула Д.А. Использование распределения Бенфорда для снижения риска необнаружения искажений финансовой отчетности // Проблемы анализа риска. 2025. Т. 22. № 1. С. 88–95. — EDN: LTXGRW

**Авторы заявляют об отсутствии конфликта интересов**

# Using the Benford Distribution to Reduce the Risk of Undetected Misstatements of Financial Statements

**Sergey Y. Krivolapov\***,  
**Anna V. Komissarova,**  
**Daniil A. Khamula,**

Financial University under the  
Government of the Russian  
Federation,  
Leningradsky av., 49, Moscow,  
125167, Russia

## Abstract

A set of numerical arrays is considered, each of which describes the economic activities of some companies. For each array, the frequencies of occurrence of each of the possible digits in the first digit and in the second digit of the array elements are determined. The "distances" from the obtained empirical frequencies to the theoretical frequencies of Benford's law are calculated in several ways. Cluster analysis is performed on a set of points whose coordinates are calculated distances, dividing arrays into two groups characterized by varying degrees of "proximity" to Benford's law. The results of cluster analysis are used to train a classifier based on logistic regression, which is then used to predict the presence (or absence) of distortions in financial statements received from new companies.

**Keywords:** Benford's law; falsification of reports; cluster analysis; logistic regression.

**For citation:** Krivolapov S.Y., Komissarova A.V., Khamula D.A. Using the Benford distribution to reduce the risk of undetected misstatements of financial statements // *Issues of Risk Analysis*. 2025;22(1):88-95. (In Russ.). — EDN: LTXGRW

**The authors declare no conflict of interest**

## Содержание

Введение

1. Закон Бенфорда
2. «Расстояние» между распределениями
3. Предсказание на основе работы классификатора
4. Объем данных компаний

Заключение

Список источников

## Введение

Данные о финансовом состоянии организации важны как для внутренних, так и для внешних пользователей. Внешние пользователи в лице контролирующих органов, банков или инвесторов могут обращаться к бухгалтерским документам для того, чтобы проверить компанию на благонадежность и оценить, как хорошо она исполняет свои обязательства перед государством и собственными работниками.

В большинстве случаев финансовая отчетность компаний подлежит обязательному аудиту. Однако существует высокий риск того, что финансовая отчетность будет содержать искаженные данные, а аудиторская проверка не сможет гарантировать отсутствие фальсификации отчетных показателей. Существует ненулевая вероятность так называемого *аналитического риска* — риска того, что при проверке выбранной совокупности проверяемых объектов используемые аудиторские процедуры не позволят обнаружить имеющиеся ошибки.

Чтобы обеспечить сбор достаточно весомой доказательной базы для вынесения конечного вердикта компании относительно наличия каких-либо финансовых манипуляций в ее деятельности, необходим широкий инструментарий, позволяющий выявлять несоответствия в отчетности фирм. Одним из инструментов для выявления несоответствий между поддельными данными и фактическими является закон Бэнфорда или закон первой цифры [1].

Этот закон показывает вероятность появления определенной цифры в первом разряде величин, описывающих различные процессы жизнедеятельности, в том числе при составлении финансовых отчетов.

Отклонение эмпирической частоты появления цифр в первом разряде числовых данных может являться признаком наличия определенных искажений в этих показателях. Примеры и методы применения закона Бенфорда для выявления искажений в данных можно найти в работах [2–10]. В указанных работах рассматривается применение закона Бенфорда для анализа данных различных предметных областей: проверка финансовой отчетности [1–5], анализ банковских транзакций [6], контроль изображений отпечатков пальцев [7, 8], анализ контрактов [9], проверка результатов голосования [10].

Задача выявления расхождений с законом Бенфорда решается путем оценки статистической значимости

соответствия эмпирических частот цифр первого и второго разрядов чисел данных теоретическим частотам закона Бенфорда.

Недостатком такого решения является достаточно большая степень субъективности. Решение принимается на основе задаваемого пользователем уровня значимости (вероятности ошибочного отклонения гипотезы о соответствии распределения первой цифры данных распределению Бенфорда).

В представленной работе предложено решение, использующее числовую меру, характеризующую степень отличия распределения первой цифры от распределения Бенфорда для первой цифры и распределения второй цифры от распределения Бенфорда для второй цифры. В качестве такой меры используется кросс-энтропия — показатель, являющийся частью расстояния Кульбака-Лейблера. Само по себе значение кросс-энтропии не имеет содержательного описания, но его можно использовать для сравнения: если проверяются два массива числовой информации на соответствие их распределения закону Бенфорда, то массив, у которого кросс-энтропия меньше, точнее описывается этим законом.

Предлагается следующий алгоритм действий:

### 1. Исходные данные.

Берется некоторое количество массивов, содержащих финансовую отчетность различных компаний. Требования, которым должны удовлетворять массивы: они должны иметь различную степень достоверности данных, различную степень имеющихся в них искажений. Чем большее разнообразие по степени достоверности информации будет представлено в совокупности массивов, тем лучше. Оптимальным представляется набор из нескольких десятков компаний.

### 2. Вычисление признаков, численно характеризующих близость распределения цифр массивов данных к распределению Бенфорда.

Для каждого массива вычисляются два признака:  $x_1$  — кросс-энтропия между распределением первой цифры и распределением Бенфорда для первой цифры;  $x_2$  — кросс-энтропия между распределением второй цифры и распределением Бенфорда для второй цифры.

### 3. Подготовка обучающего набора данных на основе кластерного анализа.

На множестве точек  $(x_{1i}, x_{2i})$ , ( $i = 1, 2, \dots, n$ ;  $n$  — число компаний) проводится кластерный анализ, позволяющий разбить это множество на некоторое

количество кластеров (сравнительно однородных групп). Полученные кластеры можно дифференцировать по степени близости признаков  $(x_{1i}, x_{2i})$  к нулю.

#### 4. Предсказание с использованием классификатора.

Имея обучающий набор данных, можно для нового проверочного массива делать прогноз: к какому из кластеров обучающего набора относится этот массив.

Классификатор (это может быть наивный байесовский классификатор, логистическая регрессия или метод  $k$  ближайших соседей) определяет вероятности принадлежности проверочного массива данных тому или иному кластеру. В качестве предсказания подходящего кластера указывается тот, для которого была получена максимальная из вычисленных вероятностей.

В случае, когда кластерный анализ проводился с числом кластеров — два, предсказание кластера с наименьшими значениями признаков  $(x_{1i}, x_{2i})$  можно трактовать как наличие массива с достоверными данными. В случае числа кластеров больше двух можно расширить варианты ответов прогноза («массив с достоверными данными», «массив с недостоверными данными», «массив с промежуточными (неопределенными) данными»).

## 1. Закон Бенфорда

Пусть генеральная совокупность  $X$  состоит из чисел, записанных в десятичной системе счисления и имеющих, по крайней мере, два разряда ненулевой целой части. Обозначим через  $Y$  случайную величину, равную цифре, стоящей в первом разряде числа совокупности  $X$ . Закон Бенфорда [1] утверждает, что для совокупности  $X$ , основанной на данных источников реальной жизни, функция вероятности случайной величины  $Y$  имеет вид:

$$p_j = \mathbf{P}(Y = j) = \lg(j + 1) - \lg(j), j = 1, 2, \dots, 9.$$

Продemonстрируем выполнение закона Бенфорда для некоторых реальных данных. В массив  $X$  записаны данные о размере площади стран мира, вслед за которыми записаны данные о населении стран мира. На рис. 1 приведен график функции вероятности закона Бенфорда и эмпирические вероятности цифр в первом разряде чисел массива  $X$ .

Закон Бенфорда допускает обобщения на цифры, составленные из разрядов чисел, начиная со второго и далее<sup>1</sup> [11].

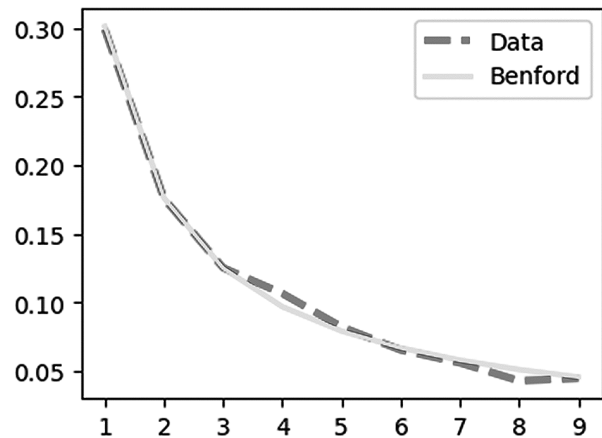


Рис. 1. График теоретических и эмпирических вероятностей первой цифры

Figure 1. Graph of theoretical and empirical probabilities of the first digit

Пусть совокупность  $X$  содержит числа, записанные в десятичной системе счисления и с целой частью, содержащей, по крайней мере, два разряда. Пусть  $Z$  — случайная величина, равная двузначному числу, составленному из первых двух разрядов. Обобщение закона Бенфорда для случайной величины  $Z$  гласит, что функция вероятности величины  $Z$  имеет вид:

$$q_l = \mathbf{P}(Z = l) = \lg(l + 1) - \lg(l), l = 10, 11, \dots, 99.$$

Предполагая справедливым закон Бенфорда для первой цифры и для первого двузначного числа, можно получить вид функции вероятности для случайной величины  $U$ , равной отдельной второй цифре числа:

$$\mathbf{P}(U = j) = \sum_{k=1}^9 \lg\left(1 + \frac{1}{10k + j}\right).$$

## 2. «Расстояние» между распределениями

Классическим способом оценки близости распределений является расстояние Кульбака-Лейблера. Для дискретных распределений  $f_k$  и  $g_k$  вычисляется по формуле:

$$D_{KL} = \sum_k f_k \ln \frac{f_k}{g_k}.$$

В нашем случае распределением  $f$  является закон Бенфорда, распределение  $g$  — эмпирические распределения, полученные из массивов данных компаний. Для нас важным является сравнительное значение

<sup>1</sup> [https://en.wikipedia.org/wiki/Benford%27s\\_law](https://en.wikipedia.org/wiki/Benford%27s_law)

«расстояний» для различных компаний. Если записать формулу для расстояния Кульбака-Лейблера в виде:

$$D_{KL} = \sum_k f_k \ln \frac{f_k}{g_k} = \sum_k f_k \ln f_k - \sum_k f_k \ln g_k,$$

можно сделать вывод, что для сравнения «расстояний» между распределением  $f$  и различными распределениями  $g$  достаточно использовать только второе слагаемое, так как первое слагаемое от распределения  $g$  не зависит.

Соответствующее выражение:

$$D = -\sum_k f_k \ln g_k$$

имеет наименование «кросс-энтропия» и используется в различных программах машинного обучения.

### 3. Предсказание на основе работы классификатора

В представленной работе рассматривается вариант разбиения данных на две группы (с числом кластеров, равным двум; массивы с достоверными данными и массивы с недостоверными данными). С учетом этого факта для целей предсказания была выбрана бинарная логистическая регрессия.

Бинарную классификацию можно визуализировать. Наши два кластера образуют два облака, отделенных друг от друга (их условно называют класс «+» и класс «-»). Между облаками проводится разделяющая их плоскость (линейный дискриминант с уравнением  $y = ax_1 + bx_2 + c$ ). При подстановке в уравнение дискриминанта координат точки, отвечающей нашему проверочному массиву, получится некоторое число  $t$ . Если оно будет положительным, точка находится со стороны класса «+», она будет отнесена к кластеру 1; в случае  $t < 0$  точка находится со стороны класса «-» и она будет отнесена к кластеру 2. Для получения вероятности отнесения точки к определенному кластеру используется логистическая функция. Вероятность попадания точки в класс «+» вычисляется по формуле:

$$P_+ = \frac{e^t}{e^t + 1}.$$

Вероятность попадания в класс «-»:  $P_- = 1 - P_+$ .

### 4. Объем данных компаний

Проверка на соответствие эмпирических частот теоретическим частотам закона Бенфорда предполагает использование большого массива данных.

При исследовании вопроса о необходимом размере массивов использовался следующий факт: закону распределения Бенфорда очень хорошо соответствуют объемы продаж акций российских компаний (их соответствие вполне сопоставимо с соответствием таких классических примеров для закона Бенфорда, как численность населения и размер площадей стран мира). На рис. 2 приведен график функции вероятности закона Бенфорда и эмпирические вероятности цифр в первом разряде чисел массивов: «Численность населения стран мира», «Объемы продаж акций компании «Башнефть»», «Объемы продаж акций компании «Лензолото»».

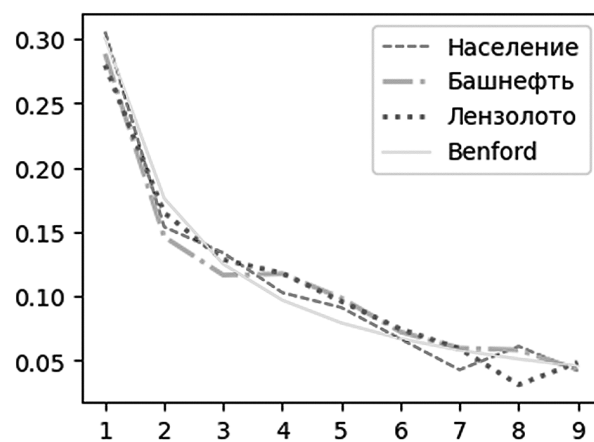


Рис. 2. Эмпирические вероятности первой цифры некоторых компаний

Figure 2. Empirical probabilities of the first digit of some companies

Данные, касающиеся объемов продаж акций, доступны в любых требуемых объемах<sup>2</sup> [12]. При увеличении длины массива данных степень соответствия закону распределения Бенфорда увеличивается. На рис. 3 приведены эмпирические вероятности первой цифры для объема продаж акций компании «Башнефть» длиной 500 и 5000.

Вычислялись значения «расстояний» (признаков  $x_1$  и  $x_2$ ) до теоретического закона распределения для массивов, содержащих объемы продаж акций различной длины (500, 1000, 2000, 3000, 4000 и 5000). Получены следующие результаты:

[[4.5138847 4.7797392]  
[3.81286855 4.08236587]  
[3.12204432 3.38687422]

<sup>2</sup> <https://mfd.ru/export/>

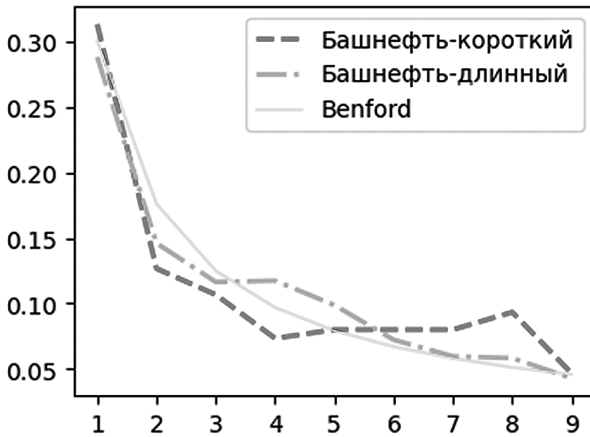


Рис. 3. Эмпирические вероятности первой цифры для данных различной длины

Figure 3. Empirical probabilities of the first digit for data of different lengths

[2.71353516 2.97866075]  
 [2.42378512 2.71024354]  
 [2.38100096 2.67878585]]

Близкие результаты были получены для данных различных компаний. Для объемов порядка  $n = 5000$  происходит стабилизация значений признаков. Все дальнейшие расчеты проводились на массивах данных объема 5000.

Демонстрация описанной процедуры на данных, содержащих сведения по 36 компаниям. Расчеты проводились на языках Python и R.

#### 1. Чтение данных.

Результат в таблице датафрейм с 36 столбцами.

#### 2. Вычисление эмпирических вероятностей.

Для каждого столбца (для каждой компании) вычисляются эмпирические вероятности (относительные частоты)  $\hat{p}_{ij}$  — появления определенной цифры в первом разряде элементов столбца и  $\hat{q}_{il}$  — появления определенной цифры во втором разряде числа,  $i = 1, 2, \dots, 36$ ;  $j = 1, 2, \dots, 9$ ;  $l = 0, 1, \dots, 9$ .

Некоторые цифры могут не встречаться в исходных данных. Чтобы исключить появление нулевых значений частот (в дальнейшем от них будет браться логарифм), нулевое значение заменялось малым положительным числом ( $10^{-5}$ ).

#### 3. Формирование признаков $x_{i1}, x_{i2}$ .

Для каждого из 36 столбцов вычисляются «расстояния» (кросс-энтропия, формула (1))  $x_{i1}, x_{i2}$  между теоретическими вероятностями закона Бенфорда

$p_{ij}, q_{il}$  и эмпирическими вероятностями  $\hat{p}_{ij}, \hat{q}_{il}$ ,  $i = 1, 2, \dots, 36$ ;  $j = 1, 2, \dots, 9$ ;  $l = 0, 1, \dots, 9$ .

$$x_{i1} = -\sum_{j=1}^9 p_{ij} \ln \hat{p}_{ij}, x_{i2} = -\sum_{l=0}^9 q_{il} \ln \hat{q}_{il}.$$

#### 4. Нормирование признаков.

Для приведения к сопоставимому виду признаки нормировались согласно формуле  $(x_i - x_{\min}) / (x_{\max} - x_{\min})$ .

Из нормированных значений признаков формировалась таблица датафрейм.

#### 5. Кластерный анализ.

На множестве точек  $(x_{i1}, x_{i2})$ ,  $i = 1, 2, \dots, 36$  проводился кластерный анализ методом  $k$ -средних с числом кластеров  $k = 2$ . Визуализация результата приведена на рис. 4.

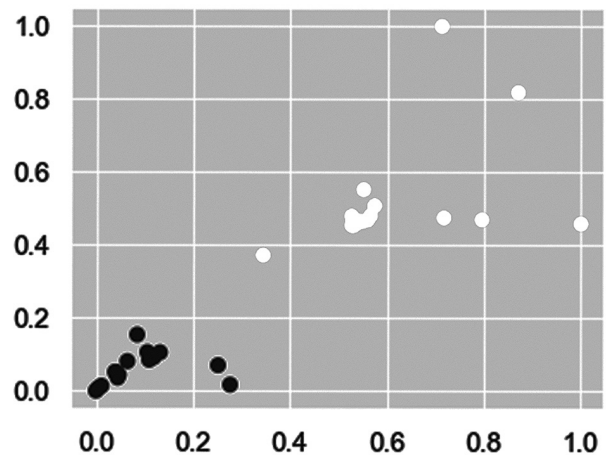


Рис. 4. Результат кластерного анализа с числом кластеров 2

Figure 4. The result of cluster analysis with the number of clusters 2

Метки кластеров:

[001000111111101010100000111110101011]

Точки кластера 0 соответствуют компаниям с малыми значениями признаков-расстояний  $x_1, x_2$ .

Результат работы — размеченная выборка: матрица признаков  $X$  размера  $36 \times 2$  и массив меток  $u$  длиной 36 (значения меток: 1 — недостоверная информация, 0 — достоверная информация).

#### 6. Выполнение предсказания.

Для выполнения предсказания о степени достоверности новых данных использовалась логистическая регрессия (функция `LogisticRegression()` пакета `sklearn.linear_model` языка Python).

Размеченные данные  $(X, y)$  делились на две части: тренировочный набор  $(X_{train}, y_{train})$  и тестовый набор  $(X_{test}, y_{test})$ . Тестовый набор формировался путем случайного выбора шести значений из размеченного набора  $(X, y)$ . В тренировочный набор вошли данные оставшихся тридцати компаний.

В целях контроля точности будущего предсказания меток тестового набора запишем, какие они имели метки после кластерного анализа.

Результат случайного выбора номеров компаний тестового набора: 3, 16, 19, 20, 29, 36. Выше был приведен массив меток. На указанных позициях стоят метки: 1, 0, 1, 0, 1, 1.

На вход классификатора подавалась размеченная тренировочная выборка  $(X_{train}, y_{train})$ .

```
from sklearn.linear_model import \
    LogisticRegression
lr = LogisticRegression()
lr_model = lr.fit(Xtrain, ytrain)
```

По обучающей выборке классификатор строит разделяющую плоскость.

Теперь, подавая на вход функции `lr.predict()` набор признаков  $X_{test}$  тестового набора, можно получить предсказание: классификатор оценит вероятность попадания точки  $(x_1, x_2)$  по одну или другую сторону разделяющей плоскости.

```
lr_predictions = lr.predict(Xtest)
Результат предсказания:
print(lr_predictions)
[1,0,1,0,1,1]
```

Все метки тестового набора предсказаны точно.

Проверим работоспособность предложенной процедуры, выполнив предсказание еще для двух массивов: первый содержит раздел финансовой отчетности компании «Роснефть»; второй — раздел отчетности компании «Трансаэро» (компании, у которой были вскрыты проблемы с отчетностью).

Вычисляем для одного и второго массивов эмпирические вероятности  $\hat{p}_{ij}, \hat{q}_{il}, i = 1, 2; j = 1, \dots, 9; l = 0, \dots, 9$  появления первой цифры и второй цифры в исходных данных. Формируем признаки («расстояния»)  $(x_{i1}, x_{i2}), i = 1, 2$  и записываем их в матрицу  $X_{test}$ . Вызываем функцию `lr.predict()`.

```
lr_predictions = lr.predict(Xtest)
Результат предсказания:
print(lr_predictions)
[0,1]
```

Для компании «Роснефть» результат: «Массив данных содержит достоверную информацию», для компании «Трансаэро»: «Массив данных содержит недостоверную информацию».

Логистический классификатор позволяет посмотреть, с какой вероятностью производится назначение определенной метки класса.

```
prob_test = lr.predict_proba(Xtest)
print(prob_test)
[[0.0528321 0.9471679]
 [0.8993031 0.1006969]]
```

В рассмотренном примере метка класса 0 (для компании «Роснефть») предсказана с вероятностью 0,947; метка класса 1 (для компании «Трансаэро») — с вероятностью 0,899.

## Заключение

В работе изложена процедура обучения и использования для предсказания классификатора, основанного на проверке близости частот цифры первого разряда и цифры второго разряда теоретическим частотам закона Бенфорда.

Для обучения классификатора был использован кластерный анализ методом  $k$ -средних с числом кластеров 2.

Вычисления, проведенные для реальных данных, содержащих сведения о финансовой отчетности компаний, показали работоспособность предложенной процедуры.

## Список источников [References]

- Кечкова И. В., Кеворкова Ж. А. Закон Бенфорда как метод выявления мошеннических действий // Молодой ученый. 2017. № 11(145). С. 219–221 [Kechkova I. V., Kevorkova J. A. Benford's law as a method of detecting fraudulent actions // Young Scientist. 2017;(11(145)):219–221. (In Russ.)]
- Назарова В. В., Чуракова И. Ю., Куприянов В. А. Проверка достоверности финансовой отчетности европейских компаний законом Бенфорда // AlterEconomics. 2023. Т. 20. № 3. С. 691–711. <https://doi.org/10.31063/AlterEconomics/2023.20–3.10> [Nazarova V. V., Churakova I. Yu., Kupriyanov V. A. Assessing financial statement reliability in european companies using Benford's law // AlterEconomics. 2023;20(3):691–711. (In Russ.). <https://doi.org/10.31063/AlterEconomics/2023.20–3.10>]

3. Зверев Е., Никифоров А. Распределение Бенфорда: выявление нестандартных элементов в больших совокупностях финансовой информации // Внутренний контроль в кредитной организации. 2018. № 4. С. 4–18 [Zverev E., Nikiforov A. Benford distribution: identification of non-standard elements in large sets of financial information // Internal control in a credit institution. 2018;(4):4–18. (In Russ.)]
4. Herteliu, C., Jianu, I., Dragan, I.M., Apostu, S. and Luchian, I. (2021). Testing Benford's Laws (non)conformity within disclosed companies' financial statements among hospitality industry in Romania. *Physica A: Statistical Mechanics and its Applications*. 582p. 126221  
<https://doi.org/10.1016/j.physa.2021.126221>
5. Durtschi, Cindy & Hillison, William & Pacini, Carl. (2004). The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data. *J. Forensic Account.* 5
6. Žgela, Mario & Krakar, Zdravko. (2009). Application of Benford's Law in Payment Systems Auditing. *Journal of Information and Organizational Sciences*. 33
7. Nigrini, M. (1996) A Taxpayer Compliance Application of Benford's Law. *The Journal of the American Taxation Association*, 18, 72–91
8. Nigrini, Mark J. and Linda Jean Mittermaier. "The Use of Benford's Law as an Aid in Analytical Procedures." *Auditing-a Journal of Practice & Theory* 16 (1997):52
9. Silva, Wilton & Travassos, Silvana & Costa, José. (2017). Using the Newcomb-Benford Law as a Deviation Identification Method in Continuous Auditing Environments: A Proposal for Detecting Deviations over Time. *Revista Contabilidade & Financas*. 28. 11–26  
<https://doi.org/10.1590/1808-057x201702690>
10. Pericchi, Luis & Torres, David. (2012). Quick Anomaly Detection by the Newcomb — Benford Law, with Applications

to Electoral Processes Data from the USA, Puerto Rico and Venezuela. *Statistical Science — STAT SCI*. 26. 10.1214/09-STS296

## Сведения об авторах

**Криволапов Сергей Яковлевич:** кандидат физико-математических наук, доцент, доцент Финансового Университета при Правительстве Российской Федерации  
Количество публикаций: 90, в т.ч. 10 учебников  
Область научных интересов: теория вероятностей, математическая статистика, анализ данных  
Scopus Author ID: MFZ-7354-2025  
ORCID: 0009-0009-4745-8047  
SPIN-код: 7149-9620

*Контактная информация:*

Адрес: 125167, г. Москва, Ленинградский пр-т, д. 49  
[skrivolapov@fa.ru](mailto:skrivolapov@fa.ru)

**Комиссарова Анна Владимировна:** студент Факультета экономики и бизнеса Финансового Университета при Правительстве Российской Федерации  
ORCID: 0009-0005-3952-4631  
SPIN-код: 3086-9234

*Контактная информация:*

Адрес: 125167, г. Москва, Ленинградский пр-т, д. 49  
[annakomissarova04@gmail.com](mailto:annakomissarova04@gmail.com)

**Хамула Даниил Александрович:** студент Факультета экономики и бизнеса Финансового Университета при Правительстве Российской Федерации  
ORCID: 0000-0001-9633-3747

*Контактная информация:*

Адрес: 125167, г. Москва, Ленинградский пр-т, д. 49  
[khamula.2003@mail.ru](mailto:khamula.2003@mail.ru)

Статья поступила в редакцию: 06.06.2024

Одобрена после рецензирования: 07.10.2024

Принята к публикации: 25.10.2024

Дата публикации: 28.02.2025

*The article was submitted: 06.06.2024*

*Approved after reviewing: 07.10.2024*

*Accepted for publication: 25.10.2024*

*Date of publication: 28.02.2025*

# Инструкция для авторов

## I. Рекомендации автору до подачи статьи

Представление статьи в журнал «Проблемы анализа риска» подразумевает, что: статья не была опубликована ранее в другом журнале; статья не находится на рассмотрении в другом журнале; статья не содержит данных, не подлежащих открытой публикации; все соавторы согласны: с публикацией текущей версии статьи.

Перед отправкой статьи на рассмотрение убедитесь, что в файле (файлах) содержится вся необходимая информация на русском и английском языках, указаны источники информации, размещенной на рисунках и таблицах, все цитаты оформлены корректно.

На титульном листе статьи размещаются (на русском и английском языках):

1. УДК статьи.
2. Имя автора (авторов).
3. Информация об авторе (авторах).

В этом разделе перечисляются: фамилия, имя и отчество (полностью), степень, звание и занимаемая должность, полное и краткое наименование организации, число публикаций, в том числе монографий, учебных изданий, область научных интересов, контактная информация: почтовый адрес (рабочий), телефон, e-mail, моб. телефон ответственного автора для связи с редакцией.

### 4. Аффiliation автора (авторов).

Аффiliation включает в себя следующие данные: полное официальное название организации, полный почтовый адрес (включая индекс, город и страну). Авторам необходимо указывать все места работы, имеющие отношение к проведению исследования. Если в подготовке статьи принимали участие авторы из разных учреждений, необходимо указать принадлежность каждого автора к конкретному учреждению с помощью надстрочного индекса. Необходимо официальное англоязычное название учреждения для блока информации на английском языке.

### 5. Название статьи.

Название статьи на русском языке должно соответствовать содержанию статьи. Англоязычное название должно быть грамотно с точки зрения английского языка, при этом по смыслу полностью соответствовать русскоязычному названию.

### 6. Аннотация.

Рекомендуемый объем структурированной аннотации: 200–250 слов. Аннотация содержит следующие разделы: Цель, Методы, Результаты, Заключение.

### 7. Ключевые слова.

5–7 слов по теме статьи. Желательно, чтобы ключевые слова дополняли аннотацию и название статьи.

### 8. Конфликт интересов.

Автор обязан уведомить редактора о реальном или потенциальном конфликте интересов, включив информацию о конфликте интересов в соответствующий раздел статьи. Если конфликта интересов нет, автор должен также сообщить об этом. Пример формулировки: «Автор заявляет об отсутствии конфликта интересов».

### 9. Текст статьи.

В журнале принят формат IMRAD (Introduction, Methods, Results, Discussion — Введение, Методы, Результаты, Обсуждение) Основной текст статьи должен содержать:

- введение,
- структурированные, пронумерованные разделы статьи,
- заключение,
- литературу.

### 10. Рисунки.

Рисунки должны быть хорошего качества, пригодные для печати. Все рисунки должны иметь подрисночные подписи. Подрисночная подпись должна быть переведена на английский язык. Рисунки нумеруются арабскими цифрами по порядку следования в тексте. Если рисунок в тексте один, то он не нумеруется. Перевод подрисночной подписи следует располагать после подрисночной подписи на русском языке.

### 11. Таблицы.

Таблицы должны быть хорошего качества, пригодные для печати. Предпочтительны таблицы, пригодные для редактирования, а не отсканированные или в виде рисунков. Все таблицы должны иметь заголовки. Название таблицы должно быть переведено на английский язык. Таблицы нумеруются арабскими цифрами по порядку следования в тексте. Если таблица в тексте одна, то она не нумеруется. Заголовок таблицы включает порядковый номер таблицы и ее название. Перевод заголовка таблицы следует располагать после заголовка таблицы на русском языке.

### 12. Скриншоты и фотографии.

Фотографии, скриншоты и другие нарисованные иллюстрации необходимо загружать отдельно в специальном разделе формы для подачи статьи в виде файлов формата \*.jpeg, \*.bmp, \*.gif (\*.doc и \*.docx — в случае, если на изображение нанесены дополнительные пометки). Разрешение изображения должно быть >300 dpi. Файлам изображений необходимо присвоить название, соответствующее номеру рисунка в тексте. В описании файла следует отдельно привести подрисночную подпись, которая должна соответствовать названию фотографии, помещаемой в текст.

### 13. Сноски.

Сноски нумеруются арабскими цифрами, размещаются постранично. В сносках могут быть размещены: ссылки на анонимные источники в сети Интернет, ссылки на учебники, учебные пособия, ГОСТы, статистические отчеты, статьи в общественно-политических газетах и журналах, авторефераты, диссертации (если нет возможности процитировать статью, опубликованные по результатам диссертационного исследования), комментарии автора.

### 14. Список литературы.

В журнале используется Ванкуверский формат цитирования, который подразумевает отсылку на источник в квадратных скобках и последующее упоминание источников в списке литературы в порядке

упоминания. Страница указывается внутри скобок, через запятую и пробел после номера источника: [6, с. 8]. В список литературы включаются только рецензируемые источники (статьи из научных журналов и монографий), упоминающиеся в тексте статьи. Нежелательно включать в список литературы авторефераты, диссертации, учебники, учебные пособия, ГОСТы, информацию с сайтов, статистические отчеты, статьи в общественно-политических газетах, на сайтах и в блогах. Если необходимо сослаться на такую информацию, следует поместить информацию об источнике в сноску. При описании источника следует указывать его DOI, если удается его найти (для зарубежных источников удается это сделать в 95% случаев). Ссылки на принятые к публикации, но еще не опубликованные статьи должны быть помечены словами «в печати»; авторы должны получить письменное разрешение для ссылки на такие документы и подтверждение того, что они приняты к печати. Информация из неопубликованных источников должна быть отмечена словами «неопубликованные данные/документы», авторы также должны получить письменное подтверждение на использование таких материалов. В ссылках на статьи из журналов должны быть обязательно указаны год выхода публикации, том и номер журнала, номера страниц. В описании каждого источника должны быть представлены все авторы. Ссылки должны быть верифицированы, выходные данные проверены на официальном сайте журналов и/или издательств. Необходим перевод списка литературы на английский язык. После описания русскоязычного источника в конце ссылки ставится указание на язык работы: (In Russ.). Для транслитерации имен и фамилий авторов, названий журналов следует использовать стандарт BS.

## II. Как подать статью на рассмотрение

Рукопись статьи направляется в редакцию через online форму или в электронном виде на e-mail [parjournal@mail.ru](mailto:parjournal@mail.ru). Загружаемый в систему направляемый на электронную почту файл со статьей должен быть представлен в формате Microsoft Word (иметь расширение \*.doc, \*.docx, \*.rtf).

## III. Взаимодействие между журналом и автором

Редакция журнала ведет переписку с ответственным (контактным) автором, однако при желании коллектива авторов письма могут направляться всем авторам, для которых указан адрес электронной почты. Все поступающие в журнал «Проблемы анализа риска» статьи проходят предварительную проверку ответственным секретарем журнала на соответствие формальным требованиям. На этом этапе статья может быть возвращена автору (авторам) на доработку с просьбой устранить ошибки или добавить недостающие данные. Также на этом этапе статья может быть отклонена из-за несоответствия ее целям журнала, отсутствия оригинальности, малой научной ценности. После предварительной проверки ответственный редактор передает статью рецензенту с указанием сроков рецензирования. Автору отправляется соответствующее уведомление. При положительном заключении рецензента статья передается редактору для подготовки к печати. При принятии решения о доработке статьи замечания и комментарии рецензента передаются автору. Автору дается 2 месяца на устранение замечаний. Если в течение этого срока автор не уведомил редакцию о планируемых действиях, статья снимается с очереди публикации. При принятии решения об отказе в публикации статьи автору отправляется соответствующее решение редакции. Ответственному (контактному) автору принятой к публикации статьи направляется финальная версия верстки, которую он обязан проверить. Ответ ожидается от авторов в течение 2 суток. При отсутствии реакции со стороны автора верстка статьи считается утвержденной.

## IV. Порядок пересмотра решений редактора/рецензента

Если автор не согласен с заключением рецензента и/или редактора или отдельными замечаниями, он может оспорить принятое решение. Для этого автору необходимо:

- исправить рукопись статьи согласно обоснованным комментариям рецензентов и редакторов;
- ясно изложить свою позицию по рассматриваемому вопросу.

Редакторы содействуют повторной подаче рукописей, которые потенциально могли бы быть приняты, однако были отклонены из-за необходимости внесения существенных изменений или сбора дополнительных данных, и готовы подробно объяснить, что требуется исправить в рукописи для того, чтобы она была принята к публикации.

## V. Действия редакции в случае обнаружения плагиата, фабрикации или фальсификации данных

В случае обнаружения недобросовестного поведения со стороны автора, обнаружения плагиата, фабрикации или фальсификации данных редакция руководствуется правилами COPE. К «недобросовестному поведению» журнал «Проблемы анализа риска» не относит честные ошибки или честные расхождения в плане, проведении, интерпретации или оценке исследовательских методов или результатов, или недобросовестное поведение, не связанное с научным процессом.

## VI. Исправление ошибок и отзыв статьи

В случае обнаружения в тексте статьи ошибок, влияющих на ее восприятие, но не искажающих изложенные результаты исследования, они могут быть исправлены путем замены pdf-файла статьи и указанием на ошибку в самом файле статьи и на странице статьи на сайте журнала. В случае обнаружения в тексте статьи ошибок, искажающих результаты исследования, либо в случае плагиата, обнаружения недобросовестного поведения автора (авторов), связанного с фальсификацией и/или фабрикацией данных, статья может быть отозвана. Инициатором отзыва статьи может быть редакция, автор, организация, частное лицо. Отзыванная статья помечается знаком «Статья отозвана», на странице статьи размещается информация о причине отзыва статьи. Информация об отзыве статьи направляется в базы данных, в которых индексируется журнал.

Подробная инструкция на сайте <https://www.risk-journal.com>