ISSN 2686-679X

ВЕСТНИК РГГУ

Серия
«Информатика.
Информационная безопасность.
Математика»

Научный журнал

RSUH/RGGU BULLETIN

"Information Science.
Information Security. Mathematics"
Series

Academic Journal

Основан в 2018 г.
Founded in 2018

2
2023

VESTNIK RGGU. Seriya “Informatica. Informacionnaya bezopasnost. Matematica”

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” Series
Academic Journal

There are 4 issues of the printed version of the journal a year.

Founder and Publisher
Russian State University for the Humanities (RSUH)

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is included: in the Russian Science Citation Index. Peer-reviewed publications fall within the following research area:

20.00.00 Informatics

81.93.29 Information security, data protection

27.00.00 Mathematics

Objectives and areas of research

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series publishes the results of research by scientists from RSUH and other universities and other Russian and foreign academic institutions. The areas covered by contributions include theoretical and applied computer science, up-to-date IT, means and technologies of information protection and information security as well as the issues of theoretical and applied mathematics including analytical and imitation models of different processes and objects. Special emphasis is put on articles and reviews covering research in indicated directions in the areas of social and humanitarian problems and also issues of personnel training for these directions.

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is registered by Federal Service for Supervision of Communications Information Technology and Mass Media. 25.05.2018, reg. No. FS77-72977

Editorial staff office: 6, Miusskaya sq., Moscow, Russia, 125047
e-mail: grnat@rambler.ru

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика»
Научный журнал

Выходит 4 номера печатной версии журнала в год.

Учредитель и издатель – Российский государственный гуманитарный университет (РГГУ)

ВЕСТНИК РГГУ, серия «Информатика. Информационная безопасность. Математика», включен: в систему Российского индекса научного цитирования (РИНЦ). Научные рецензируемые публикации соответствуют отраслям науки:

20.00.00 Информатика

81.93.29 Информационная безопасность, защита информации

27.00.00 Математика

Цели и область

В журнале «Вестник РГГУ», серия «Информатика. Информационная безопасность. Математика» публикуются результаты научных исследований ученых и специалистов РГГУ, а также других университетов и научных учреждений России и зарубежных стран. Направления публикаций включают теоретическую и прикладную информатику, современные информационные технологии, методы, средства и технологии защиты информации и обеспечения информационной безопасности, а также проблемы теоретической и прикладной математики, включая разработку аналитических и имитационных моделей процессов и объектов различной природы. Особое внимание уделяется статьям и обзорам, посвященным исследованиям по указанным направлениям в области социальных и гуманитарных проблем, а также вопросам подготовки кадров по соответствующим специальностям для данных направлений.

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика», зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 25.05.2018 г., регистрационный номер ПИ № ФС77-72977.

Адрес редакции: 125047, Россия, Москва, Миусская пл., 6

электронный адрес: grnat@rambler.ru

Учредитель и издатель
Российский государственный гуманитарный университет (РГГУ)

Ответственный за выпуск:

Н.В. Гришина, кандидат технических наук, доцент,
Российский государственный гуманитарный университет (РГГУ)

CONTENTS

СОДЕРЖАНИЕ

УДК 004.4
DOI: 10.28995/2686-679X-2023-2-8-29

Расширение нотации IDEF0 для функционального описания динамических систем

Владимир А. Бочаров
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, bocharovva@student.bmstu.ru

Тамара М. Волосатова
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, tamaravol@gmail.com

Аннотация. Разработка правил переходов между этапами проектирования динамических систем – цели потребителя системы, системные требования, технические решения и потребительские свойства систем – остается одним из самых важных аспектов проектирования сложных систем. В статье реализовано расширение нотации IDEF0 – системы обозначений для функций и их составных частей. Для более детального функционального описания динамических систем реализовано расширение семантического языка нотации. Данное расширение позволяет получить более детализированную информацию о системе в целом, а также создает связи между функциональной и поведенческими моделями. Расширенная семантика применена для проектирования функционального описания авиационных частей самолетов. Также расширение нотации является компонентом разрабатываемой системы по управлению жизненным циклом, которое, в частности, должно решить проблему дефицита инженерной семантики, не позволяющий обеспечить в процессах разработки соответствие между требованиями и техническими решениями, верификацию этих отношений и валидацию разрабатываемой системы. В результате расширения нотации IDEF0 формируются новые, расширенные свойства модели системы, которые способствуют решению задач валидации и верификации в процессах разработки сложных технических систем. Специализация исходных данных, данных управления и данных результатов работы функции расширили возможность контролировать правильность принимаемых при разработке системы решений.

Ключевые слова: системный инжиниринг, IDEF0, функции, требования, цели, связи

Для цитирования: Бочаров В.А., Волосатова Т.М. Расширение нотации IDEF0 для функционального описания динамических систем // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 2. С. 8–29. DOI: 10.28995/2686-679X-2023-2-8-29

Extension of the IDEF0 notation of the functional description of dynamical systems

Vladimir A. Bocharov
Bauman Moscow State Technical University, Moscow, Russia,
bocharovva@student.bmstu.ru

Tamara M. Volosatova
Bauman Moscow State Technical University, Moscow, Russia,
tamaravol@gmail.com

Abstract. The development of rules for transitions between the design stages of dynamic systems: the goals of the system consumer, system requirements, technical solutions and consumer properties of systems, remains one of the most important aspects in the design of complex systems. The article implements an extension of the IDEF0 notation – a notation system for functions and their components. For a more detailed functional description of dynamic systems, an extension of the semantic notation language is introduced. Such an extension allows getting more detailed information about the system as a whole, and creates links between the functional and behavioral models. Extended semantics is applied to the design of functional descriptions of the aircraft parts. The notation extension is also a component of the lifecycle management system under development, that, in particular, should solve the issue of engineering semantics deficiency, not allowing to ensure in the elaborating processes the correspondence between requirements and technical solutions, the verification of those relationships and the validation of the system being developed. As a result, the expansion of the IDEF0 notation, new, expanded properties of the system model will be formed, which contribute to solving validation and verification problems in the development of complex technical systems.

Keywords: system engineering, IDEF0, functions, requirements, goals, connections

For citation: Bocharov, V.A. and Volosatova, T.M. (2023), "Extension of the IDEF0 notation of the functional description of dynamical systems", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 8–29, DOI: 10.28995/2686-679X-2023-2-8-29

Введение

В разработке сложной наукоемкой системы есть важные составляющие для ее внедрения: начиная от времени разработки до запуска системы в эксплуатацию и заканчивая обнаружением скрытых потребностей и последующим выполнением требований заказчиков. Перечисленные выше составляющие необходимо учитывать с самого первого этапа разработки, когда из технического задания заказчика необходимо сформировать требования, цели и структуру системы, которые непосредственно влияют на последующие этапы проектирования. Для выполнения данного этапа используется комплексная методология «системный инжиниринг» [Manenti, Ebrahimiarjestan, Yang, Yu 2019].

Системный инжиниринг (Systems Engineering, SE), управляющий всеми техническими и управленческими этапами, необходимыми для преобразования набора потребностей, ожиданий и ограничений заказчика в решение и поддержку этого решения на протяжении всей его жизни, является важным элементом при разработке наукоемкой продукции[1]. Системная инженерия необходима, так как позволяет решить три проблемы инженерии: проблему сложности (недооценки сложности проекта), проблему непонимания (целей проекта, отношений внутри элементов системы, решения проблем, возникших в течение жизненного цикла проекта) и проблему коммуникации (между инженерами в команде, между организациями, внутри проекта), что было доказано во многих исследованиях (например, Suranto 2015) [Suranto 2015]. В связи с этим совершенствование SE способствует более эффективному процессу разработки сложной системы.

Инженерное проектирование в значительной степени зависит от модели разработки системы и процессов, методов и инструментов, которые поддерживают его. Предприятия ожидают, что инженерное проектирование системы будет происходить максимально легко и предсказуемо, а где это необходимо, будут внесены соответ-

[1] ISO/IEC/IEEE 24765 Systems and software engineering – Vocabulary, 2017 // ISO. URL: https://www.iso.org/standard/71952.html (дата обращения 2 февраля 2023).

ствующие изменения. Стандарт системной инженерии ISO-15288 определяет общие и стандартные процессы системного проектирования, которые подходят для разных областей приложения[2]. Международным советом по системной инженерии подготовлено «Руководство по системной инженерии INCOSE» (далее именуемое «Руководство INCOSE»), в котором подробно описывается применение стандарта и предоставляются рекомендации по адаптации и масштабированию данных процессов [Walden, Roedler, Forsberg, Hamelin, Shortell 2015].

В настоящее время руководство INCOSE (текущее издание – версия 4, 2015 г.) во многих организациях становится основным справочником по созданию документов внутреннего процесса системного проектирования [Walden, Roedler, Forsberg, Hamelin, Shortell 2015]. Но его недостаток состоит в чрезвычайной сложности, являющейся препятствием для потенциальных пользователей (особенно новичков в системной инженерии) и не позволяющей быстро получить исчерпывающее представление о системной инженерии и ее приложениях. В частности, руководство INCOSE описывает процессы жизненного цикла линейно и последовательно, используя схемы Input-Process-Output (IPO), но без общей картины того, как они связаны [Brook 2015; Walden, Roedler, Forsberg, Hamelin, Shortell 2015].

Но самая главная проблема SE и подобных ему современных методологий в том, что они работают в пределах четырех этапов проектирования систем: цели потребителя системы, системные требования, технические решения и потребительские свойства систем, но не решают проблему переходов между данными этапами, что приводит к неоптимальному результату, долгому проектированию системы и частым ошибкам, как, например, при разработке американского самолета F-35. Примером проблемы, которая возникает при отсутствии правильного перехода между системными требованиями и техническим решением, может служить проблема 25-мм пушки, установленной на F-35, так как ее точность не соответствует требованиям из-за плохого крепления, которое часто растрескивается и перекашивается. Возможной причиной возникновения данной проблемы (фактически невыполнения ТЗ) может служить несогласованность технического решения и требований. Поэтому целью данной работы является обзор возможных методологий создания сложных систем (в частности, авиационного бортового

[2]ISO/IEC/IEEE 15288 Systems and software engineering – System life cycle processes, 2015 // ISO. URL: https://www.iso.org/standard/63711.html (дата обращения 2 февраля 2023).

оборудования), которые позволили бы связать все этапы определенными правилами и привели бы к следующим результатам:

– сделает процесс разработки регулярным: подчинит его заранее подготовленному и утвержденному процессу, использующему проверенные методы;
– позволит проверить, что каждое действие в ходе процесса разработки обосновано и не выходит за рамки установленных порядков, а его результат не противоречит поставленным целям;
– позволит проверять выбор вариантов реализации из множества возможных, используя аналитические методы.

Новизна данной работы заключается в том, что это позволит расширить семантику языка моделирования динамических систем, что приведет к детализации информации о системе в целом, а также создаст связи между функциональной и поведенческими моделями.

В настоящее время в разных работах [Chein, Mugnier 2009; Buche, Fortin, Gutierrez 2014; Huth, Mark 2000; Goknil, Kurtev, Berg 2016; Fagin, Halpern, Moses, Vardi 2003; Wolfgang 2010; Yang, Cormican, Yu 2017; Rumbaugh 2003] идет изучение семантических связей, которые существуют при моделировании динамических систем, что позволило выявить, какие отношения с какими свойствами лежат в основе семантики функций, но не было работ, идущих на создание или расширение семантики, которая позволила бы создать связи между функциональной и поведенческими моделями.

В некоторых работах [Buche, Fortin, Gutierrez 2014; Huth, Mark 2000; Goknil, Kurtev, Berg 2016; Fagin, Halpern, Moses, Vardi 2003] рассмотрена нотация функционального описания систем IDEF0 и сделан анализ ее преимуществ и недостатков. Сделан вывод, что система в целом может быть составлена из элементов деятельности, имеющих четыре составные части – исходные данные, управление, механизмы и результаты работы, соединенные друг с другом по входам, выходам и управлению. Проверить состоятельность (работоспособность) системы, имея ее описание в IDEF0, можно лишь в объеме сведений о системе как о «черном ящике». Природу внутренних возможностей и ограничений системы исследовать нельзя в силу недостатка информации о данных и процессах их обработки. Поэтому в данной статье задачей является детализация представления о составных частях элемента деятельности, опираясь на IDEF0 как на основу, и анализ, какие новые возможности это может дать разработчику систем.

Автоматизированная информационная система управления жизненным циклом

В мире существует большое число различных систем (Teamcenter, T-FLEX, Лоцман, Enovia и другие), которые помогают разработчикам следить за процессом разработки сложных динамических систем, частью которого является этап функционального описания. Однако эти системы имеют ряд недостатков.

1. Дефицит доверия к данным, обусловленный неопределенностью их происхождения, копированием, интерпретацией, трактовками и иными трансформациями содержания в процессе движения информации (Проблема отношения «*оригинал – копия*»).

2. Проблема формы и содержания, когда одно и то же смысловое содержание, представленное в разных формах и читаемое с точки зрения разных предметных областей, может быть интерпретировано по-разному.

3. Терминологические противоречия между различными предметными областями (Проблема отношения «*термин – значение*»).

4. Дефицит инженерной семантики, не позволяющий обеспечить в процессах разработки соответствие между требованиями и техническими решениями, верификацию этих отношений и валидацию разрабатываемой системы.

5. Дефицит связей между целевой системой и ее прототипами (макетами, цифровыми двойниками, экспериментальными образцами и иными формами моделей) с учетом принятых допущений и упрощений (адекватности модели).

6. Дефицит связей предмета деятельности со знаниями предметной области – научно-техническими заделами (научными теориями, технологиями на промежуточных уровнях готовности, опытами и экспериментами). Основной вид отношения – «*теория – практика*».

7. Дефицит связей предмета научно-технической деятельности со свойствами людей и коллективов, осуществляющих эту деятельность, такими как *компетенция*, *полномочия* и *ответственность* (инженерная этика).

Из-за перечисленных проблем появился проект по разработке Автоматизированной Информационной Системы Управления Жизненным Циклом (АИС УЖЦ) [Автоманов, Попов 2017], который должен решить данные проблемы, в том числе и проблемы, связанные с описанием функциональной модели динамических систем. Схема системы представлена на рис. 1.

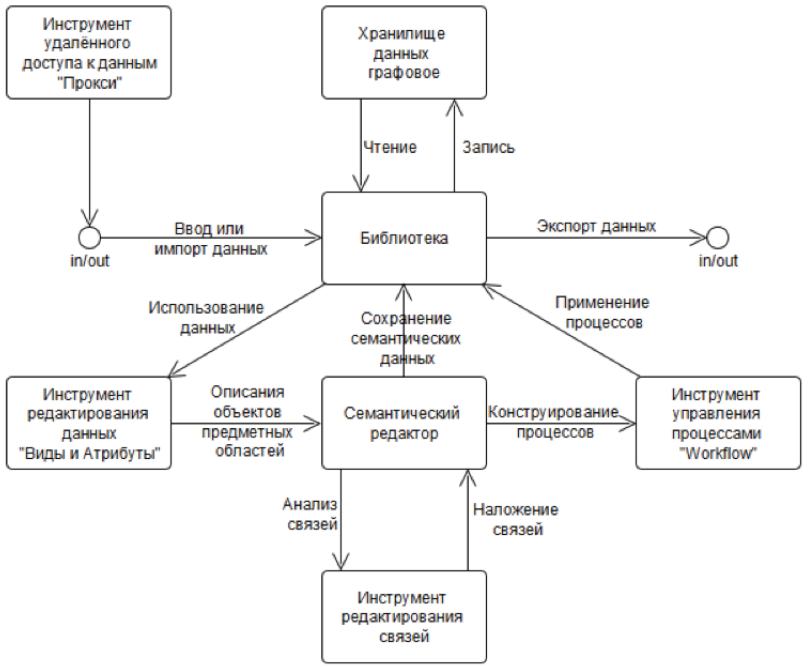

Рис. 1. Схема системы АИС УЖЦ
(семантический редактор, который на входе получает данные
от подсистемы «Виды и Атрибуты», а на выходе выдает данные
для построения процесса в “Workflow”, а также связан
с «Инструментом редактирования связей»
и подсистемой хранения данных «Библиотека»)

Для реализации инструмента «Семантический редактор» была взята за основу нотация IDEF0[3]. Нотация была проанализирована, выделены шаги для ее доработки, так как в изначальном варианте она не позволяет решить все необходимые проблемы, которые встают перед инженерами для описания функциональной модели.

[3] INTEGRATION DEFINITION FOR FUNCTION MODELING (IDEF0). Draft Federal Information Processing Standards Publication 183. December. 1993. URL: https://archive.org/details/federalinformati183nati/page/n9/mode/2up (дата обращения 2 февраля 2023).

Расширение специализации данных нотации IDEF0

Для расширения возможностей анализа системы в нотации IDEF0 детализируем определения некоторых ее составных частей.

1. Разделим *исходные данные* по своей роли в исполняемой функции на две части – принимаемые извне системы и передаваемые от функции к функции внутри системы.

2. Разделим *управление* на целевое, выполняемое всей системой в интересах ее потребителя, и регулирование – внутреннее изменение режимов работы функций, необходимое для корректной работы самой системы.

3. Разделим *результат исполнения* функции на предметные данные, данные управления и данные регулирования, влияющие на исполнение функций системы.

4. Разделим *механизмы* на исполняющие целевую функцию при заданном управлении и меняющие параметры других функций для приведения их к предусмотренной норме.

Общий вид *функционального элемента* системы показан на рис. 2.

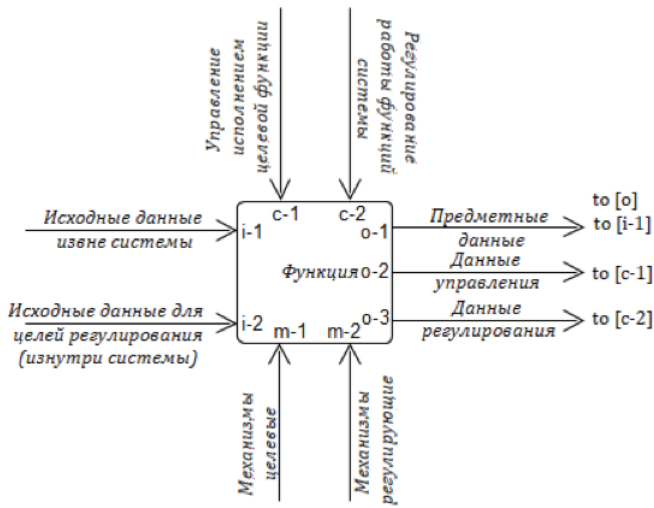

Рис. 2. Расширенное представление обобщенного функционального элемента диаграммы в нотации IDEF0

Расширение нотации IDEF0 обеспечивает возможность не только определить саму функцию, но и наложить ограничение на ее применение. Например, задать условие применения исходных данных по их назначению или обусловить выполнение действий над исходными данными только в соответствии с предусмотренными процессами.

Функции системы соответственно могут быть соединены друг с другом таким образом, как показано на рис. 3.

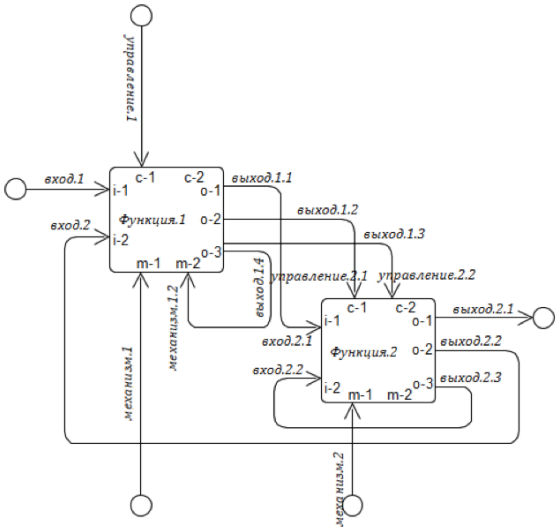

Рис. 3. Схема возможных взаимодействий простейшей системы, состоящей из двух взаимосвязанных функций

Как видно из схемы на рис. 3, начальные исходные данные имеют двухшаговый путь преобразования от *вход.1* к *выход.2*, который имеет промежуточный выход из первой функции *выход.1.1*, направленный на вход второй функции *вход.2.1*. При этом первая функция управляется извне (*управление.1*), а управление второй функции зависит от итога работы первой функции: *выход.1.2 -> управление.2.1* и *выход.1.3 -> управление.2.2*.

На рис. 3 также показаны примеры, как выход функции *выход.1.4* может служить «настройке» механизма *механизм.1.2* (первая функция) и как выход функции *выход.2.3* может возвращаться на вход в функцию *вход.2.2*, когда реализуется обратная связь для самоконтроля.

Как видно из приведенного примера, в графическом и формальном описании систем можно выделять в обособленную группу и рассматривать раздельно пути преобразования предметных данных, контуры управления и контуры регулирования системы. Это дает возможность проверять конструкцию системы раздельно по данным, управлению и регулированию, а также привязать оборот данных к словарям предметной области, требованиям и ограничениям и взаимодействиям с внешним миром. В результате проверки можно выделять и анализировать цепочки связей, проходящие сквозь систему, в форме размеченного графа, как показано на рис. 4.

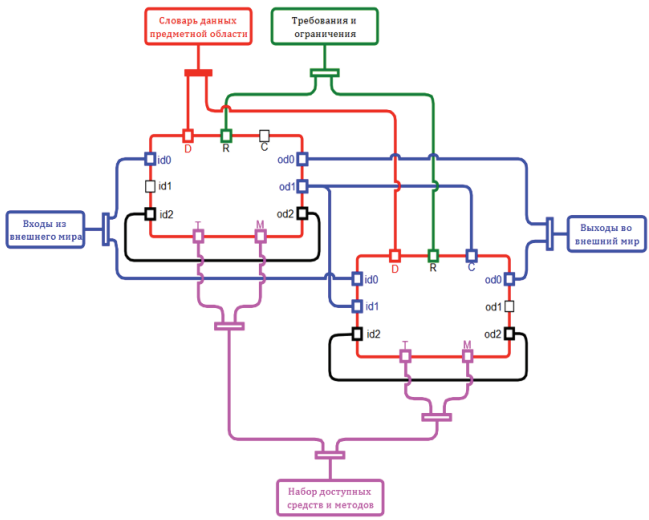

Рис. 4. Пример выделения функциональных связей при анализе системы

Условные обозначения на рис. 4:
id – input data, входные данные;
od – output data, выходные данные – результаты выполнения функции;
D – dictionary, словарь объектов данных;
R – requirements, требования;
C – control, управляющее воздействие;
T – tools, средства исполнения функции;
M – method, методы преобразования id в od под управлением C.

Пусть есть система из двух взаимосвязанных функциональных модулей, обозначенных красными прямоугольниками. Они ссылаются на общий словарь предметной области, используя из него понятия и отношения соответственно своему предназначению. Каждый модуль использует свое подмножество терминов.

Движение предметных данных начинается на входе из внешнего мира и завершается на выходе во внешний мир, претерпевая по пути два последовательных преобразования и подвергаясь двум прецедентам управления и регулирования.

Преобразование предметных данных осуществляется на основании требований и ограничений, обозначенных зелеными прямоугольниками, которые разделены таким образом, что реализация последующих требований зависит от реализации предшествующих.

Исполнение функций преобразования предметных данных, данных управления и данных регулирования обеспечивается набором доступных средств и методов/механизмов.

Разметка цветами на рис. 4 дает наглядную возможность оценить целостность системы с точки зрения наличия отношений с внешним миром, требованиями и механизмами с одной стороны, и проконтролировать пути движения данных – с другой.

Примеры использования расширенной нотации IDEF0 к авиационным системам

Рассмотрим в качестве примера две подсистемы «Летательного аппарата» (ЛА) – шасси и закрылки. Вначале представим ЛА как набор состояний и переходов, как показано на рис. 5.

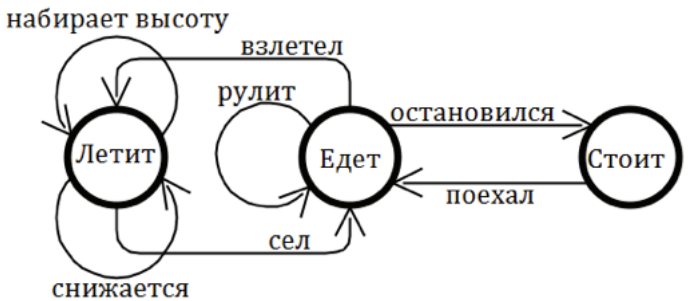

Рис. 5. Обобщенная модель системы «Летательный аппарат» в терминах состояний и переходов

Роль шасси состоит в компенсации массово-инерционной нагрузки через реакцию опоры земли, управлять движением на земле («ехать») и поглощать кинетическую энергию ЛА при посадке. Функциональная система ЛА представлена на рис. 6.

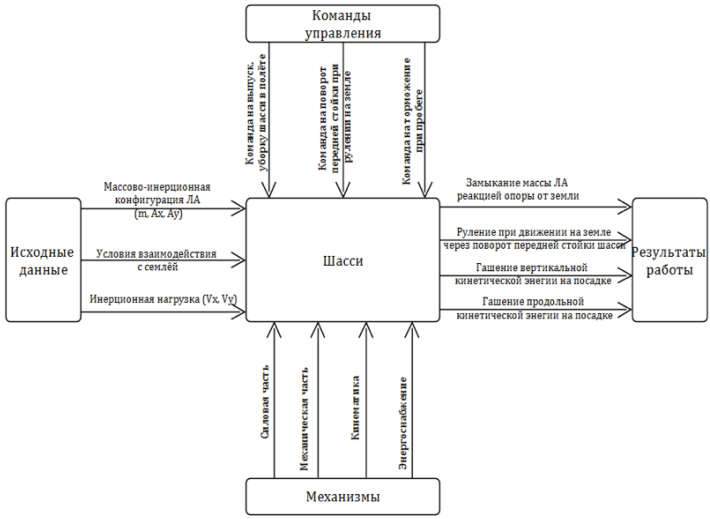

Рис. 6. Функциональная схема системы ЛА «Шасси»

Назначение системы ЛА «Шасси», показанной на рис. 6:
- замыкание массы ЛА реакцией опоры от земли;
- контроль направления движения на земле через поворот передней стойки шасси;
- гашение вертикальной кинетической энергии на посадке (не требует управления);
- гашение продольной кинетической энергии на посадке (торможение на пробеге);
- команды управления (управляющие воздействия на систему);
- команда на выпуск, уборку шасси в полете;
- команда на поворот передней стойки при рулении на земле (педали);
- команда на торможение при пробеге.

Исходные данные для работы (переменные): массово-инерционная конфигурация ЛА (масса m, положение центра масс); условия взаимодействия с землей; инерционная нагрузка (путевая скорость Vx, вертикальная скорость Vy).

Механизмы (логические части механизмов):
- передачи массово-инерционной нагрузки от ЛА в землю (силовая часть);
- механическая часть (тела, механические связи, степени свободы);
- кинематика (уборки/выпуска, разворота, обжатия амортизатора, тормоза);
- энергоснабжение (привода уборки/выпуска, привода тормоза, датчиков).

Система шасси реализует поведение, как показано на рис. 7.

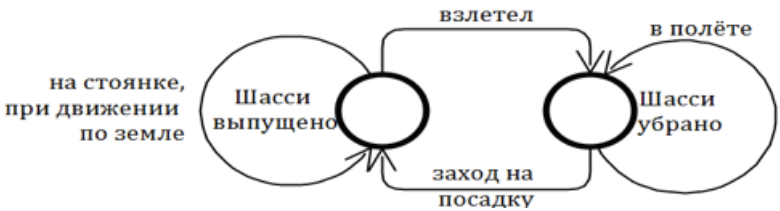

Рис. 7. Схема работы шасси, где «движение по земле» включает в себя буксировку, руление, разбег и пробег.

Роль закрылков в составе ЛА по определению – управлять коэффициентом подъемной силы крыла при изменениях скоростного напора набегающего потока воздуха с тем, чтобы располагаемая подъемная сила крыла всегда была больше силы тяжести ЛА.

Конструкция и углы отклонения закрылков зависят от массово-инерционной и аэродинамической конфигурации ЛА и в техническое задание на проектирование попадают, как предварительно исследованная зависимость углов отклонения от условий полета. Предположим, что данная зависимость:

1. Стоянка, крейсерский полет – 0 градусов.
2. Взлет, заход на посадку – 15 градусов.
3. Посадка – 40 градусов.

Назначение закрылков ЛА, показанной на рис. 8 – реализовывать условие «Подъемная сила крыла больше или равна массе ЛА» для всех условий полета ЛА.

Команды управления:
- команда на выпуск, от предыдущей позиции к следующей;
- команда на уборку, от предыдущей позиции к следующей;
- команда на отмену команды на уборку или выпуск и возврат в исходное положение (предыдущую позицию).

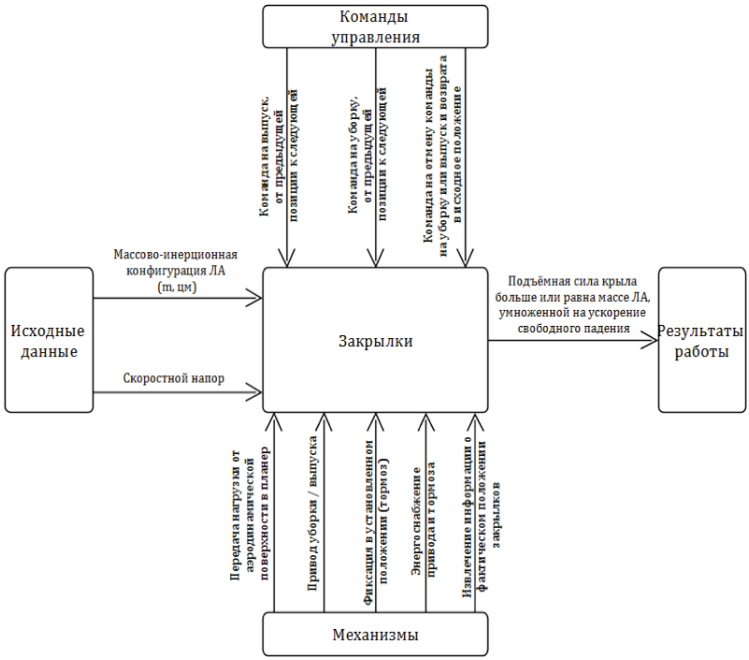

Рис. 8. Функциональная модель закрылков ЛА

Исходные данные для работы:

– массово-инерционная конфигурация ЛА (величина массы, положение центра масс и основных моментов инерции);

– скоростной напор $\frac{\rho * V^2}{2}$, где V – это скорость полета (потока).

Логические части механизмов:

– передачи аэродинамической нагрузки от поверхности в планер (силовая часть);
– привод уборки/выпуска;
– фиксация в установленном положении (тормоз);
– энергоснабжение привода и тормоза;
– извлечение информации о фактическом положении закрылков.

Соединим поведение двух систем – шасси и закрылки в одну модель состояний и переходов, как показано на рис. 9.

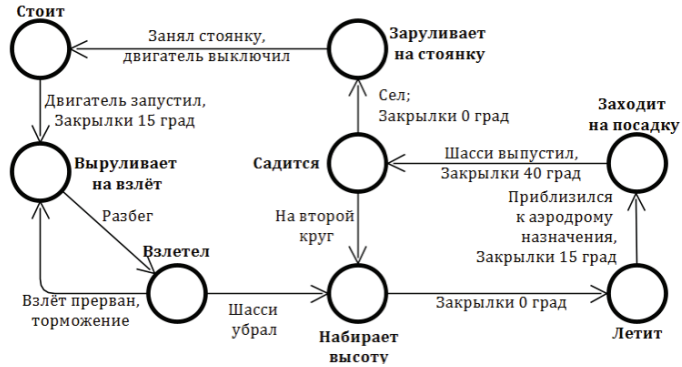

Рис. 9. Модель поведения комплекса систем «шасси» и «закрылки» в терминах состояний и переходов ЛА

Общие исходные данные:
- массово-инерционная конфигурация ЛА (величина массы, положение центра масс и основных моментов инерции);
- режим применения (стоянка, руление, разбег, взлет, набор высоты, крейсерский полет, снижение, заход на посадку, уход на второй круг, посадка, пробег).

Взаимосвязи по управлению:
- переход от взлета к набору высоты – уборка шасси;
- переход от снижения к заходу на посадку – выпуск шасси;
- перед взлетом – закрылки во взлетном положении;
- на стоянке – закрылки в убранном положении, шасси выпущены, и уборка шасси заблокирована.

Общие результаты работы системы:
- система «ЛА» реализует поведение (см. рис. 2);
- граничное условие для силы веса ЛА (массы, помноженной на ускорение свободного падения) (рис. 10).

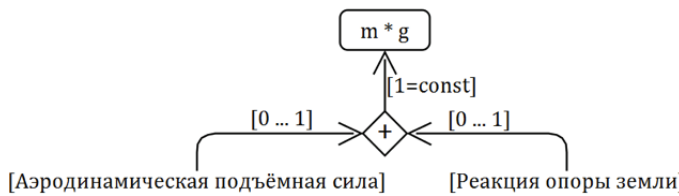

Рис. 10. Определение параметра модели «Вес ЛА» в виде граничного условия

Данное граничное условие выражает тот факт, что сила веса ЛА уравновешивается суммой двух других сил – реакции опоры земли при движении по земле и аэродинамической подъемной силы. Из данного граничного условия следует, что сила веса самолета есть величина постоянная, и она уравновешивается суммой двух сил – аэродинамической подъемной силой, обусловленной обтеканием воздуха, и реакцией опоры земли, обеспеченной со стороны шасси. На разбеге и пробеге обе силы действуют одновременно и однонаправленно, в разных пропорциях, в зависимости от доли скорости относительно взлетной или посадочной, но их сумма всегда равна (m*g).

Самолет может двигаться в воздушной среде, не теряя скорость, при условии, когда величина аэродинамической подъемной силы больше или равна величине силы веса: $Y > m*g$, как показано на рис. 11.

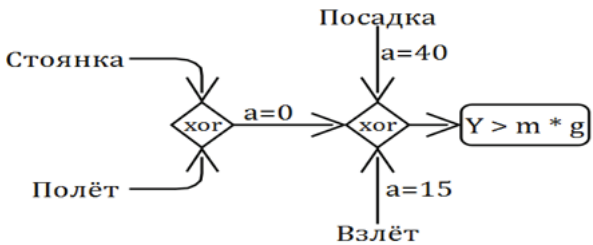

Рис. 11. Графическое представление формулы «вклад –> результат», где результат «подъемная сила должна быть больше веса» образован одним из трех взаимоисключающих «вкладов»

Если скоростного напора недостаточно для выполнения указанного условия, то необходимо увеличение коэффициента аэродинамической подъемной силы крыла. Для этой цели применяется механизация крыла – закрылки. В нашем примере работа закрылков задана правилом соответствия между режимом полета и углов отклонения закрылков «a»:

- полетном или стоянкой при угле отклонения закрылков a = 0 град;
- взлетном при a = 15 град;
- посадочном при a = 40 град.

Оператор исключительного выбора «xor» в данной модели определяет, что вклад в конечный результат $Y > m*g$ дает только один из трех указанных составляющих, что свидетельствует о том,

что они не пересекаются во времени, и, следовательно, их можно считать раздельными фазами полетного цикла ЛА.

Собираем из вышеперечисленных определений схему комплексной системы «Шасси и закрылки» в расширенной нотации IDEF0, как показано на рис. 12.

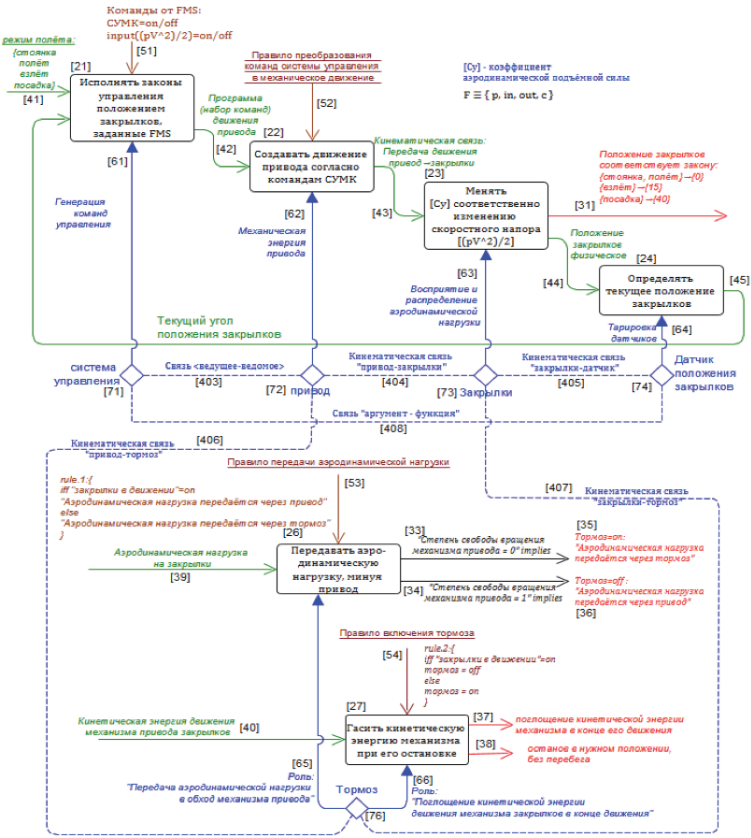

Рис. 12. Система «Шасси и закрылки» в расширенной нотации IDEF0

Таким образом, получена модель системы, строение и возможности которой можно сопоставить друг с другом и проверить на соответствие.

Как видно в представленной схеме, имена механизмов развернуты в ролевые отношения между функциональным и физическим

представлением системы. Эти отношения сформировали «мост», связывающий функциональное определение системы с физическим. Благодаря ему становится понятным, что для каждой функции существует источник – физический объект, играющий роль механизма в ее работе. Физические объекты связаны между собой материальными отношениями, такими как генерация, преобразование или передача движения, нагрузки или сигнала. По такому «мосту» появляется возможность проверить соответствие функций системы физическим процессам во время работы ее составных частей. Кроме того, появляется возможность совмещать несколько различных механизмов в одном агрегате или, наоборот, снабжать одну и ту же функцию различными источниками механизмов.

Выбор физического способа реализации функции может породить новое функциональное требование, потому что удовлетворение одного требования, как правило, приводит к возникновению новых функций и новых связей между функциями. Например, применение электропривода для смены положения закрылков порождает требование электроснабжения и наличие системы управления электроснабжением. Также работа электропривода требует функции охлаждения. Процесс продолжается до тех пор, пока производные требования не перестают возникать. Причем на каждой итерации процесса разработки строение и возможности целевой системы можно сопоставить друг с другом и проверить на соответствие, что исключительно важно для принятия инженерных и конструкторских решений.

Совокупность указанных возможностей дает возможность разрабатывать системы не раздельно по различным дисциплинам, а комплексно.

Заключение

Как было проверено в ходе исследования, исходная нотация IDEF0 обеспечивает возможность связывать выходы предшествующих функций с входами или управлением последующих, в результате чего обеспечена возможность проверять цепочки преобразования данных и, следовательно, проверять соответствие начальных входов с конечными выходами. Однако в подобной модели внутреннего устройства системы отсутствуют отношения между физическими компонентами, и, соответственно, не выводится ее поведение.

С целью сопоставления и взаимосвязей внутренних и внешних свойств модели системы к исходной нотации функционального описания систем IDEF0 добавлен ряд дополнительных описаний.

1. Исходные данные функции разделены на вход в систему извне (ввод внешних условий и воздействий) и данные управления, поступающие от предшествующей функции. Это дало возможность разделить более сложную задачу проектирования и проверки правильности обработки данных в системе на две более простые задачи.

2. Управление функции разделено на целевое управление и регулирование, которые подчиняются разным правилам построения и проверки. Это дает возможность структурировать правила проектирования и применять их только там, где требуется.

3. К аргументу «механизм» нотации IDEF0 добавлена возможность присоединять ссылку на физический объект или его прототип (макет) с тем, чтобы контролировать наличие и соответствие средств исполнения заложенных в системе функций.

4. Ко внешним ссылкам на физические объекты добавлены физические связи, которые могут быть проверены на соответствие функциональным связям.

Вместе указанные меры добавляют возможность связать внутренние и внешние свойства разрабатываемой системы, в том числе их строение и поведение.

Таким образом, в результате расширения нотации IDEF0 сформировались новые, расширенные свойства модели системы, которые способствуют решению задач валидации и верификации в процессах разработки сложных технических систем.

Специализация исходных данных, данных управления и данных результатов работы функции расширили возможность контролировать правильность принимаемых при разработке системы решений, в том числе:

- результат работы каждой функции системы может быть проверен на соответствие внешним исходным данным, командам управления и правилам регулирования (настройке режимов работы системы);
- работа всей системы может быть проверена на связность по исходным данным, начиная от первоначальных, поступающих извне, и заканчивая последними, отправляемыми во внешнюю среду;
- работа всей системы может быть проверена на связность по данным управления и регулирования;
- в системе могут быть выявлены функции, не влияющие на ее поведение по отношению к окружающей среде, взаимно дублирующие функции или функции, конфликтующие с ожидаемым результатом функционирования системы;
- в системе могут быть выявлены циклические функции;

– проект системы в целом может быть проверен на согласование внутреннего устройства, функциональных возможностей и поведения.

Соответственно, совокупность всех дополненных возможностей улучшит качество принятия решений в процессе разработки систем.

Постановка задачи на следующий этап исследований: интегрировать функциональную модель системы с моделью требований и проверить, каким образом описание функции в расширенном IDEF0 обеспечит возможность верифицировать ее относительно требований и ограничений, с одной стороны, и как доказать, что описание функции вытекает из требований – с другой; изучить, каким образом конструктивные решения, заключенные в механизмах, реализуют заданную функциональную логику, с учетом переменного характера их ролей, различия режимов их работы в составе системы и в зависимости от меняющихся внешних условий.

Литература

Автоманов, Попов 2017 – *Автоманов С.А., Попов А.Е.* Автоматизированная среда поддержки процессов проектирования авионики: концепция, программа, возможность применения в проекте // МС-21: IV Международная научно-практическая конференция: Перспективные направления развития бортового оборудования гражданских воздушных судов. М., 2017. С. 21–26.

Brook 2015 – *Brook N.J.* Integration of technical development within complex project environment. Literature review: MSc Safety-Critical Systems Engineering. P. 41. URL: https://www.researchgate.net/publication/312554485_Integration_of_technical_development_within_complex_project_environment_-_Literature_Survey (дата обращения 2 февраля 2023).

Buche, Fortin, Gutierrez 2014 – *Buche P., Fortin J., Gutierrez A.* Default Reasoning COGUI // Lecture Notes in Computer Science 2014. Vol. 8577. P. 118–129.

Chein, Mugnier 2009 – *Chein M., Mugnier M.-L.* Graph-based knowledge representation: Computational Foundations of Conceptual Graphs. Cham: Springer, 2009. P. 219.

Fagin, Halpern, Moses, Vardi 2003 – *Fagin R., Halpern J.Y., Moses Y., Vardi M.* Reasoning about knowledge. New York: MIT Press, 2003. P. 75.

Goknil, Kurtev, Berg 2016 – *Goknil A., Kurtev I., Berg van den K.* A rule-based change impact analysis approach in software architecture for requirements changes. URL: https://arxiv.org/ftp/arxiv/papers/1608/1608.02757.pdf (дата обращения 2 февраля 2023).

Huth, Ryan 2000 – *Huth M., Ryan M.* Logic in computer science modelling and reasoning about systems. Cambridge: Cambridge University Press, 2000. P. 443.

Manenti, Ebrahimiarjestan, Yang, Yu 2019 – *Manenti G., Ebrahimiarjestan M., Yang Lan, Yu Ming*. Functional modelling and IDEF0 to enhance and support process tailoring in systems engineering // 2019 International Symposium on Systems Engineering (ISSE), 1–3 October 2019, Edinburgh, UK. New York: IEEE, 2019. P. 1–8.

Rumbaugh 2003 – *Rumbaugh J*. Object-oriented analysis and design (OOAD) // Encyclopedia of Computer Science. Chichester: John Wiley and Sons Ltd, 2003. P. 1275–1279.

Suranto 2015 – *Suranto B*. Systems engineering: why is it important? // The 4th ICIBA 2015, International Conference on Information Technology and Business Applications. Palembang: Bina Darma University, 2015. P. 20–21.

Walden, Roedler, Forsberg, Hamelin, Shortell 2015 – *Walden D.D., Roedler G.J., Forsberg K.J., Hamelin R.D., Shortell T.M*. Systems engineering handbook: a guide for system life cycle processes and activities. San Diego, CA: International Council on Systems Engineering (INCOSE), 2015.

Wolfgang 2010 – *Wolfgang G*. Concepts semantic relations in information science // Journal of the American Society for Information Science and Technology. 2010. Vol. 61 (10). P. 1951–1969.

Yang, Cormican, Yu 2017 – *Yang L., Cormican K., Yu M*. Towards a methodology for systems engineering ontology development – an ontology for system life cycle processes // IEEE International Systems Engineering Symposium (ISSE), 11 October 2017, Vienna, Austria. New York, NY: IEEE, 2017. P. 1–7.

References

Avtomanov, S.A. and Popov, A.E. (2017), "Automated environment for supporting avionics design processes. Concept, program, possibility of application in the project", *MS-21: IV Mezhdunarodnaya nauchno-prakticheskaya konferentsiya: Perspektivnye napravleniya razvitiya bortovogo oborudovaniya grazhdanskikh vozdushnykh sudov* [MS-21, 4th International Scientific and Practical Conference, Prospective Directions for the Development of Airborne Equipment], Moscow, Russia, pp. 21–26.

Brook, N.J. (2015), "Integration of technical development within complex project environment, Literature review: MSc Safety-Critical Systems Engineering", p. 41, available at: https://www.researchgate.net/publication/312554485_Integration_of_technical_development_within_complex_project_environment_-_Literature_Survey (Acceded 2 February 2023).

Buche, P., Fortin, J. and Gutierrez, A. (2014), "Default Reasoning COGUI", *Lecture Notes in Computer Science*, vol. 8577, pp. 118–129.

Chein, M. and Mugnier, M.-L. (2009), Graph-based knowledge representation: Computational Foundations of Conceptual Graphs, Springer, Cham, Switzerland, 219 p.

Fagin, R., Halpern, J.Y., Moses, Y. and Vardi, M. (2003), Reasoning about knowledge, MIT Press, New York, USA.

Goknil, A., Kurtev, I. and Berg, van den, K. (2016), "A rule-based change impact analysis approach in software architecture for requirements changes", p. 44, available at: https://arxiv.org/ftp/arxiv/papers/1608/1608.02757.pdf (Acceded 2 February 2023).

Huth, M. and Ryan, M. (2000), Logic in computer science modelling and reasoning about systems, Cambridge University Press, Cambridge, USA, 443 p.

Manenti, G., Ebrahimiarjestan, M., Lan, Y. and Ming, Y. (2019), "Functional modelling and IDEF0 to enhance and support process tailoring in systems engineering", *2019 International Symposium on Systems Engineering (ISSE), 1–3 October 2019, Edinburgh, UK*, IEEE, New York, USA, pp. 1–8.

Rumbaugh, J. (2003), "Object-oriented analysis and design (OOAD)", *Encyclopedia of Computer Science*, John Wiley and Sons Ltd, Chichester, UK, pp. 1275–1279.

Suranto, B. (2015), "Systems Engineering: why is it important?", *The 4th ICIBA 2015, International Conference on Information Technology and Business Applications*, Bina Darma University, Palembang, Indonesia, pp. 20–21.

Walden, D.D., Roedler, G.J., Forsberg, K.J., Hamelin, R.D. and Shortell, T.M. (2015), Systems engineering handbook: a guide for system life cycle processes and activities, International Council on Systems Engineering (INCOSE), San Diego, CA, USA.

Wolfgang, G. (2010), "Concepts semantic relations in information science", *Journal of the American Society for Information Science and Technology*, vol. 61 (10), pp. 1951–1969.

Yang, L., Cormican, K. and Yu, M. (2017), "Towards a methodology for systems engineering ontology development – an ontology for system life cycle processes", *IEEE International Systems Engineering Symposium (ISSE), 11 October 2017, Vienna, Austria*, IEEE, New York, NY, USA, pp. 1–7.

Информация об авторах

Владимир А. Бочаров, аспирант, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; bocharovva@student.bmstu.ru

Тамара М. Волосатова, кандидат технических наук, доцент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; tamaravol@gmail.com

Information about the authors

Vladimir A. Bocharov, postgraduate student, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; bocharovva@student.bmstu.ru

Tamara M. Volosatova, Cand. of Sci. (Engineering), associate professor, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; tamaravol@gmail.com

УДК 004.6
DOI: 10.28995/2686-679X-2023-2-30-45

Сохранение ресурса вычислительного узла брокера туманного слоя в приложениях обработки данных

Анна Б. Клименко
Российский государственный гуманитарный университет, Москва, Россия, anna_klimenko@mail.ru

Ольга В. Клименко
Лицей № 28, Таганрог, Россия, anna_klimenko@mail.ru

Аннотация. В соответствии с концепцией туманных вычислений при обработке больших объемов данных вычислительная нагрузка сдвигается от «облака» к краю сети, на узлы туманного слоя. При этом, однако, весьма малое количество опубликованных работ посвящено вопросам снижения остаточного ресурса периферийных устройств, которые, как правило, не столь производительны, как устройства в датацентрах. Вероятность безотказной работы устройства также связана с такой характеристикой, как средний остаточный ресурс – величиной, обратной интенсивности отказов, и в целом тенденция убывания этой величины характеризует сохранность вычислительного ресурса устройства и то время, на протяжении которого его эксплуатация будет целесообразна за счет допустимой интенсивности отказов.

Современные реализации концепции туманных вычислений предполагают наличие так называемого брокера туманного слоя (cloud-fog broker), на который возложены функции планирования вычислений, которые могут быть выполнены близлежащими узлами туманного слоя, либо задача отправляется в облако. Очевидно, что при этом брокер туманного слоя функционирует с повышенной нагрузкой и вполне целесообразно ставить вопрос о сбережении ресурса этого узла.

Данная статья посвящена исследованию вопроса сравнения «эгоистичной» стратегии распределения вычислительной нагрузки по узлам туманного слоя сети и подхода, основанного на выборе узла для вычислений на основе моделирования среднего остаточного ресурса. Предложенный алгоритм делает возможным, в зависимости от предпочтений в сохранности ресурса узла, реализовать выбор устройства.

Проведенное моделирование демонстрирует целесообразность включения брокера туманного слоя в подмножество рассматриваемых канди-

датов для распределения нагрузки даже в том случае, когда в соответствии с «эгоистичным» подходом брокеру выгоднее передать вычисления в следующий узел. Также последнее актуально для случая, когда приоритетно снижение расходования ресурса для группы устройств, включая брокер.

Ключевые слова: туманные вычисления, распределение нагрузки, средний остаточный ресурс, вероятность безотказной работы

Для цитирования: Клименко А.Б., Клименко О.В. Сохранение ресурса вычислительного узла брокера туманного слоя в приложениях обработки данных // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 2. С. 30–45. DOI: 10.28995/2686-679X-2023-2-30-45

Conservation of fog layer broker compute node resource in data processing applications

Anna B. Klimenko
Russian State University for the Humanities, Moscow, Russia, anna_klimenko@mail.ru

Ol'ga V. Klimenko
Lyceum № 28, Taganrog, Russia, anna_klimenko@mail.ru

Abstract. In accordance with the concept of fog computing, when processing large amounts of data, the computing workload shifts from the "cloud" to the edge of the network, to the nodes of the fog layer. At the same time, however, a very small number of published works deal with the issues of reducing with that the residual resource of peripheral devices, which, as a rule, are not of a high computational power comparing with devices in data centers. The reliability indicator, the probability of failure-free operation are also associated with such a characteristic as the average residual resource – the value of the reciprocal of the failure rate, and in general, the decreasing trend of the value characterizes the safety of the computing resource of the device and the time during which its operation will be expedient due to the allowable failure rate.

Modern implementations of the concept of fog computing suggest the presence of a so-called cloud-fog broker, which is entrusted with the functions of computing scheduling that can be performed by nearby fog layer nodes. Obviously, in this case, the cloud-fog broker operates with an increased load, and it is quite reasonable to raise the question of saving the resource of the node.

The article is concerned with the study of comparing the "selfish" strategy of distributing the computational load over the nodes of the foggy layer in the network and the approach based on the choice of a node for computing based

on the simulation of the average residual resource. The proposed algorithm makes it possible, depending on the preferences in the safety of the resource of the node, to implement the choice of device.

The simulation performed demonstrates the expediency of including the fog layer broker in the subset of considered candidates for load distribution even in the case when, in accordance with the "selfish" approach, it is more profitable for the broker to transfer calculations to the next node. The latter is also relevant for the case when it is a priority to reduce resource consumption for a group of devices, including a broker.

Keywords: fog computing, load distribution, average residual life, probability of failure-free operation

For citation: Klimenko, A.B. and Klimenko, O.V. (2023), "Conservation of fog layer broker compute node resource in data processing applications", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 30–45, DOI: 10.28995/2686-679X-2023-2-30-45

Введение

В настоящее время одним из интенсивно развивающихся направлений в области организации распределенной обработки данных является реализация приложений на основе концепции туманных вычислений.

К настоящему времени сложился достаточно широкий круг приложений, где используются «туманные» вычисления, например: системы умных светофоров [Довгаль, Довгаль 2018], дополненной реальности [Смирнов, Голохваст, Тумялис 2019], системы «умный город», системы видеонаблюдения и другие.

Если рассмотреть исследования, проводимые в данной области (области «туманных» вычислений), то следует отметить следующие основные направления [Mouradian 2017]:

– распределение ресурсов между «туманом» и «облаком»,
– обеспечение безопасности при реализации туманных вычислений,
– обеспечение взаимодействия между пользовательскими устройствами, «туманом» и облаком.

Однако только немногие работы ориентированы на решение такой проблемы, как сбережение вычислительного ресурса.

Проблема эта возникает в связи с тем, что в рамках концепции «туманных» вычислений вычислительная нагрузка переносится с вычислительных устройств, расположенных в датацентрах, на вычислительные устройства, составляющие сетевую инфраструк-

туру и обладающие значительно меньшей вычислительной мощностью.

В ряде работ российских ученых было продемонстрировано, что работа вычислительного устройства в условиях повышенной нагрузки сокращает срок целесообразной эксплуатации устройства. Последнее связано с уменьшением такой величины, как вероятность безотказной работы устройства и гамма-процентной наработки на отказ [Каляев, Мельник 2011].

В результате, перенося вычислительную нагрузку на более слабые устройства, их срок службы – как части сетевой инфраструктуры – сокращается, что нежелательно.

В процессе данного исследования был проведен анализ работ, связанных с описываемой проблематикой: в работах [Клименко 2022; Klimenko 2022] представлено аналитическое выражение, позволяющее оценить целесообразность переноса нагрузки на устройство в сравнении с работой этого же устройства в режиме передачи данных дальше, в облачный слой, и представлен метод распределения нагрузки среди устройств с акцентом на ресурсосбережение.

В рамках данного исследования внимание будет акцентировано на работе такого устройства, как брокер туманного слоя (cloud-fog broker). Основной задачей этого устройства является принятие решения по планированию вычислений в туманном слое либо отправка данных дальше, в «облако» [Klimenko 2022].

Поскольку брокер туманного слоя, по сути, реализует распределение вычислительной нагрузки, и сам при этом постоянно решает собственные функциональные задачи, продление сроков его целесообразной эксплуатации актуально.

1. Оценивание ресурса вычислительного устройства

В данной работе ресурсом вычислительного устройства является средний остаточный ресурс:

$$R = \frac{1}{\lambda}, \tag{1}$$

где – интенсивность отказов вычислительного узла.

В работах [Каляев, Мельник 2011] представлено теоретическое обоснование, позволяющее связать загруженность вычислительного устройства и величину интенсивности отказов, а именно:

$$\lambda = \lambda_0 \cdot 2^{\frac{kD}{10}}, \tag{2}$$

где k – коэффициент, связывающий загруженность вычислителя с его температурой, D – загруженность устройства в процентах.

$$D = \frac{W_0}{p_0 \cdot t_{constra\,int}}, \quad (3)$$

где W_0 – трудоемкость решаемой задачи устройством, p_0 – производительность устройства, $t_{\text{constraint}}$ – ограничение на время решения задачи.

Модель функционирования брокера туманного слоя выглядит следующим образом (рис. 1):

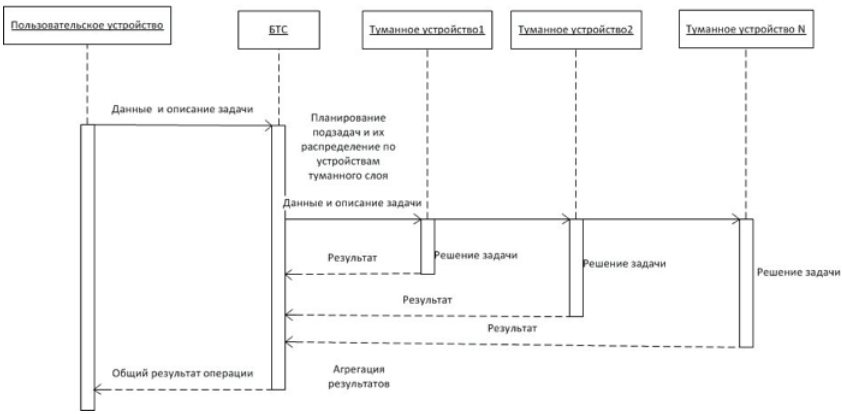

Рис. 1. Функционирование брокера туманного слоя

В [Klimenko 2022] представлен метод выбора вычислительного узла для размещения нагрузки в туманном слое.

1. В качестве первого варианта решения выбирается сам узел-брокер. Для него производится оценка трудоемкости уже решаемых задач, при которой целесообразно решать поступившую, в соответствии с выражением

$$w_{receive} + w_{process} + w_{send} < 2w_{receive} / x.$$

2. Брокер осуществляет просмотр локального списка состояний узлов S, выбирая ближайшие к нему, расположенные не более чем на расстоянии одного транзитного участка сети, и составляет список Si. Здесь мы делаем допущение, что если ни один узел не подойдет, то он автоматически становится транзитным.

3. Для каждого Si выполняется проверка: $x < 1$ с учетом добавляемого времени на транзитную передачу данных.

3.1. Проверить выполнение неравенства:

$$w_{receive} + w_{process} + w_{send} < 2w_{receive} / x.$$

То есть перенос обработки данных на туманный узел целесообразен только в том случае, если суммарная трудоемкость задач получения данных, обработки и отправки результата не будет превышать удвоенное значение отношения трудоемкости получения данных к доле времени от пользовательской операции, выделяемой для этого.

3.2. Поместить Si в список узлов-кандидатов.

3.3. Из сформированного списка выбрать тот узел, для которого значение x будет минимальным (это означает, что время, приходящееся на транзит данных и прием-передачу, будет минимальным, и, следовательно, основная нагрузка будет иметь «полезный» характер).

4. Если ни одного узла Si не обнаружено, брокер выбирает из локального списка состояний узлы, расположенные на расстоянии двух транзитных участков сети.

5. Если ни один из узлов Si не удовлетворяет условию $w_{receive} + w_{process} + w_{send} < 2w_{receive} / x$, то тогда из списка узлов на расстоянии одного транзитного участка сети, включая сам брокер, выбирается узел с максимальной производительностью, для которого будет выполняться x.

Особенностями этого метода является следующее.

1. Делается допущение о том, что каждый узел имеет подготовленные данные о состоянии соседних узлов, что реализуется посредством использования технологий распределенного реестра.

2. Метод можно отнести к «эгоистичным», то есть каждый узел в результате вычисления предложенной аналитической оценки выбирает такую стратегию поведения, чтобы уменьшить собственные расходы ресурса.

Эти особенности приводят к недостаткам метода, а именно:

– в случае невозможности реализовать осведомленность узла о состоянии ресурсов сети необходимо, чтобы брокер туманного слоя опросил сперва все соседние узлы, а после этого – если ни один из соседних узлов в соответствии с «эгоистичной» стратегией не взял на себя решение задачи – продолжить опрос узлов более удаленных, либо другие узлы должны опрашивать соседей. Это приводит к дополнительным затратам времени, что критично в случае необходимости

обеспечения работ приложений в реальном времени (дополненная реальность, например);

– применение «эгоистичной стратегии», как и применение «жадных» методов, может привести к тому, что результатом решения задачи будет далеко не самое лучшее решение. В частности, «эгоистичная» стратегия приводит к тому, что для группы узлов принятое решение по распределению не будет удовлетворительным.

Поэтому в рамках данной статьи проведем сравнение «эгоистичного» подхода и подхода, основанного на оценивании остаточного ресурса для соседних с брокером узлов и выбора узла с наименьшими потерями ресурса при решении вычислительной задачи.

2. Распределение нагрузки на основе результатов моделирования

Входными параметрами алгоритма являются следующие.

1. Производительности брокера туманного слоя p_0 и соседних узлов p_i, i = 1..n.

2. Трудоемкость решения вычислительной задачи w и трудоемкость приема-передачи данных в сеть w_{send} и $w_{receive}$ в зависимости от объема данных V_{send} и $V_{receive}$.

3. Исходные значения загруженности брокера туманного слоя и соседних узлов L_0 и L_i, i = 1..n.

Рассмотрим основные этапы распределения нагрузки.

1. Брокер туманного слоя получает данные для обработки объемом $V_{receive}$. Трудоемкость задачи приема данных соответственно $w_{receive}$ ($V_{receive}$) = $\beta(V_{receive})$, обработки данных – w, W_{send} (V_{send}) = $\beta(V_{send})$. Таким образом, для получения, обработки данных и отправки результатов пользователю брокер туманного слоя будет решать задачу общей трудоемкостью:

$$W_0 = w + \beta(V_{receive} + V_{send}). \quad (5)$$

В случае если брокер туманного слоя только передает данные, трудоемкость решаемой им задачи будет следующей:

$$W_0 = w + \beta(2V_{receive} + 2V_{send}). \quad (6)$$

2. Производится моделирование значений остаточного вычислительного ресурса на основе следующих выражений (1–4), при этом переменная $t_{constraint}$ в случае обработки данных брокером туманного слоя будет равна времени, отводимому на выполнение операции. В случае, когда брокер только передает данные дальше, время, отводимое на передачу данных, будем считать следующим образом:

$$t' = \frac{W_0}{p_0}. \quad (7)$$

3. Производится моделирование значений остаточного ресурса для соседних узлов (при условии, что брокер туманного слоя передает этим узлам задачу на выполнение, а также пересылает данные).

$$W_i = w + \beta(V_{receive} + V_{send}), \quad (8)$$

при этом время, отводимое на прием данных узлов, обработку данных и отправку обратно брокеру туманного слоя, будет соответственно равно:

$$t'' = t_{const} - t', \quad (9)$$

то есть все оставшееся время, отведенное на выполнение пользовательской операции за вычетом времени, которое понадобится брокеру туманного слоя для передачи данных. Следует отметить, что временем ожидания сообщений в очереди при приеме-передаче данных мы пренебрегаем.

4. Производится ранжирование значений остаточного ресурса для всех R_i, включая R_0 по убыванию.

5. Выполнение задачи назначается на устройство, для которого при моделировании было получено максимальное значение R.

3. Моделирование

1. Рассмотрим и сравним две ситуации: когда брокер реализует обработку данных сам, а узлы бездействуют, и когда брокер передает обработку данных на один из имеющихся узлов-соседей.

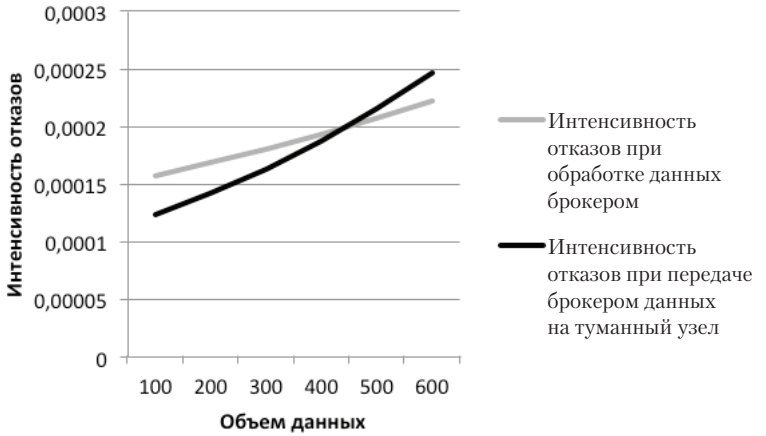

Рис. 2. Моделирование значений интенсивности отказов узла-брокера

Видно, что при увеличении объемов данных, которые брокер туманного слоя должен передавать соседнему узлу на обработку, наблюдается картина, когда это становится невыгодно делать, интенсивность отказов растет быстрее, чем в случае «обработки на месте».

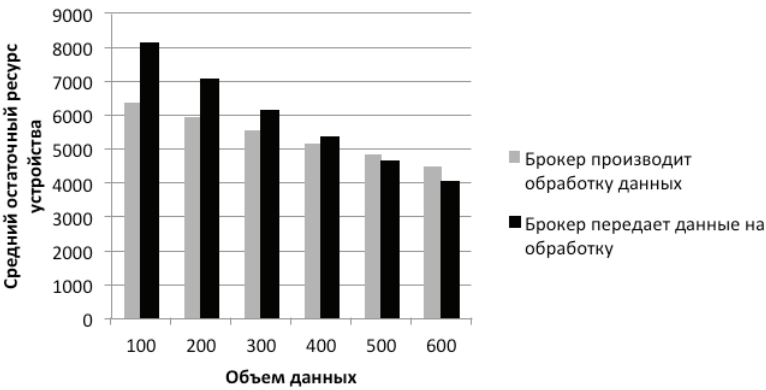

Рис. 3. Моделирование значений среднего остаточного ресурса брокера туманного слоя

Соответственно, изменяется и средний остаточный ресурс устройства: при увеличении объемов передаваемых по сети данных брокеру становится выгоднее производить обработку на месте.

Далее рассмотрим значения интенсивности отказов и среднего остаточного ресурса комплексно для группы устройств, включая брокер туманного слоя, рассматривая ту область данных, где брокеру выгоднее производить передачу данных на устройство туманного слоя.

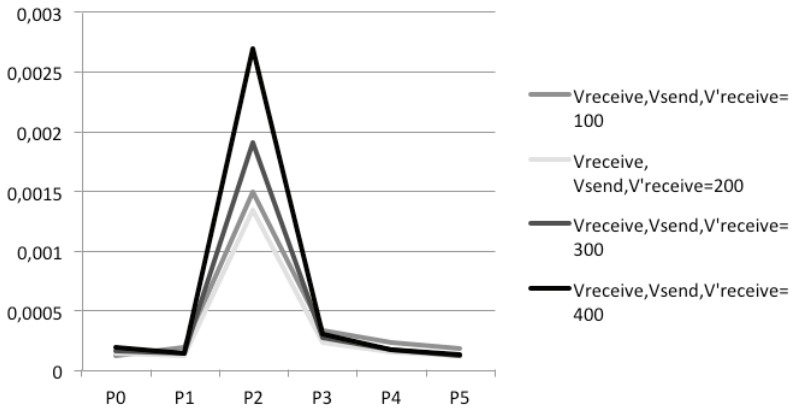

Рис. 4. Моделирование интенсивности отказов для группы узлов

Когда передаваемые объемы данных позволяют осуществлять обработку данных на соседних узлах, возникают ситуации, когда действительно узел туманного слоя, соседний с брокером, выполнит задачу с меньшим ухудшением показателя интенсивности отказов и, следовательно, задачу выгоднее выполнить на этом узле, что подтверждает целесообразность ранжирования значений среднего остаточного ресурса и выбора наилучшего значения в алгоритме.

Однако при этом не исключаются ситуации, когда брокеру туманного слоя выгодно передавать данные в сеть, но при этом он также может оказаться вычислительным узлом, который выполнит задачу наиболее эффективно в плане снижения значения остаточного ресурса и наоборот, когда брокеру выгоднее выполнить задачу самостоятельно, одним из соседних узлов может оказаться узел, который выполнит задачу более эффективно, даже с учетом затрат времени на передачу данных.

Примеры показаны на рис. 5 и 6.

Пусть Vreceive = 300, Vsend = 300, V'receive = 50, P0(брокер) = 500 м. е., P1 = 1000, P2 = 100, P3 = 300, P4 = 600, P5 = 1500.

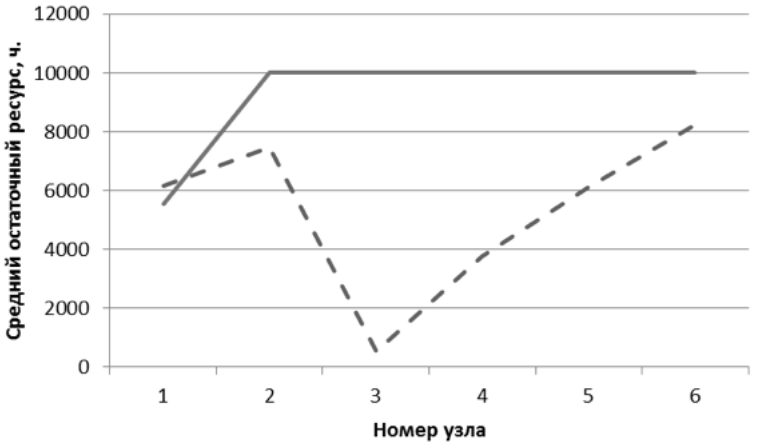

Рис. 5. Моделирование значений среднего остаточного ресурса при распределении по узлам: сплошная линия иллюстрирует ситуацию, когда обработку данных выполняет брокер, все остальные узлы не принимают участия в вычислениях

Здесь сплошной линией показаны значения среднего остаточного ресурса (в ч.) по узлам 1–6 для ситуации, когда брокер самостоятельно обрабатывает данные, а узлы туманного слоя не принимают участия в вычислениях, соответственно – ситуация, когда брокер передает данные в сеть любому из узлов. При этом при очевидной «выгоде» передачи данных на обработку соседу имеется узел (№ 5) высокой производительности, который более эффективно обработает данные.

Благодаря этому средний остаточный ресурс брокера увеличивается на 10% по сравнению, если бы брокер решал задачу сам, а средний остаточный ресурс выбранного для решения узла уменьшился на 20% относительно отсутствия нагрузки. Если оценивать ВБР для группы устройств, очевидно, что такая оценка будет хуже, чем если оценивать «невыгодную» обработку данных для одного узла-брокера.

В случае, если брокер «оставит» задачу на выполнение себе, то он потеряет 10% остаточного ресурса, а другие узлы не потеряют

ничего. Такая ситуация является маркерной для выбора целей оптимизации, а именно: что будет более приоритетным – сохранение показателей остаточного ресурса для группы либо только для брокера?

Следует отметить, что для ситуации Vreceive = 300, Vsend = 300, V'receive = 50, P0(брокер) = 1200 м. е., P1 = 1000, P2 = 100, P3 = 300, P4 = 600, P5 = 1300 ситуация меняется следующим образом, как показано на рис. 6:

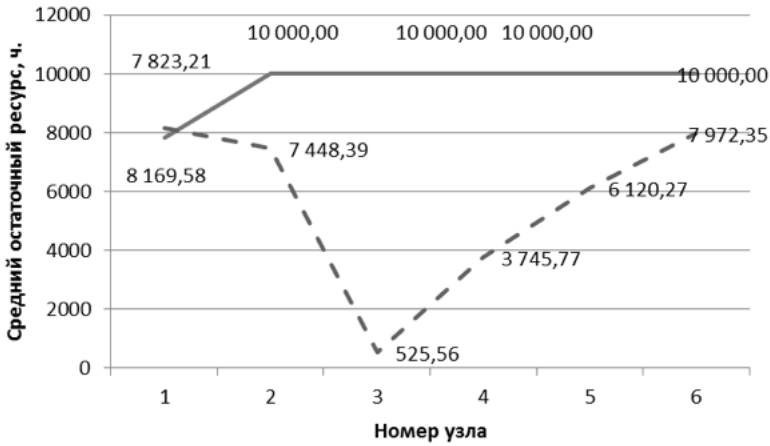

Рис. 6. Моделирование значений среднего остаточного ресурса при распределении по узлам: график, отображенный сплошной линией, иллюстрирует ситуацию, когда обработку данных выполняет брокер, все остальные узлы не принимают участия в вычислениях. Эффективность брокера выше, чем у узла № 6

1. Брокеру туманного слоя выгоднее отправлять данные для обработки соседнему туманному узлу.

2. Однако, ранжируя модельные оценки для туманных узлов, включая брокер, мы получаем ситуацию, когда при передаче данных соседним узлам по-прежнему брокер выполнит задачу более эффективно, чем прочие узлы: средний остаточный ресурс для брокера, решающего задачу, превышает средний остаточный ресурс узла P5. При этом остаточный ресурс брокера ухудшится на 5%, в то время как, перекладывая выполнение задачи на узел P5, мы получим ухудшение до 20% остаточного ресурса узла № 5 и в совокупности, оценивая остаточный ресурс группы устройств, получим общее ухудшение.

Исходя из этого, сформулируем важное правило для корректировки алгоритма функционирования брокера туманного слоя: способ распределения нагрузки прежде всего будет зависеть от целей управления. Иными словами, должен быть выбран приоритет: либо одиночный узел, например брокер туманного слоя, либо группа устройств, включая брокер.

Модернизируем алгоритм следующим образом.

1. Для имеющихся исходных данных оценить целесообразность передачи брокером туманного слоя данных в сеть либо обработки на месте.

2. Если моделированием подтверждается целесообразность передачи в сеть, то:

2.1. Произвести оценку остаточного ресурса для рассматриваемых узлов.

2.2. Если наивысший приоритет сохранения ресурса только у брокера туманного слоя, то произвести ранжирование полученных значений, не включая в сравнение значение, полученное для брокера с условием обработки им данных.

2.3. Если приоритетно сохранение вычислительного ресурса у группы узлов, то произвести ранжирование полученных значений, не включая в сравнение значение, полученное для брокера с условием обработки им данных.

2.4. Выбрать узел, для которого ухудшение значения среднего остаточного ресурса будет минимальным среди всего множества узлов.

То есть в зависимости от выбранного приоритета сохранения вычислительного ресурса, мы можем либо не включать в результирующее множество узлов брокер туманного слоя (если для него целесообразно отправить данные на обработку дальше), либо, наоборот, если выбирается стратегия, сохраняющая вычислительный ресурс для группы устройств, мы принимаем в рассмотрение в том числе и брокер туманного слоя, потому что в таком случае для группы может быть достигнута значительная выгода.

Эффективность алгоритмов

Поскольку край сети – это, как правило, динамичная вычислительная среда, а увеличение времени на планирование ведет, соответственно, к сокращению времени на обработку данных (что особенно важно для систем реального времени), алгоритмы могут быть оценены также с точки зрения временных затрат.

В случае, когда вычислительная среда распределена географически, мы не можем пренебречь временем, которое уходит на опросы узлов, например, в случае составления списка узлов, располагающих необходимыми вычислительными ресурсами. Также временная оценка работы алгоритма важна и для сетей спутниковой связи, особенно при наличии регенерации сигнала, когда группы низкоорбитальных спутников уже могут выполнять распределенную обработку данных, но при этом распределение должно происходить как можно быстрее.

Таким образом, помимо оценивания подходов к распределению нагрузки с точки зрения продления срока службы устройств, также целесообразно оценить подходы и с точки зрения времени, которое может быть затрачено при реализации того или иного алгоритма. В табл. 1 приведено рассмотрение худшего случая: когда необходимо опросить все имеющиеся поблизости от брокера узлы, прежде чем обнаружится узел, располагающий необходимыми ресурсами.

Таблица 1

	Выбор брокера	Поиск среди соседних узлов	Поиск среди узлов на расстоянии двух транзитных участков сети
«Эгоистичный» алгоритм	C	C+2NT	C+2NT+4NT
Алгоритм на основе моделирования	C	C+2NT	–

Следует отметить, что рассмотрение исключительно соседних узлов может приводить к потере лучших решений, при этом происходит выигрыш во времени. В случае, когда среди соседних узлов не обнаружено ни одного узла, обладающего свободными ресурсами в наличии, задача может быть выполнена непосредственно брокером туманного слоя либо передана на выполнение в облако в соответствии с концепцией туманных вычислений.

Заключение

В статье проведено сравнение двух подходов к распределению нагрузки в туманном слое сети с акцентом на увеличение среднего вычислительного ресурса брокера туманного слоя. В ходе проведенного исследования и моделирования мы выяснили, что «эгоистичный» подход полезен в частных случаях, особенно тогда, когда

есть приоритет в сохранении вычислительного ресурса узлов, но в целом «эгоистичный» подход может иметь отрицательное влияние на вероятность безотказной работы группы узлов. Предложенный алгоритм распределения нагрузки учитывает возможность приоритета в сохранении ресурса брокера туманного слоя путем включения его в множество, из которого производится выбор узла для распределения нагрузки.

Литература

Довгаль, Довгаль 2018 – *Довгаль В., Довгаль Д.* Роль туманных вычислений в Интернете Вещей // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2018. № 4 (231). URL: https://cyberleninka.ru/article/n/rol-tumannyh-vychisleniy-v-internete-veschey (дата обращения 13 февраля 2023).

Каляев, Мельник 2011 – *Каляев И.А., Мельник Э.В.* Децентрализованные системы компьютерного управления: монография. Ростов н/Д.: ЮНЦ РАН, 2011. 196 с.

Клименко 2022 – *Клименко А.* Метод ресурсосберегающего планирования распределенных вычислений в туманной вычислительной среде // Моделирование, оптимизация и информационные технологии. 2022. № 10 (3). С. 27–28.

Смирнов, Голохваст, Тумялис 2019 – *Смирнов А., Голохваст К., Тумялис А.* Развитие «Интернета вещей», дополненной реальности и коммуникационных технологий. https://arxiv.org/ftp/arxiv/papers/1902/1902.08008.pdf (дата обращения 13 февраля 2023).

Klimenko 2022 – *Klimenko A.* Model and method of resource-saving tasks distribution for the fog robotics // Lecture Notes in Computer Science. 2022. Vol. 13719. P. 210–222.

Mouradian 2017 – *Mouradian C., Naboulsi D., Yangui S., Glitho E., et al.* A comprehensive survey on fog computing: state-of-the-art and research challenges // IEEE Communications Surveys & Tutorials. Vol. 20, no. 1. P. 416–464.

References

Dovgal', V. and Dovgal', D. (2018), "Role of fog computing in the Internet of Things", *Vestnik Adygeiskogo gosudarstvennogo universiteta, Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki*, vol. 4 (231), available at: https://cyberleninka.ru/article/n/rol-tumannyh-vychisleniy-v-internete-veschey (Acceded 13 February 2023).

Kalyaev, I.A. and Mel'nik, E.V. (2011), *Detsentralizovannye sistemy komp'yuternogo upravleniya: monografiya* [Decentralized computer control systems. Monograph], YuNC RAN, Rostov-on Don, Russia, 196 p.

Klimenko A. (2022), "A method for resource-efficient scheduling of distributed computing in the fog computing environment", *Modelirovanie, optimizacija i informacionnye tehnologii*, vol. 10 (3), pp. 27–28.

Klimenko, A. (2022), "Model and method of resource-saving tasks distribution for the fog robotics", *Lecture Notes in Computer Science,* vol. 13719, pp. 210–222.

Mouradian, C., Naboulsi, D., Yangui, S. and Glitho, E. et al. (2018), "A comprehensive survey on fog computing: state-of-the-art and research challenges", *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 416–464.

Smirnov, A., Golokhvast, K. and Tumyalis, A. (2019), "Development of the Internet of Things, augmented reality and communication technologies", available at: https://arxiv.org/ftp/arxiv/papers/1902/1902.08008.pdf (Acceded 13 February 2023).

Информация об авторах

Анна Б. Клименко, кандидат технических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; anna_klimenko@mail.ru

Ольга В. Клименко, учащаяся, лицей № 28, Таганрог, Россия; 347923, Россия, Таганрог, пер. Трудовых Резервов, д. 1; anna_klimenko@mail.ru

Information about the authors

Anna B. Klimenko, Cand. of Sci. (Engineering), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; anna_klimenko@mail.ru

Ol'ga V. Klimenko, pupil, Lyceum № 28, Taganrog, Russia; bld. 1, Trudovykh Rezervov lane, Taganrog, Russia, 347923; anna_klimenko@mail.ru

УДК 004.056+336.22
DOI: 10.28995/2686-679X-2023-2-46-69

Моделирование процесса оценки угроз безопасности информационных систем налоговых органов

Юлия Ю. Косенкова
Финансовый университет при Правительстве РФ, Москва, Россия, academy@fa.ru

Сергей В. Романовский
Московский государственный лингвистический университет, Москва, Россия, info@linguanet.ru

Елена П. Цацкина
Московский государственный лингвистический университет, Москва, Россия, info@linguanet.ru

Аннотация. Современный этап развития российского общества характеризуется реализацией мер, направленных на развитие цифровых технологий и внедрение их в различные сферы экономики. Примером инновационного цифрового прорыва в России является Федеральная налоговая служба, аккумулирующая значительные объемы конфиденциальной информации, ведущая большое число реестров и реализующая большое количество сервисов, в том числе не связанных с налогообложением. Реализация угроз информационной безопасности в отношении информационных коммуникационных технологий Федеральной налоговой службы может привести к ряду негативных последствий. Целью исследования является построение модели, позволяющей оценить вероятность реализации рассматриваемых угроз и степень их негативного воздействия на систему цифрового взаимодействия налоговых органов с налогоплательщиками и безопасность сформированных налоговыми органами баз данных. В статье приведены универсальные методы научного познания и математические методы, использованные при построении модели оценки рисков. В результате экспертной оценки предложена модель, позволяющая оценить риски информационной безопасности, которым подвергаются информационные коммуникационные технологии ФНС России. Предложенная модель может использоваться как на различных уровнях налогового администрирования, так и в иных сферах государственного и муниципального управления.

Ключевые слова: большие данные, цифровая экономика, угроза, информационная безопасность, модель оценки рисков

Для цитирования: Косенкова Ю.Ю., Романовский С.В., Цацкина Е.П. Моделирование процесса оценки угроз безопасности информационных систем налоговых органов // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 2. С. 46–69. DOI: 10.28995/2686-679X-2023-2-46-69

Information security threats assessment process modeling for tax authorities' information systems

Yulia Yu. Kosenkova
Financial University under the Government of the Russian Federation, Moscow, Russia, academy@fa.ru

Sergei V. Romanovskii
Moscow State Linguistic University, Moscow, Russia, info@linguanet.ru

Elena P. Tsatskina
Moscow State Linguistic University, Moscow, Russia, info@linguanet.ru

Abstract. The current stage of Russian society development is characterized by the implementation of measures aimed at the development of digital technologies and their introduction into various spheres of the economy. An example of an innovative digital breakthrough in Russia is the Federal Tax Service, which accumulates significant amounts of confidential information, maintains a large number of registries, and implements a large number of services, including those not related to taxation. The realization of threats to information security in relation to information and communication technologies of the Federal Tax Service can lead to negative consequences. The purpose of the study is to build a model that allows assessing the probability of occurrence of the threats in question and their impact on digital interaction system between tax authorities and taxpayers, and the security of databases formed by tax authorities. The study applies universal methods of scientific cognition and mathematical methods for the construction of a risk assessment model. As a result, a model is proposed that allows assessment of information security risks, which information and communication technologies of the Federal Tax Service of Russia are exposed to. The proposed model can be used both at various levels of tax administration and in other spheres of state and municipal administration.

Keywords: big data, digital economy, threat, information security, risk assessment model

For citation: Kosenkova Yu.Yu., Romanovskii, S.V. and Tsatskina, E.P. (2023), "Information security threats assessment process modeling for tax authorities' information systems", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 46–69, DOI: 10.28995/2686-679X-2023-2-46-69

Введение

Провозглашенный Клаусом Швабом переход к IV промышленной революции имеет в своей основе цифровизацию всех основных сфер экономики и управления: применение искусственного интеллекта, функционирование «интернета вещей», широкомасштабное использование цифровых технологий в промышленности, финансах, сфере услуг, государственном управлении и т. д. Определений термина «цифровая экономика» в научной литературе встречается достаточно много. Обобщая их, приходим к выводу, что под ней понимается экономика, основанная на новой технологической основе (с применением цифровых технологий на базе ИТ-инфраструктуры и систем связи), способная коренным образом изменить науку, бизнес, социальную сферу и, что немаловажно, государственное управление (так называемое цифровое правительство). Российская Федерация, наряду с иными развитыми экономиками, находится в рамках подготовки к процессу перехода к Индустрии 4.0.

В настоящее время большинство программ и операционных систем, используемых во всем мире, разработаны американскими корпорациями IBM, Oracle и Microsoft. Число пользователей Интернета достигает ⅔ от общей численности населения России, которые являются «заложниками» программ и операционных систем этих транснациональных корпораций. Использование продуктов данных корпораций потенциально обеспечивает техническую возможность сбора данных о пользователях, которые могут применяться в целях коммерческой разведки, воздействия на политические процессы в иных государствах, что является прямой угрозой национальной безопасности, технологической независимости и будущему России. Усиление политических и экономических санкций в отношении России диктует необходимость построения фундамента цифровой экономики на основе импортозамещения в сфере информационных технологий, аппаратного обеспечения и компьютерных сетей.

Цифровизация любой сферы экономики и управления включает в себя внедрение информационных систем, баз данных, сетевого и серверного оборудования. Поправки 2015 г. к Федеральному закону «О персональных данных» от 27.07.2006 № 152-ФЗ[1], Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21.07.2014 № 242-ФЗ регламентируют хранение информации о российских пользователях на территории Российской Федерации. Российский рынок серверного оборудования в настоящее время не богат отечественными решениями, однако государственная политика импортозамещения стимулирует этот сегмент к постепенному развитию.

В настоящее время одной из целей политики, реализуемой Правительством Российской Федерации, является обеспечение цифрового суверенитета России. Термин «цифровой суверенитет» появился почти пять лет назад. Он рассматривается как цифровая независимость, право государства самостоятельно определять свою информационную политику, распоряжаться информационными ресурсами, инфраструктурой и обеспечивать информационную безопасность на уровне личности, общества, государства. Инфраструктура безопасности цифровой экономики включает автономизацию российской части Интернета, который обеспечит безопасное использование баз данных России, размещенных на серверах на территории нашей страны.

Особенность цифровизации всех сфер экономики в России заключается в том, что одним из драйверов цифровизации в стране является Федеральная налоговая служба Российской Федерации (ФНС России). В настоящее время ФНС России аккумулирует, обрабатывает и хранит большие объемы данных. По результатам научных исследований отмечается, что по состоянию на начало 2022 г. налоговые органы способны администрировать более 150 млн человек, 3,4 млн юридических лиц и 3,5 млн индивидуальных предпринимателей. Ежегодно налоговая служба автоматически обрабатывает 76 млн налоговых деклараций, 15 млрд счетов-фактур по НДС, информацию по 131 млн объектов имущества и по 250 млн сделок по трансфертному ценообразованию [Колосок, Гурина 2019].

---

[1] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (ред. от 30.12.2020; с изм. и доп., вступ. в силу с 01.03.2021) // СПС «КонсультантПлюс». URL: https://student2.consultant.ru/cgi/online.cgi?req=doc&base=NBU&n=373130&dst=0&rnd=5058CE324EE44443B97F776BF895FBF4#07679488274614152 (дата обращения 27 сентября 2022).

На сайте ФНС России реализуется множество цифровых сервисов по:

– уплате налогов и сборов;
– выбору оптимального режима налогообложения;
– созданию и регистрации собственного бизнеса;
– определению уровня налоговой нагрузки;
– определению уровня налогового риска.

Также ФНС России осуществляет доступ к информации из реестров сведений об идентификационном номере налогоплательщиков (как физических, так и юридических лиц), по налоговой и бухгалтерской отчетности; имеются личные кабинеты как юридических лиц (отдельно для российских и иностранных организаций), так и физических лиц, индивидуальных предпринимателей, самозанятых граждан и многое другое. ФНС России формирует и ведет такие реестры, как Единый государственный реестр недвижимости (ЕГРН), Единый государственный реестр юридических лиц (ЕГРЮЛ), Единый государственный реестр индивидуальных предпринимателей (ЕГРИП), Единый реестр субъектов малого и среднего предпринимательства (МСП), Единый государственный реестр записей актов гражданского состояния (ЕГР ЗАГС) и пр. В ведении ФНС России находится ведение системы ФИАС – федеральной информационной адресной системы, БФО – государственного информационного ресурса бухгалтерской (финансовой) отчетности. Всего налоговые органы предоставляют более 80 наборов открытых данных.

Информационной системой, обеспечивающей автоматический сбор, обработку, анализ и предоставление данных о налогоплательщиках по всем направлениям работы ФНС России является автоматизированная информационная система (АИС) «Налог-3». Целевой инфраструктурой, предназначенной для эксплуатации АИС «Налог-3», являются Федеральные центры обработки данных ФНС России в городах Москва и Дубна (Московской области), а также Резервный центр обработки данных № 1 в г. Городец Нижегородской области. Таким образом, ФНС России обеспечивает безопасное хранение и обработку информации, хранящейся в базах данных, размещенных на серверах на территории нашей страны.

Функционирование АИС «Налог-3» позволяет формировать информационные ресурсы налоговых органов, на основе которых принимаются управленческие решения; кроме того, она может являться источником предоставления данных внешним потребителям информации. АИС «Налог-3» является крупнейшей базой данных не только в России, но и (по некоторым оценкам) в мире. Размер базы на настоящее время – около 755 Тбайт с ежедневным

приростом в 1 Тбайт[2]. АИС «Налог-3» является основой для реализации множества проектов, часть из которых не была заложена в проект изначально. Помимо этого, она постоянно развивается, дополняясь все новыми блоками. В частности, в 2021 г. в рамках АИС «Налог-3» было введено в эксплуатацию программное обеспечение, автоматизирующее контроль применения контрольно-кассовой техники, создан сводный реестр задолженности по платежам в бюджет, введен в эксплуатацию блок «Налоговые споры», позволяющий повысить эффективность досудебного урегулирования споров между налогоплательщиками и налоговыми органами. В 2022 г. было введено в промышленную эксплуатацию прикладное программное обеспечение по осуществлению зачета излишне уплаченных налогов. С 1 января 2024 г. АИС «Налог-3» должна получить доступ к информационным системам крупнейших налогоплательщиков – участников программы налогового мониторинга и интегрирована с ними.

Кратко остановимся на некоторых важнейших подсистемах сбора, обработки и хранения информации в рамках основной деятельности налоговых органов.

Несомненно, важнейшим цифровым проектом является автоматизированная система контроля НДС. АСК НДС впервые была запущена в 2013 г. Она позволяет проследить движение товара и расчетов от производителя к конечному потребителю через цепочку продавцов-посредников и выявлять «разрывы» в цепочке НДС (разницу между суммой НДС, которая теоретически должна быть уплачена налогоплательщиками при движении по цепочке добавленной стоимости и суммой фактически уплаченного налога). В настоящее время разработана очередная усовершенствованная версия информационной системы – АСК НДС-3, которая позволяет также отслеживать движение средств по счетам физических и юридических лиц и, кроме того, обнаруживает признаки уклонения от уплаты других налогов. По сравнению с первой версией система обрабатывает больший объем информации и предоставляет более точные сведения. В результате функционирования системы АСК НДС-2 доля сомнительных вычетов сократилась в 17 раз – с 8 до 0,46% (по сравнению с 1 кварталом 2016 г.). Данный показатель считается самым низким в мире. Технологии анализа больших данных позволяют оперативно обрабатывать более 24 Тб данных в годовом исчислении. Другим положительным результатом внедрения АСК НДС является сокращение сроков

[2]Б1 – Консалт. URL: https://www.ey.com (дата обращения 30 сентября 2022).

возмещения НДС из бюджета (для сравнения: общий срок проведения камеральной проверки – 3 мес., срок камеральной проверки по НДС – 2 мес.; уже сейчас планируется сократить данный срок до 1 мес.), автоматизация проверок, а также охват контролем всех сделок, осуществляемых в стране (а это 5 млн деклараций и 15 млрд счетов-фактур в год).

С 2017 г. ФНС России администрирует поэтапный переход всех хозяйствующих субъектов (как организаций, так и индивидуальных предпринимателей) на применение контрольно-кассовой техники с фискальными накопителями (онлайн-касс). Целью применения онлайн-касс является как легализация части оборота, находящегося в теневом секторе экономики, так и обеспечение возможности для государственных органов осуществлять статистический анализ объема и структуры товарных потоков. К 2021 г. в России зарегистрировано 3,6 млн онлайн-касс, через которые ежемесячно проводятся до 4 трлн руб. выручки. Помимо очевидных преимуществ от использования онлайн-касс (повышение прозрачности экономики, уменьшение теневого сектора экономики, создание равной конкурентной среды для организаций торговли, защита интересов покупателей, возможность для покупателей проверять чеки на достоверность и т. д.) появляются и дополнительные. Реализация эксперимента по введению нового налогового режима «Автоматизированная упрощенная система налогообложения» (АУСН) стартовала с 01.07.2022 г. в четырех российских регионах: Москве, Московской и Калужской областях, а также в Республике Татарстан. Данный режим предполагает освобождение налогоплательщиков от формирования и предоставления большого количества отчетности (включая налоговую декларацию), а также от самостоятельного расчета суммы налогов и страховых взносов, причитающихся уплате в бюджет. Функционирование налогового режима основывается на прозрачности информационных потоков.

Очевидным прорывом и в цифровизации, и в деятельности налоговых органов стал эксперимент по введению нового специального налогового режима – налога на профессиональный доход («налога на самозанятых»). Успех реализации данного проекта предрекла не только низкая ставка налога, но и, в первую очередь, легкость и простота использования, которая основывается на применении цифровых инструментов. Регистрация гражданина в качестве самозанятого, а также исчисление и уплата налога осуществляются без посещения налоговых органов, через мобильное приложение «Мой налог». Кроме того, специально разработан API, позволяющий применять налоговые режимы, используя привычные приложения. По состоянию на январь 2022 г. в налоговых орга-

нах зарегистрировано 4,3 млн самозанятых. Фискальный контроль за деятельностью самозанятых граждан осуществляется полностью в цифровой среде, а это – почти 300 млн сформированных чеков. Реализация данного проекта требует от налоговых органов навыков работы с большими данными в потоковом режиме.

Накопленный опыт работы с BigData позволяет налоговым органам вести работу по реализации нового проекта: с 1 июля 2021 г. в России начала функционировать национальная система прослеживания движения товаров, а с 1 июля 2022 г. пилотный проект заработал и в рамках ЕАЭС. Система прослеживания представляет собой документальный контроль движения партий товара вплоть до конечного покупателя. Импортируемые товары будут получать идентификаторы, указание которых будет обязательно при всех операциях с товаром, что существенным образом сократит возможности производства и продажи контрафактного товара. Реализация данного проекта еще больше увеличит объем данных, обрабатываемых налоговой службой.

Накопленный опыт и технические возможности позволяют налоговым органам создавать информационные системы, не имеющие прямого отношения к налоговому администрированию. Так, с 01.01.2018 г. функционирует Единый государственный реестр записей актов гражданского состояния, основанный на информационной системе, созданной в рамках ФНС России. ЕГР ЗАГС позволяет гражданам России получать услуги ЗАГС без привязки к месту проживания (сервис функционирует благодаря системе межведомственного электронного взаимодействия СМЭВ). В системе конвертировано в цифровой формат около 525 млн записей начиная с 1926 г. Объем хранимой и обрабатываемой информации – около 20 Тб. Именно функционирование данного сервиса позволило оперативно оказать помощь семьям с детьми в период распространения коронавируса.

Материалы и методы

Оценку угроз безопасности информационным системам налоговых органов рассматриваем как процесс, в начале которого необходимо оценить и классифицировать риски функционирования информационных систем налоговых органов [Kurbatov 2019]. Содержание деятельности налоговой службы, использование АИС влекут за собой появление событий и действий – угроз, препятствующих достижению стратегических целей и наносящих существенный ущерб экономике и бюджетной системе страны. Конечной целью оценки

рисков является определение вероятности их возникновения и определение существенности ущерба, наносимого реализацией того или иного риска. Можно выделить следующие угрозы, являющиеся источниками рисков: естественные (вызванные объективными физическими явлениями, неподконтрольными человеку) и искусственные (вызванные деятельностью человека). Эти угрозы разделяются на случайные (неумышленные), вызванные ошибками в проектировании систем и элементов, ошибками в программном обеспечении, в действиях персонала и т. п. и преднамеренные (умышленные), связанные с сознательным причинением вреда.

Классифицируем риски по источнику происхождения в табл. 1.

Таблица 1

Классификация рисков по источнику происхождения

Вид риска	Содержание
Организационные риски, связанные с деятельностью сотрудников	ошибки, вызванные низкой квалификацией и отсутствием опыта работы сотрудников; низким уровнем профессиональной коммуникации, информационной и корпоративной культуры; психологическим состоянием сотрудников.
Технические риски	повреждение целостности технических и аппаратных компонентов информационной системы; возможность утечки или перехвата информации по техническим каналам связи компонентов системы; сбои и поломки оборудования.
Технологические риски	нарушение защищенности данных и инфраструктуры в информационной системе от искусственных и естественных воздействий, способных нарушить целостность, доступность, конфиденциальность персональных данных, например масштабный сбой в работе приложений и онлайн-сервисов из-за проблем работы или несовместимости системного обеспечения.
Производственные риски	следствие ошибок при проектировании объекта, в том числе риски причинения вреда окружающей среде как следствие производственных ошибок.

Управление рисками является важнейшим компонентом государственного управления. Негативно воздействовать на АИС «Налог-3» могут внешние и внутренние риски. К внешним рискам отнесем:

– возможность отключения от глобальной Интернет-сети;
– запрет на покупку технических и аппаратных средств автоматизации информационных процессов, производимых в иностранных государствах;
– санкционные ограничения на использование импортного программного обеспечения, систем управления базами данных, связующего ПО и бизнес-приложения.

Данные риски обусловлены масштабной зависимостью России от разработок зарубежных IT-компаний (и, как следствие, от правительств иностранных государств).

В настоящее время Россия практически полностью зависит от зарубежных разработок как в сфере технических средств, так и в сфере технологий: программное обеспечение, электронные средства связи, сеть Интернет и т. д. Все эти разработки широко используются как обычными российскими пользователями, так и государственными структурами. В результате они могут стать объектами манипулирования, шантажа и умышленного нанесения ущерба российской экономике и сфере государственного управления. Признание проблемы на государственном уровне произошло. Правительство РФ инициировало изменения в проводимой налоговой политике, направленные в том числе на стимулирование создания отечественного программного обеспечения (в частности для IT-компаний предусмотрены налоговые льготы). Ведется обсуждение проблемы обособления русскоязычной части сети Интернет (так называемая национализация Интернета).

Реализация угроз, вызванных зависимостью АИС «Налог-3» от разработок зарубежных IT-компаний, способна нанести существенный ущерб отлаженной системе цифровизации деятельности налоговых органов и, как следствие, снизить качество налогового администрирования, эффективность осуществляемого налогового контроля, что отразится на объеме налоговых поступлений и объеме теневого сектора экономики.

Рассмотрим модель, позволяющую оценить вероятность реализации указанных выше угроз и степень их негативного воздействия на систему цифрового взаимодействия налоговых органов с налогоплательщиками, безопасность сформированных ФНС России баз данных, на текущую работу сотрудников налоговой службы.

Моделируя процедуру анализа рисков, можно определить и дать оценку уровню информационной безопасности (ИБ) в ФНС России, которая необходима для устойчивого функционирования информационно-коммуникационных технологий (ИКТ). Рассмотрим их в терминах снижения вероятности реализации риска ИБ и уменьшения возможных последствий в случае его реализации.

В процессе оценки устанавливаются пороговые значения приемлемого уровня риска и определяются критерии для своевременного предоставления полной и достоверной информации заинтересованным лицам для принятия управленческих решений.

Согласно международным стандартам и лучшим практикам в области управления рисками процедура анализа риска ИБ реализуется в рамках двух этапов – идентификации риска и оценки риска[3]. Идентификация риска ИБ проводится применительно к ключевым информационным активам (ИА) ФНС России. На этапе идентификации определяются:

– перечень ИА, входящих в область оценки;
– временной горизонт;
– перечень актуальных угроз для рассматриваемых ИА;
– перечень мер и средств защиты.

Определяются ключевые информационные системы организации, обрабатываемая информация и присущие риски ИБ. Ценность информационных активов определяется их владельцами исходя из:

– ценности обрабатываемой информации;
– ценности информационной системы;
– влияния на основную деятельность в случае реализации риска.

Идентификация временного горизонта представляет собой определение периода времени, в течение которого идентифицированный риск ИБ в ИКТ ФНС России остается актуальным. Принимается, что в течение выбранного периода компоненты риска ИБ, включая значения его уровня и рейтинга, остаются неизменными.

Отсчет временного горизонта начинается с момента идентификации риска. При реализации изменений в компонентах риска, в том числе вследствие действий по митигации риска, отсчет прекращается. По истечении либо прекращении отсчета временного горизонта риск ИБ требует повторной идентификации и переоценки, после проведения которых отсчет временного периода начинается заново.

Значением временного горизонта по умолчанию для рисков ИБ ИКТ ФНС России возможен 1 год. Для каждого индивидуального случая выявления риска ИКБ данное значение может быть изменено, исходя из индивидуальных особенностей риска.

---

[3] ISO/IEC 27005: 2018. Information technology – Security techniques – Information security risk management // ISO. URL: https://www.iso.org/standard/75281.html (дата обращения 30 сентября 2022); FIPS 199 Standards for Security Categorization of Federal Information and Information Systems, February 2004 // NIST. URL: https://csrc.nist.gov/publications/detail/fips/199/final (дата обращения 30 сентября 2022).

Угрозы ИБ реализуются их источниками, которые могут воздействовать на объекты среды активов ФНС России. В случае успешной реализации атаки информационные активы теряют частично или полностью свойства защищенности и/или устойчивости. Атака может включать в себя реализацию одной или более угроз ИБ. Эффективность мер защиты определяется для снижения или полного исключения вероятности реализации актуальных угроз, применимых к активу.

Для оценки рейтинга и уровня риска ИБ необходимо определить значения следующих показателей: ценность ИА; вероятность возникновения угрозы.

Для оценки ценности ИА необходимо определить категорию обрабатываемой информации и ее ценность, ключевые ИКТ и их ценность в терминах, а также влияние на бизнес в случае выхода из строя ИКТ.

Критерии оценки ценности информационных активов и информационной безопасности, с соответствием качественных и цифровых значений[4], использующихся при расчете качественного уровня риска, представлены в табл. 2.

Таблица 2[5]

Критерии оценки ценности актива

Качественное значение	Описание критерия	Цифровое значение
Очень низкая	Основной функцией ИКТ является обслуживание внутренних пользователей. Сбой в работе ИКТ более 72 час не приведет к ущербу компании.	1
Низкая	Основной функцией ИКТ является обслуживание внутренних пользователей. Сбой в работе ИКТ приведет к недоступности одного или нескольких поддерживающих процессов, что не приведет к негативным последствиям для организации. Утечка информации не приведет к негативным последствиям для организации.	2

[4] Все приведенные цифровые значения могут быть скорректированы в зависимости от особенностей оцениваемого риска.

[5] Приведенные цифровые значения в табл. 3 носят экспертный характер и могут быть скорректированы в зависимости от особенностей оцениваемого риска.

Окончание табл. 2

Качественное значение	Описание критерия	Цифровое значение
Средняя	ИКТ используется для обслуживания клиентов (или контрагентов). Основной функцией ИКТ является подготовка отчетности, установленной законодательно. Сбой в работе ИКТ до 4 часов приведет к нарушению внутреннего функционирования организации. Утечка информации может привести к предписаниям со стороны регулятора и надзорных органов.	3
Высокая	ИКТ используется для обслуживания клиентов (или контрагентов). Основной функцией ИКТ является подготовка отчетности, установленной законодательно. Сбой в работе ИКТ до 2 часов приведет к ущербу для организации (жалобы со стороны заинтересованных сторон). Утечка информации может привести к оттоку клиента, массовым штрафным санкциям со стороны регулятора и надзорных органов, к срыву реализации стратегических инициатив. Модификация информации приведет к косвенным потерям для организации.	4
Очень высокая	ИКТ используется для обслуживания клиентов (или контрагентов). ИКТ используется для проведения транзакций. Сбой в работе ИКТ до 30 мин приведет к значимому ущербу для компании (жалобы со стороны заинтересованных сторон). Утечка информации может привести к сокращению числа клиентов, расторжению договорных обязательств, массовым штрафным санкциям со стороны регулятора и надзорных органов, к потере технологического/технического лидерства, к срыву долгосрочной стратегии. Модификация информации приведет к массовым штрафным санкциям со стороны регулятора и надзорных органов.	5

Критерии оценки степени влияния на устойчивость в случае реализации риска, с соответствием качественных и цифровых значений, использующимися при расчете качественного уровня риска и их описанием, представлены в табл. 3.

Таблица 3

Критерии оценки степени влияния
на бизнес-процессы

Качественное значение	Описание критерия	Цифровое значение
Критическое	Остановка деятельности. Международная огласка негативной информации в сети Интернет, понижение рейтингов рейтинговыми агентствами. Наложение массовых штрафных санкций со стороны регулятора и надзорных органов. Совместные гражданские иски, предъявляемые к организации. Массовая выплата компенсаций. Потеря ключевых работников.	6
Высокое	Возможное распространение негативной информации в сети Интернет на международном уровне, понижение рейтингов рейтинговыми агентствами. Наложение штрафных санкций со стороны регулятора и надзорных органов. Совместные гражданские иски, предъявляемые к организации. Отток кадров.	4,5
Среднее	Возможное распространение негативной информации в сети Интернет на региональном уровне. Наложение отдельных штрафных санкций со стороны регулятора и надзорных органов. Ограниченное число исков и выплат компенсаций клиентам в судебном порядке. Риски увеличения оттока кадров.	2
Низкое	Отсутствие информации негативного характера в Интернете. Активность со стороны регулятора и надзорных органов выражена в рамках нефинансовых санкций, например вынесение предупреждений. Жалобы со стороны клиентов, не повлекшие за собой финансовых компенсаций.	1

Переходим к расчету ценности актива. По каждому риску составляется таблица значений риск-факторов ущерба, имеющая вид, описанный в табл. 4.

Таблица 4[6]

Риск-факторы ущерба

Риск-фактор ущерба	Цифровое значение риск-фактора ущерба	Максимально возможное цифровое значение (A_{imax})
Ценность информации	A_1	5
Ценность ИКТ	A_2	5
Влияние на бизнес-процессы	A_3	6

Цифровые значения риск-факторов ущерба A_1, A_2, A_3 заполняются на основе фактических значений в соответствии с табл. 2 и 3.

Применительно к одному информационному активу может оцениваться более одной категории информации и информационной системы. Совокупная ценность применительно к риск-фактору ущерба определяется по следующей формуле:

$$A_{jc} = \sqrt[k]{\prod_{i=1}^{k} A_k}, \quad (1)$$

где A_{jc} – совокупное значение риск-фактора ущерба, $i \in \{1, \dots, k\}$,
k – количество значений, проставленных для оцениваемого риск-фактора ущерба.

Итоговое значение ценности актива рассчитывается следующим о образом:

$$Val = \frac{A_{1c} + A_{2c} + A_{3c}}{A_{1max} + A_{2max} + A_{3max}} \quad (2)$$

Расчет вероятности реализации угроз (P_y) с соответствием качественных и цифровых значений, использующихся при расчете качественного уровня риска в соответствии с критериями, представлены в табл. 5. Цифровые значения носят экспертный характер и могут быть скорректированы в зависимости от особенностей оцениваемого риска.

[6] Приведенные максимально возможные цифровые значения в табл. 4 носят экспертный характер и могут быть скорректированы в зависимости от особенностей оцениваемого риска.

Таблица 5

Критерии оценки вероятности возникновения угроз

Качественное значение	Описание критерия	Цифровое значение
Очень высокая	Нарушители, скорее всего, предпримут попытку реализовать угрозу информационной безопасности.	0,87
Высокая	Скорее предпримут, чем не предпримут.	0,62
Средняя	Скорее не предпримут, чем предпримут.	0,37
Низкая	Нарушители, скорее всего, не предпримут попытку реализовать угрозу информационной безопасности.	0,12

Критерии оценки эффективности мер защиты (P_m) с соответствием качественных и цифровых значений, использующихся при расчете качественного уровня риска, так же как и в предыдущей таблице, носят экспертный характер и представлены в табл. 6.

Таблица 6

Критерии оценки эффективности мер защиты

Качественное значение	Описание критерия	Цифровое значение
Высокая	Мера защиты, скорее всего, предотвратит реализацию угрозы через уязвимость нарушителем.	0,9
Средняя	Скорее предотвратит, чем не предотвратит.	0,5
Низкая	Скорее не предотвратит, чем предотвратит.	0,1
Мера отсутствует	Мера защиты гарантированно не предотвратит реализацию угрозы через уязвимость нарушителем.	0

Повышающий коэффициент (k) вероятности реализации риска зависит от количества инцидентов и вероятности реализации угроз и устанавливается в соответствии с табл. 7.

Таблица 7

Определение коэффициента вероятности

Вероятность реализации (P_y) / Количество инцидентов (k)	Низкая	Средняя	Высокая	Очень высокая
Не было	1	1	1	1
Были, 1–2 раза	1,7	1,5	1,3	1,1
Были, 3 и более раз	1,9	1,7	1,5	1,14

Итоговое значение вероятности реализации риска определяется по следующей формуле:

$$P = P_y * k * (1 - P_m), \quad (3)$$

где P – вероятность реализации риска.

Результаты

Проведем расчет значения уровня риска (R); рассчитаем его, перемножив вероятность реализации риска (P) на значение ценности актива (Val).

$$R = P * Val, \quad (4)$$

Для присвоения качественного уровня риска используется шкала в табл. 8.

Таблица 8

Шкала уровней риска

Критический	Высокий	Средний	Низкий
$0,75 \leqslant R$	$0,5 \leqslant R < 0,75$	$0,25 \leqslant R < 0,5$	$R < 0,25$

Итоговое качественное значение совокупного уровня подверженности ФНС России риску ИБ (R_c) определяется по следующей формуле:

$$R_c = \sqrt[k]{\prod_{i=1}^{k} R_i}, \quad (5)$$

где $i \in \{1, \ldots, k\}$, где k – количество значений оцененных рисков КБ.

Итоговое значение подверженности риску информационной безопасности определяется на основе шкалы табл. 9.

Таблица 9

Шкала подверженности риску информационной безопасности

Рейтинг	1 (очень высокий)	2 (высокий)	3 (средний)	4 (низкий)	5 (очень низкий)
Значение R_c	$0{,}8 < R_c$	$0{,}6 < R_c \leqslant 0{,}8$	$0{,}3 < R_c \leqslant 0{,}6$	$0{,}1 < R_c \leqslant 0{,}3$	$R_c \leqslant 0{,}1$

Установим пороговые значения, которые представляют собой предел (лимит) или допустимое отклонение, превышение которого указывает на то, что воздействие риска ИКБ является неприемлемым, и необходимо предпринять ответные меры на уровне руководства организации (ФНС России или даже Минфина России).

В рамках данной методики в качестве пороговых значений выступают:

– контрольный (лимитный) уровень, который определяет допустимый порог толерантности;
– сигнальный (приемлемый) уровень, который служит сигналом раннего предупреждения о приближении к контрольному уровню.

Для визуального обозначения пороговых значений применяется «трехзонная» система:

– превышение значения R_c = 0,6 – достигается контрольный уровень – «красная» зона;
– при нахождении R_c в интервале между сигнальным и контрольным уровнями – «желтая» зона;
– при значении R_c меньше 0,4 не достигается сигнальный уровень – «зеленая» зона.

Описание значений подверженности риску ИКБ и необходимые действия по обработке рисков ИБ приведены в табл. 10.

Таблица 10

Описание значений рейтинга P

Рейтинг	Описание рейтинга	Необходимые действия
1 – очень высокий	– Прогнозируется скачок количества и опасности успешных кибератак на организацию. – Наличие критичных уязвимостей в процессах и технологиях организации. – Ожидается резкое увеличение объема успешных мошеннических операций в отношении организации или ее клиентов. – Существует опасность остановки критичных процессов организации. – Велика вероятность потери конфиденциальности или доступности критичной информации, полученной в рамках обмена с внешними организациями.	Необходимо немедленное принятие решения по обработке рисков на уровне руководства
2 –высокий	Прогнозируется увеличение количества успешных кибератак на организацию. Наличие критичных уязвимостей в процессах и технологиях организации. Ожидается резкое увеличение объема успешных мошеннических операций в отношении организации или ее клиентов. Существует опасность остановки критичных процессов организации. Велика вероятность потери конфиденциальности или доступности критичной информации, принадлежащей организации.	Необходимо немедленное принятие решения по обработке рисков на уровне руководства
3 – средний	Имеется тенденция к росту количества успешных кибератак. Прогнозируется увеличение объемов мошенничества в отношении организации и ее клиентов. Существует опасность нарушений функционирования критичных процессов. Существуют предпосылки к потере конфиденциальности или доступности важной информации, принадлежащей компании.	Необходимо принятие решений по обработке рисков в рабочем порядке

Окончание табл. 10

Рейтинг	Описание рейтинга	Необходимые действия
4 – низкий	Кибератаки на организацию отражаются в рабочем порядке. Недоступность активов в результате инцидентов восстанавливается в штатном режиме. Объем успешных мошеннических операций может незначительно изменяться. Не ожидается утечек конфиденциальной информации с ощутимыми последствиями.	Необходим мониторинг за уровнем рисков с целью недопущения перехода на более высокий уровень
5 – очень низкий	Кибератаки отражаются в рабочем порядке. Нет предпосылок к нарушению конфиденциальности информации, недоступности и целостности активов организации.	Нет необходимости вмешательства, только мониторинг

Обсуждение

Вопросы обеспечения ИБ являются актуальными в последние десятилетия во всем мире. В качестве внешних угроз ИБ России на общегосударственном уровне можно выделить атаки на российскую информационную инфраструктуру; усиление деятельности организаций, осуществляющих техническую разведку в отношении российских государственных органов, оказание информационно-психологического воздействия на дестабилизацию внутриполитической и социальной ситуации в России, приводящего к подрыву суверенитета и нарушению территориальной целостности и т. д. Вычленение подобных угроз определяется объектом исследования ИКТ российских органов власти и управления в целом.

В то же время применение подхода, основанного на анализе рисков ИБ в узкоспециализированной сфере, приводит к выделению другого перечня угроз, а применение конкретных математических методов приводит к появлению разнообразных моделей. Например, для анализа рисков в сфере интеллектуальных энергетических систем [Колосок, Гурина 2019] оценку риска предлагается проводить на основе теории нечетких множеств. При этом угроза безопасности ИКТ рассматривается в качестве одного из компонентов органи-

зационного риска, который может включать в себя многие виды риска (например, инвестиционный риск, риск управления программой, риск безопасности и т. д.). В качестве входных переменных рассматриваются возможности, намерения, цели противника, уязвимости ИКТ и воздействия на нее. Выходными переменными являются вероятность инициирования угрозы, вероятность события угрозы, полная вероятность реализации и риск.

Необходимо отметить, что в России и международном сообществе особое внимание уделяется вопросам ИБ критической информационной инфраструктуры [Korotkov, Zinov'eva 2011]. В Российской Федерации, в частности, под критической информационной инфраструктурой понимают «информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов». В соответствии с данным подходом ИКТ налоговых органов с полным правом можно отнести к критической информационной инфраструктуре.

Таким образом, если вопросы обеспечения ИБ являются актуальной для обсуждения темой, то вопросы оценки риска ИБ становятся объектом исследования существенно реже. Изучение подверженности ИКТ налоговых органов рискам можно проводить в контексте критической информационной инфраструктуры, но необходимо отметить, что при таком подходе не будут учтены специфические особенности именно ИКТ ФНС России. Анализ же исследований оценки подверженности ИКТ рискам ИБ в узкоспециализированных сферах показал, что серьезные исследования относительно ИКТ Федеральной налоговой службы практически отсутствуют, т. е. данная тема является недостаточно разработанной.

Заключение

Методика управления ИБ ФНС России основана в этой работе на экспертном анализе рисков АИС «Налог-3», в этом заключается ее новизна. Безопасность функционирования ИКТ налоговой службы напрямую связана с безопасностью налогово-бюджетной системы страны, вопросы ее обеспечения можно отнести к обеспечению национальной безопасности Российской Федерации. На фоне внешнего роста угроз ИБ государственных организаций необходимо начать анализировать возможности по снижению рисков ИБ и оценивать свой уровень риска, который организа-

ция готова принять, не предпринимая дополнительных действий для его снижения. Максимально нивелировать риски ИБ – это непростая задача, связанная с поиском баланса между величиной потерь от реализации угроз ИБ и инвестиций в снижение вероятности наступления событий ИБ. Если в качестве основной цели определить снижение риска ИБ, то предлагаемый подход поможет лицу, принимающему решения (руководству) добиться четких, прагматичных результатов, которые могут быть реализованы в виде проектных инициатив в целях осуществления стратегических и тактических действий в части улучшения системы обеспечения ИБ, позволяя организации направлять свои усилия на наиболее уязвимые компоненты ИС; особенно это применимо к задачам, связанным с внедрением сложных контролей, включая средства защиты информации. Например, точнее и эффективнее расставлять приоритеты при выделении бюджетов на ИБ.

Функционирование модели основывается на идентификации рисков, определении ценности информационных активов, подвергаемых угрозам, и определении степени влияния реализованных рисков на организацию бизнес-процессов в организации. Оценка риска ИБ предполагает выявление риск-факторов ущерба в отношении каждого риска и определение итогового значения ценности информационного актива посредством расчета показателя совокупного риск-фактора ущерба в отношении каждого идентифицированного риска. Расчет итогового значения вероятности реализации риска осуществляется на основе оценки вероятности возникновения угроз (с использованием коэффициента вероятности реализации риска) и оценки эффективности мер защиты от возможности реализации риска. Таким образом, итоговое значение уровня риска ИБ определяется двумя факторами – вероятностью реализации риска и уровнем ценности актива. Установление пороговых значений в отношении уровня риска позволяет оптимизировать управление рисками (выражающееся в принятии управленческих решений для предотвращения реализации риска).

Преимущества данной модели заключаются в возможности для сотрудников налоговых органов самостоятельно идентифицировать риски, актуальные на данный момент, оценивать вероятность возникновения угроз и нанесения ущерба вследствие их реализации, что позволит в нужный период установить текущую подверженность ИКТ риску ИБ. Также модель позволит определить необходимую скорость реакции на существующий риск и уровень компетенции должностных лиц, принимающих решения по управлению рисками.

Литература

Колосок, Гурина 2019 – *Колосок И.Н., Гурина Л.А.* Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры интеллектуальной энергетической системы // Информационные и математические технологии в науке и управлении. 2019. № 2 (14). С. 40–51.

Korotkov, Zinov'eva 2011 – *Korotkov A.V., Zinov'eva E.S.* Security of critical information infrastructures in international humanitarian law // Bulletin of MGIMO. 2011. Vol. 4. P. 154–162.

Kurbatov 2019 – *Kurbatov N.M.* On the formation of legal and scientific bases of ensuring the safety of critical information infrastructure of the Russian Federation // Bulletin of Udmurt University. 2019. Vol. 29 (5). P. 644–654.

References

Kolosok, I.N. and Gurina, I.N. (2019), "Assessment of cybersecurity risks for the information and communication infrastructure of the intelligent energy system", *Information and mathematical technologies in science and management,* vol. 2 (14). pp. 40–51.

Korotkov, A.V. and Zinov'eva, E.S. (2011), "Security of critical information infrastructures in international humanitarian law", *Bulletin of MGIMO,* vol. 4, pp. 154–162.

Kurbatov, N.M. (2019), "On the formation of legal and scientific bases of ensuring the safety of critical information infrastructure of the Russian Federation", *Bulletin of Udmurt University*, vol. 29, no. 5. pp. 644–654.

Информация об авторах

Юлия Ю. Косенкова, кандидат экономических наук, доцент, Финансовый университет при Правительстве РФ, Москва, Россия; 125167, Россия, Москва, Ленинградский проспект, д. 49/2; kkosenkova-@list.ru

Сергей В. Романовский, аспирант, Московский государственный лингвистический университет, Москва, Россия; 119034, Россия, Москва, ул. Остоженка, д. 38, стр. 1; svromanovskiy@gmail.com

Елена П. Цацкина, кандидат педагогических наук, доцент, Московский государственный лингвистический университет, Москва, Россия; 119034, Россия, Москва, ул. Остоженка, д. 38, стр. 1; e.tsaskina@linguanet.ru

Information about the authors

Yulia Yu. Kosenkova, Cand. of Sci. (Economy), associate professor, Financial University under the Government of the Russian Federation, Moscow, Russia; bld. 49/2, Leningradsky Av., Moscow, Russia, 125167; kosenkova-@list.ru

Sergei V. Romanovskii, postgraduate student, Moscow State Linguistic University, Moscow, Russia; bldg. 1, bld. 38, Ostozhenka St., Moscow, Russia, 119034; svromanovskiy@gmail.com

Elena P. Tsatskina, Cand. of Sci. (Pedagogy), associate professor, Moscow State Linguistic University, Moscow, Russia; bldg. 1, bld. 38, Ostozhenka St., Moscow, Russia, 119034; e.tsaskina@linguanet.ru

УДК 005.342
DOI: 10.28995/2686-679X-2023-2-70-80

Комплаенс в области информационной безопасности

Ирина А. Русецкая
Российский государственный гуманитарный университет, Москва, Россия, irkom@mail.ru

Аннотация. Статья посвящена исследованию основных подходов к организации комплаенса при решении проблем обеспечения информационной безопасности. Анализируется понятие комплаенса, основных его составляющих. В статье рассматривается система функций комплаенса. Автор проводит анализ категорий норм и требований, лежащих в основе реализации функций комплаенса, а также примеры правовых и нормативно-методических документов в сфере комплаенса информационной безопасности. В статье отмечаются особенности современного развития комплаенса в России в различных сферах. Рассматриваются основные задачи комплаенс-контроля в сфере информационной безопасности в российских организациях. Выделяются области, в которых реализация комплаенс-функций является особенно значимой. Проводится анализ проблем обеспечения защиты информации, которые могут быть решены при помощи использования методик комплаенса, а также инструментария, применяемого для этого. Особое внимание автор уделяет вопросам автоматизации комплаенса и анализу инструментов, которые могут при этом использоваться. В статье рассматриваются преимущества автоматизированного комплаенса перед традиционным, а также примеры существующих в сфере автоматизации комплаенса разработок. Автор статьи рассматривает факторы, указывающие на наличие в компании развитой системы комплаенса, а также значение этих факторов в обеспечении информационной безопасности организаций.

Ключевые слова: комплаенс, информационная безопасность, DLP-системы, защита информации, угрозы безопасности

Для цитирования: Русецкая И.А. Комплаенс в области информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 2. С. 70–80. DOI: 10.28995/2686-679X-2023-2-70-80

Compliance in information security

Irina A. Rusetskaya
Russian State University for the Humanities, Moscow, Russia;
irkom@mail.ru

Abstract. The article is about studying the main approaches to the organization of compliance in solving the issues of ensuring information security. It analyzes the concept of compliance and its main components. Considering the system of compliance functions, the author also analyzes the categories of norms and requirements that underlie the implementation of compliance functions, as well as examples of legal and regulatory documents in the field of information security compliance. There are notes on features of the modern development of compliance in Russia in various fields. The main tasks of compliance control in the field of information security in Russian organizations are considered. Areas are identified in which the implementation of compliance functions is especially significant.

The article considers that the information protection can be ensured by using compliance techniques, as well as the necessary tools used for that. The author pays special attention to the issues of compliance automation, and the analysis of the tools that can be used for that. The article discusses the advantages of automated compliance over the traditional one, as well as examples of existing developments in the field of compliance automation. The author of the article also considers the factors indicating the presence of a developed compliance system in the company, as well as the importance of those factors in ensuring the information security of organizations.

Keywords: compliance, information security, DLP systems, information protection, security threats

For citation: Rusetskaya, I.A. (2023), "Compliance in information security", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 70–80, DOI: 10.28995/2686-679X-2023-2-70-80

Введение

В настоящее время комплаенс является одним из необходимых элементов комплексных систем защиты информации, реализуя функцию внутреннего и внешнего контроля информационной безопасности. В свою очередь это означает защиту информационных объектов от внешних и внутренних угроз, в том числе от тех, которые определяются так называемым «человеческим фактором», что является сегодня остроактуальной задачей [Русецкая 2022].

Понятие комплаенса пришло в Россию из международной практики и активно внедряется в деловую среду в последние годы.

Существуют различные подходы к трактовке понятия «комплаенс» [Алешина 2019]. Суммируя основные из них, можно прийти к следующему выводу. Комплаенс в общем виде представляет собой деятельность по выявлению и предотвращению фактов несоответствия деятельности компании или ее сотрудников нормативно-правовым и этическим нормам.

Как следует из приведенного определения понятия, комплаенс имеет отношение к двум аспектам деятельности в сфере информационной безопасности: он обеспечивает предотвращение, профилактику нарушений установленных норм и требований, а также позволяет построить систему выявления и реагирования на уже произошедшие инциденты. Эти два аспекта являются взаимосвязанными.

Целью данной работы является анализ основных современных подходов к реализации в российских компаниях комплаенс-функций в сфере обеспечения информационной безопасности.

Место и значение комплаенса при решении проблем обеспечения информационной безопасности

Комплаенс предполагает соответствие деятельности компании требованиям как регуляторов, так и других субъектов деловых отношений: контрагентов, поставщиков, клиентов.

При этом речь идет о соблюдении не только нормативных требований, но и этики ведения бизнеса.

В случае нарушения этих норм возможны финансовые, репутационные потери, урон конкурентоспособности фирмы, наложение санкций, штрафов и другие неблагоприятные последствия.

В сфере информационной безопасности в России особенное внимание в настоящее время уделяется регуляторами сфере ответственности за нарушения, касающиеся обработки и защиты персональных данных, а также защиты объектов критической информационной инфраструктуры.

Ярким примером из мировой практики, указывающим на необходимость уделять внимание комплаенсу в части соответствия деятельности компании требованиям в области информационной безопасности, может служить список санкций, налагаемых за нарушение Закона о защите персональных данных (The General Data Protection Regulation (GDPR)), действующего в Евросоюзе. Этот

закон вступил в действие в 2018 г. и за недолгое время стал известен как один из наиболее строгих законов в мировой практике. За нарушение положений, касающихся защиты персональных данных граждан, их утечку или сбор и обработку персональных данных без разрешения лица, к которому они относятся, закон, в частности, предполагает штрафы в размере до 20 млн евро, или 4% от общего оборота компании за год [Тарасов 2022].

Таким образом, реализация комплаенс-функций является важным фактором сохранения ресурсов и репутации компании.

При этом комплаенс является достаточно широким понятием и имеет отношение к различным сторонам деятельности организаций.

Система функций комплаенса может включать в себя:

- правовой комплаенс;
- финансовый комплаенс;
- комплаенс в области информационной безопасности;
- комплаенс в области риск-менеджмента;
- комплаенс в сфере здоровья, экологии, безопасности продукции и окружающей среды;
- комплаенс в области информационно-аналитической деятельности;
- антикоррупционный комплаенс;
- антимонопольный комплаенс;
- комплаенс в сфере трудового права;
- комплаенс в сфере антитеррористической деятельности и др. направления [Свиридюк 2022].

По мнению специалистов, наиболее активно комплаенс в России внедряется в жизнь в таких сферах деятельности, как финансовый сектор, медицина и торговля. Вслед за ними развиваются комплаенс-функции в области информационных и телекоммуникационных технологий и СМИ[1].

Комплаенс предполагает контроль соответствия деятельности организации в области следующих норм и категорий требований:

- законодательных и нормативных норм государства, к которым относятся законные и подзаконные акты;
- иностранного законодательства, как имеющего экстерриториальный характер (например, касающегося норм, направленных на противодействие финансирования терроризма, отмывания денег, манипулирования инсайдерской информа-

[1] Как устроена комплаенс-политика в российских ИТ-компаниях // TAdviser, 16.11.2021. URL: https://www.tadviser.ru/index.php/Статья:-Комплаенс-политика_ИТ-компаний_в_России (дата обращения 11 февраля 2023).

цией и т. п.), так и касающегося работы компании в рамках партнерского сотрудничества с другими странами;
– международного законодательства в части, являющейся ратифицированной в стране;
– отраслевых, национальных и международных стандартов;
– нормативно-методических документов, принятых в данной организации (в частности, должностных инструкций, положений, политик, соглашений, регламентов и пр.);
– этических требований корпоративной культуры организации (которые могут носить рекомендательный характер и быть изложены, например в Кодексе корпоративной культуры компании).

В каждой из перечисленных сфер существуют свои документы, регулирующие вопросы комплаенса.

В качестве примера из российского законодательства можно привести Федеральный закон «О защите конкуренции» № 135-ФЗ, который направлен на регулирование функции антимонопольного комплаенса. В соответствии с его положениями каждая организация должна создать систему антимонопольного комплаенса, а также разместить на своем официальном сайте соответствующий документ, принятый компанией [Тарасов 2022].

В сфере информационной безопасности законодательными актами, лежащими в основе реализации комплаенс-функций, являются, например, Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ, Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ, Доктрина информационной безопасности Российской Федерации (утв. Президентом Рос. Федерации 05.12.2016, № Пр-646) и др.

К внутренним нормативно-методическим документам компаний, регламентирующих деятельность по обеспечению защиты информации, могут быть отнесены, например: Политика информационной безопасности, Положение о защите коммерческой тайны, Положение о персональных данных, Кодекс корпоративного поведения и пр.

Одной из важных задач комплаенс-контроля в сфере обеспечения информационной безопасности является оценка и выявление различных видов рисков, к которым можно отнести:
– репутационные;
– правовые;
– операционные;
– поведенческие;
– риски взаимодействия и др. [Гунина, Савич, Решетов 2021].

Основными задачами комплаенс-контроля информационной безопасности в организации будут являться следующие:

– составление ранжированного реестра норм и требований с учетом возможности использования различных поисковых фильтров, его пополнения и изменения [Стариков 2021];
– выявление и оценка потенциальных угроз безопасности и комплаенс-рисков;
– внедрение мер и средств по предотвращению угроз информационной безопасности;
– анализ и контроль эффективности используемых мер;
– мониторинг новых факторов и событий, которые могут повлиять на состояние дел в сфере компетенции комплаенс;
– консультации руководства и персонала в сфере комплаенса [Яковлева 2022].

Происходящие в мире и в России процессы цифровизации требуют использования не только традиционных технологий комплаенса, но и внедрения автоматизации комплаенс-контроля, а также использования цифровых технологий в этой области. Автоматизация функций комплаенса позволяет получить следующие преимущества:

– минимизация затрат времени и труда персонала;
– возможность учета большого количества данных, в частности в рамках использования Big Data;
– возможность непрерывного анализа инцидентов и модуляций оцениваемых критериев в режиме реального времени;
– возможность удаленного мониторинга событий;
– возможность оперативной обработки данных и реагирования на события.

Для автоматизации функций комплаенса в настоящее время, в частности, активно используются следующие инструменты[2]:

– legal Tech (legal technology);
– e-discovery (electronic discovery);
– инструменты для автоматизации горячей линии;
– DLP-системы.

Рассмотрим особенности применения в рамках комплаенса перечисленных инструментов более подробно.

Legal technologies представляют собой совокупность технологических решений для юристов и их клиентов, которые можно разделить на два класса в соответствии с кругом решаемых задач.

---

[2] Автоматизация комплаенс: обзор существующих решений // Legal-network, 04.12.2020. URL: https://legal-network.ru/blog/avtomatizatsiya_komplaens_obzor_suschestvuyuschih_resheniy-i160 (дата обращения 10 февраля 2023).

1. Инструменты, используемые для автоматизации работы юристов, например позволяющие им составлять документы, обеспечивать для них дополнительные уровни безопасности, оказывать ряд юридических услуг дистанционно, анализировать изменения в законодательстве и т. п.

2. Информационно-аналитические сервисы, позволяющие получать и анализировать различные данные, например случаи мошенничества, несанкционированного использования конфиденциальной информации, недобросовестной конкуренции и т. п. [Кириллов 2021]. К этим же инструментам относятся сервисы для проверки партнеров, контрагентов, поставщиков и других субъектов деловых отношений, которые позволяют, например, проверить платежеспособность субъекта, получить информацию о предоставлении недостоверной информации и пр.

Технологические решения второго из рассмотренных классов могут использоваться в рамках решения задач комплаенса.

Под e-discovery понимаются инструменты, реализующие процесс поиска, хранения, обработки, анализа, защиты и предоставления цифровых доказательств, которые могут иметь юридическую значимость.

Использование решений e-discovery базируется на том несомненном факте, что использование и хранение электронных документов (включающих текстовые документы, электронные письма, фотографии, аудио- и видеосообщения и т. д.) создает риски, которыми следует управлять, а следовательно, должны быть созданы методики и инструменты, которые позволяют эти риски минимизировать.

Такого рода решения могут применяться в рамках комплаенса для проверки соблюдения нормативно-правовых требований, составления ответов на запросы регуляторов и контролирующих органов, для расследования инцидентов в области информационной безопасности, расследования случаев кражи интеллектуальной собственности, утечки конфиденциальной информации, случаев кибермошенничества и пр.

Для автоматизации комплаенса в сфере информационной безопасности используются также различные решения для автоматизации горячей линии комплаенса.

Под горячей линией комплаенса понимается клиентоориентированный канал связи, пользуясь которым сотрудник организации может сообщить о готовящемся или происшедшем факте нарушения действующих требований. В качестве такого канала может выступать телефон, электронная почта, форма связи на сайте и т. д.

В качестве современных требований к организации горячей линии могут выступать:

– анонимность и конфиденциальность связи;
– доступность 24 часа в сутки, 365 дней в году из любой точки мира;
– мультиязычность;
– бесплатный доступ к сервису;
– возможность обращения в разных режимах: текстовом или голосовом.

Сотрудник службы комплаенс при использовании автоматизированного сервиса должен иметь возможность осуществлять следующие функции:

– структурировать и ранжировать полученные сообщения;
– анализировать статистику событий;
– составлять отчеты на основании полученных сообщений и направлять их в соответствующие структуры компании или руководителям подразделений;
– создавать электронные архивы событий и статистических данных.

Для автоматизации функций комплаенса, как было указано выше, также используются DLP-системы, представляющие собой программные решения, защищающие организацию от утечек данных в рамках корпоративной переписки и переговоров.

При этом должны быть учтены нормативно-правовые требования по сохранению личной информации сотрудников. Для этого анализ получаемых с помощью DLP-систем данных должен проводиться открыто, с письменного разрешения сотрудника, к которому эти данные имеют отношение, и в соответствии с положениями принятых в организации регламентов, касающихся использования DLP-систем. В частности, среди положений таких регламентов должны быть требования по ограничению использования в корпоративной переписке и переговорах конфиденциальной информации компании и сведений, касающихся личной жизни работников [Кундышева, Русецкая 2019].

Заключение

Таким образом, в данной работе были рассмотрены основные идеи, лежащие в основе использования комплаенса для нужд обеспечения информационной безопасности.

Внедрение системы комплаенс-контроля в области информационной безопасности может помочь решить следующие задачи:

– обнаружение и предотвращение инцидентов в области информационной безопасности, создающих угрозы как информации организации, так и бизнесу в целом;
– снижение финансовых, репутационных, правовых и других рисков;
– повышение экономической эффективности и конкурентоспособности деятельности компании и ее финансового потенциала;
– сохранение и упрочение деловой репутации во внешней информационной среде как в России, так и за рубежом;
– поддержание необходимого для успешного функционирования организации уровня корпоративной культуры.

О развитой системе комплаенса в организации могут свидетельствовать следующие факторы:
– наличие развивающейся комплаенс-стратегии;
– учет комплаенс-функции при принятии стратегических решений компанией;
– отражение комплаенс-функций во внутренних документах организации и регламентах корпоративного поведения;
– системный мониторинг реализации подконтрольных комплаенсу норм и требований;
– контроль и прогнозирование всей совокупности рисков и угроз;
– систематическое обучение сотрудников организации навыкам в рассматриваемой сфере (включая рассылку материалов по комплаенсу, организацию тематических квизов и прохождения тестов, проведение лекций, тренингов, обучения в формате видеосеминаров и пр.);
– заложенные в комплаенс механизмы дальнейшего совершенствования;
– автоматизация комплаенс-функций;
– наличие профессиональных сотрудников, занимающихся комплаенсом (комплаенс-менеджеров).

Особое внимание сегодня привлекает автоматизация процессов комплаенса, а также объединение различных комплаенс-функций в единый системный механизм, позволяющий компании избежать угроз информационной безопасности и улучшить репутацию организации.

Литература

Алешина 2022 – *Алешина Е.И.* Корпоративный комплаенс-контроль как инструмент повышения экономической безопасности организации // Актуальные проблемы науки и техники. 2019: Материалы национальной научно-практи-

ческой конференции, Ростов-на-Дону, 26–28 марта 2019 года. Ростов-н/Д.: Донской государственный технический университет, 2019. С. 1027–1028.

Гунина, Савич, Решетов 2021 – *Гунина И.А., Савич Ю.А., Решетов В.В.* Комплаенс в системе обеспечения экономической безопасности предприятия как основа повышения конкурентоспособности // Регион: системы, экономика, управление. 2021. № 1 (52). С. 163-171. DOI: 10.22394/1997-4469-2021-52-1-163-171.

Кириллов 2021 – *Кириллов К.* Что такое LegalTech и как он развивается в России. 25.05.2021 // РБК тренды. Индустрия 4.0. URL: https://trends.rbc.ru/trends/industry/60acbdd69a79475b37ee5e63 (дата обращения 3 февраля 2023).

Кундышева, Русецкая 2019 – *Кундышева И.Р., Русецкая И.А.* Правовые аспекты использования DLP-систем в организациях // Информационная безопасность: вчера, сегодня, завтра: Сб. ст. по материалам Междунар. научно-практич. конф. Москва, 23 апреля 2019 г. М.: РГГУ, 2019. С. 175–180.

Русецкая 2022 – *Русецкая И.А.* Роль профайлинга в обеспечении информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 3. С. 85–95.

Свиридюк 2022 – *Свиридюк Ю.Г.* Безопасность и комплаенс: сходство и различие // Вестник Луганского государственного университета имени Владимира Даля. 2022. № 1(55). С. 155–163.

Стариков 2021 – *Стариков С.* Compliance Management в банке // Anti-malware. 2021. 2 июля. URL: https://www.anti-malware.ru/practice/methods/Compliance-Management-in-banks (дата обращения 3 февраля 2023).

Тарасов 2022 – *Тарасов А.* Что такое комплаенс и для чего он нужен? // DIS Group. 30.03.2022. URL: https://dis-group.ru/company-news/articles/chto-takoe-komplaens-i-dlya-chego-on-nuzhen/ (дата обращения 5 февраля 2023).

Яковлева 2022 – *Яковлева С.* Что такое комплаенс: от А до Я // Блог ROMI center, 01.07.2022. URL: https://romi.center/ru/learning/article/compliance-from-a-to-z-info/?ysclid=ldq4cp165m573404338 (дата обращения 6 февраля 2023).

References

Aleshina, E.I. (2022), “Corporate compliance control as a tool to improve the economic security of the organization”, *Current issues of science and technology 2019: Proceedings of the National Scientific and Practical Conference*, Rostov-on-Don, March 26–28, 2019, Don State Technical University, Rostov-on-Don, Russia, pp. 1027-1028.

Gunina, I.A. Savich, Yu.A. and Reshetov, V.V. (2021), “Compliance in the system of ensuring the economic security of an enterprise as a basis for increasing competitiveness”, *Region: Systems, Economics, Management*, no. 1 (52), pp. 163–171.

Kirillov, K. (2021), “What is LegalTech and how it develops in Russia”, *RBC trends. Industry 4.0,* 25 May 2021, available at: https://trends.rbc.ru/trends/industry/60acbdd69a79475b37ee5e63 (Accessed 3 February 2023).

Kundysheva, I.R. and Rusetskaya, I.A. (2019), "Legal aspects of using DLP systems in organizations", *Information security: yesterday, today, tomorrow: Sat. Art. by the Proceedings of the Materials of the International Scientific and Practical. Conf.,* Moscow, 23 April, 2019. RSUH, Moscow, Russia, pp. 175–180.

Rusetskaya, I.A. (2022), "The role of profiling in ensuring information security". *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, vol. 3, pp. 85–95.

Starikov, S. (2021), "Compliance Management in a bank", *Anti-malware,* 2 July 2021, available at: https://www.anti-malware.ru/practice/methods/Compliance-Management-in-banks (Accessed 3 February 2023).

Sviridyuk, Yu.G. (2022), "Security and compliance. Similarities and differences", *Bulletin of Vladimir Dahl Lugansk State University*, no. 1 (55), pp. 155–163.

Tarasov, A. (2022), "What is compliance and why is it needed?", *DIS Group*, 30 March 2022, available at: https://dis-group.ru/company-news/articles/chto-takoe-komplaens-i-dlya-chego-on-nuzhen/ (Accessed 5 February 2023).

Yakovleva, S. (2022), "What is compliance. From A to Z", *Blog ROMI center*, 1 July 2022, available at: https://romi.center/ru/learning/article/compliance-from-a-to-z-info/?ysclid=ldq4cp165m573404338 (Accessed 6 February 2023).

Информация об авторе

Ирина А. Русецкая, кандидат исторических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; irkom@mail.ru

Information about the author

Irina A. Rusetskaya, Cand. of Sci. (History), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; irkom@mail.ru

УДК 512
DOI: 10.28995/2686-679X-2023-2-81-101

Об инновационных методах усреднения числовых данных

Аллаберди Г. Галканов
Государственный гуманитарно-технологический университет, Орехово-Зуево, Московская область, Россия, agalkanov@yandex.ru

Аннотация. Под числовыми данными понимается любой конечный набор данных в форме чисел, векторов, функций, матриц, представляющий результаты эксперимента или натурных наблюдений. Усреднение детерминированных, случайных величин и матриц рассматривается с единой точки зрения как минимизация функции в форме обобщенной задачи наименьших квадратов. Дано новое определение среднего. Получены три обобщения средних как решения задачи минимизации. Если известными средними являются средние гармоническое, геометрическое, арифметическое и квадратическое и, быть может, еще какие-то средние, то уже первое обобщение средних дало несчетное множество средних. Из первого обобщения выведены два новых средних. Для частных видов средних, вытекающих из первого обобщения, даны их интерпретации в понятиях абсолютной и относительной отклонений (погрешностей).

Для всех средних доказано достаточное условие средности. Доказаны неравенства для шести средних. Открыт закон девяти чисел. Дано понятие о сложном среднем. Введено понятие оптимального среднего. Предложены новые определения математического ожидания и дисперсии и их обобщения. В семействе полученных математических ожиданий лишь классическое математическое ожидание оказалось линейным. Применение обобщенного математического ожидания привело к открытию двух новых распределений в теории вероятностей, а именно определены и аналитически представлены гармоническое и относительное распределения непрерывной случайной величины.

Ключевые слова: среднее чисел, среднее матриц, обобщение, среднее относительное, неравенства, оптимальное среднее, математическое ожидание, дисперсия, гармоническое распределение, относительное распределение

Для цитирования: Галканов А.Г. Об инновационных методах усреднения числовых данных // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 2. С. 81–101. DOI: 10.28995/2686-679X-2023-2-81-101

About innovative methods of numerical data averaging

Allaberdi G. Galkanov
State University of Humanities and Technology, Orekhovo-Zuevo, Moscow Region, Russia, agalkanov@yandex.ru

Abstract. Numerical data refers to any finite set of data in the form of numbers, vectors, functions, matrices representing the results of an experiment or field observations. Averaging of deterministic, random variables and matrices is considered from a single point of view as a minimization of a function in the form of a generalized least squares problem.

A new definition of the mean is given. Three generalizations of averages are obtained as solutions to the minimization problem. If the known averages are harmonic, geometric, arithmetic and quadratic averages and, perhaps, some other averages, then the first generalization of averages has already given an uncountable set of averages. Two new averages are derived from the first generalization. For particular types of averages arising from the first generalization, their interpretations are given in terms of absolute and relative deviations (errors).

A sufficient condition of the mean is proved for all averages. Inequalities for six averages are proved. The law of nine numbers has been discovered. The concept of a complex average is given. The concept of optimal mean is introduced. New definitions of mathematical expectation and variance and their generalizations are proposed. In the family of mathematical expectations obtained, only the classical mathematical expectation turned out to be linear. The application of generalized mathematical expectation has led to the discovery of two new distributions in probability theory, namely, the harmonic and relative distributions of a continuous random variable are determined and analytically presented.

Keywords: mean of numbers, mean of matrices, generalization, relative mean, inequalities, optimal mean, expectation, variance, harmonic distribution, relative distribution

For citation: Galkanov, A.G. (2023), "About innovative methods of numerical data averaging", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 81–101, DOI: 10.28995/2686-679X-2023-2-81-101

Краткий обзор средних

Как известно [Ляпин, Евсеев 1974], средним вещественных чисел $x_1, x_2,..., x_m$ $m \in \mathbf{N}$ ($m > 1$) называется число $\overline{x}$, расположенное между наименьшим и наибольшим из этих чисел. В качестве примера приведем формулы некоторых наиболее известных средних.

$$r = \frac{x_1 + x_2 + ... + x_n}{n} \text{ – среднее арифметическое;}$$

$$h = \sqrt[n]{x_1 \cdot x_2 \cdot ... \cdot x_n} \text{ – среднее геометрическое;}$$

$$g = \frac{n}{x_1^{-1} + x_2^{-1} + ... + x_n^{-1}} \text{ – среднее гармоническое;}$$

$$s = \sqrt{\frac{x_1^2 + x_2^2 + ... + x_n^2}{n}} \text{ – среднее квадратическое.}$$

Если x свои значения принимает с соответствующими весами v_1, v_2,..., v_m – где все $v_k > 0$, то вводится понятие взвешенного среднего. Так, например, взвешенное среднее арифметическое определяют в виде:

$$\overline{x} = \sum_{k=1}^{m} v_k x_k \Big/ \sum_{k=1}^{m} v_k .$$

Дальнейшее развитие теории средних пошло по пути обобщений. Так, например, было введено понятие степенного среднего $\overline{x}_c = \left(\frac{\sum_{k=1}^{m} v_k x_k^{\alpha}}{\sum_{k=1}^{m} v_k} \right)^{1/\alpha}$ ($\alpha > 0$), частным случаем которого являются некоторые известные средние, выражаемые суммой. Но средние типа среднего геометрического не могут быть получены из степенного среднего. Поэтому вводится и такое среднее $\left(\prod_{k=1}^{m} x_k^{v_k} \right)^{1/\sum_{k=1}^{m} v_k}$, частным случаем которого при $v_1 = ... = v_m = v$ является среднее геометрическое h, [Харди, Литлвуд, Полиа 1948].

В приведенном выше определении понятия среднего некоторые средние теряют смысл, при этом функциональная зависимость $\overline{x}$ от $x_1, x_2,..., x_m$ неочевидна. Так, если хотя бы одно из чисел $x_1, x_2,..., x_m$ равно нулю, то среднее гармоническое, а если нечетное количество

их отрицательно, то и среднее геометрическое этих чисел перестает существовать. Поэтому это понятие определим несколько иначе.

Новое определение среднего

Пусть x – дискретная переменная величина, принимающая конечный набор положительных действительных значений:

$$x : x_1, x_2, ..., x_m, \tag{1}$$

таких, что $x_1 = \min(x_1, x_2, ..., x_m)$, $x_m = \max(x_1, x_2, ..., x_m)$.

Определение 1. Число $\overline{x}$, удовлетворяющее условиям 1) $\overline{x} \in [x_1; x_m]$ и 2) $\overline{x}$ функционально зависит от всех $x_1, x_2, ..., x_m$, называется средним чисел (1).

Определение 1 совпадает с определением среднего в [Ляпин, Евсеев 1974], если в нем сохранить только условие 1) и отказаться от положительности чисел (1).

Пусть $S = \{s_1, s_2, ..., s_l\}$ – множество средних чисел (1), где $l \in \mathbf{N}$ ($l > 1$). Отметим два свойства средних, вытекающих из определения 1.

1^0. Среднее арифметическое средних $\dfrac{1}{l}\sum_{k=1}^{l} s_k$ есть среднее.

2^0. Среднее геометрическое средних $\left(\prod_{k=1}^{l} s_k\right)^{1/l}$ есть среднее.

Первое обобщение средних

В данной работе предложен новый подход к обобщению средних. Он основан на решении задачи на минимум в форме обобщенной задачи наименьших квадратов [Галканов 1991, Галканов 1995, Галканов 2010]. Рассмотрим функцию

$$\mu(u) = \sum_{k=1}^{m} \rho_k \left(u^\alpha - x_k^\alpha\right)^2 \to \min, u \in U = [x_1; x_m] \subset \mathbf{R}_+, \tag{2}$$

где $\rho_k = \rho(x_k)$ – весовая функция. Задача (2) – это задача усреднения чисел $x_1, x_2, ..., x_n$: требуется числа (1) аппроксимировать одним

числом u таким образом, чтобы функция $\mu(u)$ приняла наименьшее значение. Задача (2) имеет единственное решение:

$$u^+ = u^+[\alpha, \rho(x)] = \left(\frac{\sum_{k=1}^{m} \rho_k x_k^\alpha}{\sum_{k=1}^{m} \rho_k} \right)^{1/\alpha}. \qquad (3)$$

Теорема 1 (достаточное условие средности). Для того чтобы некоторое число $\overline{x}$ было средним чисел (1) в смысле определения 1, достаточно, чтобы оно было решением задачи (2).

Доказательство. Пусть $\overline{x} = u^*$. Для всех $k = \overline{1, m}$ имеем

$$x_1 \le x_k \le x_m \Leftrightarrow x_1^\alpha \le x_k^\alpha \le x_m^\alpha \Leftrightarrow x_1^\alpha \rho_k \le x_k^\alpha \rho_k \le x_m^\alpha \rho_k \Rightarrow$$

$$\Rightarrow x_1^\alpha \sum_{k=1}^{m} \rho_k \le \sum_{k=1}^{m} \rho_k x_k^\alpha \le x_m^\alpha \sum_{k=1}^{m} \rho_k \Leftrightarrow x_1^\alpha \le \frac{\sum_{k=1}^{m} \rho_k x_k^\alpha}{\sum_{k=1}^{m} \rho_k} \le x_m^\alpha \Leftrightarrow$$

$$\Leftrightarrow x_1 \le \left(\frac{\sum_{k=1}^{m} \rho_k x_k^\alpha}{\sum_{k=1}^{m} \rho_k} \right)^{1/\alpha} \le x_m \Leftrightarrow x_1 \le \overline{x} \le x_m.$$

Отметим, что широко известное степенное среднее

$$x_c = \left(\sum_{k=1}^{m} \mathrm{v}_k x_k^\alpha \Big/ \sum_{k=1}^{m} \mathrm{v}_k \right)^{1/\alpha},$$

где $\mathrm{v}_k > 0$ – вес числа x_k, является частным случаем (3): при $\rho_k = \mathrm{v}_k = const$ из (3) получаем x_c.

Так как $\alpha \in \mathbf{R}_+$, то формулой (3) определено несчетное множество средних чисел (1). Итак, формула (3) всякому набору чисел (1) ставит в соответствие семейство средних, каждое из которых приобретает явный вид при заданных α и $\rho_k = (x_k)$. Среднее (3) назовем первым обобщением средних чисел (1). В качестве примера отметим, что

1) при $\alpha = 1$ и $\rho_k = \mathrm{v}_k$ (3) есть взвешенное среднее арифметическое

$$r = \sum_{k=1}^{m} \mathrm{v}_k x_k \Big/ \sum_{k=1}^{m} \mathrm{v}_k;$$

2) при $\alpha = 1$ и $\rho_k = \dfrac{\mathrm{v}_k}{x_k}$ (3) есть взвешенное среднее гармоническое

$$g = \sum_{k=1}^{m} \mathrm{v}_k \Big/ \sum_{k=1}^{m} \frac{\mathrm{v}_k}{x_k};$$

3) при $\alpha = 2$ и $\rho_k = \mathrm{v}_k$ (3) есть взвешенное среднее квадратическое

$$q = \left(\sum_{k=1}^{m} \mathrm{v}_k x_k^2 \Big/ \sum_{k=1}^{m} \mathrm{v}_k \right)^{1/2}.$$

Также отметим два новых средних, получаемых из (3):

4) при $\alpha = 1, \rho_k = \dfrac{\mathrm{v}_k}{x_k^2}$ из (5) имеем среднее $\tau = \sum_{k=1}^{m} \frac{\mathrm{v}_k}{x_k} \Big/ \sum_{k=1}^{m} \frac{\mathrm{v}_k}{x_k^2}$, которое автором названо взвешенным средним относительным (пояснение будет дано позже);

5) при $\alpha = 1/2, \rho_k = \mathrm{v}_k$ из (5) имеем среднее $\nu = \left(\sum_{k=1}^{m} \mathrm{v}_k \sqrt{x_k} \Big/ \sum_{k=1}^{m} \mathrm{v}_k \right)^2$, которое автором названо квадратом взвешенного среднего арифметического квадратных корней, так как $\dfrac{\sum_{k=1}^{m} \mathrm{v}_k \sqrt{x_k}}{\sum_{k=1}^{m} \mathrm{v}_k}$ есть взвешенное среднее арифметическое квадратных корней.

Некоторые средние, получаемые из (3), могут быть интерпретированы с точки зрения минимальности отклонений при помощи функции (2). Так, например,

$$\mu(u)\big|_{u=r} = \mu(r) = \min \sum_{k=1}^{m} (u - x_k)^2 = \min \sum_{k=1}^{m} |u - x_k|^2 -$$

среднее арифметическое r минимизирует сумму квадратов абсолютных отклонений (или погрешностей) $|u - x_k|^2$;

$$\mu(u)\big|_{u=g} = \mu(g) = \min \sum_{k=1}^{m} \frac{(u - x_k)^2}{x_k} = \min \sum_{k=1}^{m} |u - x_k| \frac{|u - x_k|}{x_k} -$$

среднее гармоническое g минимизирует сумму произведений абсолютных отклонений $|u - x_k|$ на относительные отклонения $\dfrac{|u - x_k|}{x_k}$;

$$\mu(u)\big|_{u=\tau} = \mu(\tau) = \min \sum_{k=1}^{m} \left(\frac{u - x_k}{x_k} \right)^2 = \min \sum_{k=1}^{m} \left(\frac{|u - x_k|}{x_k} \right)^2 -$$

среднее относительное τ минимизирует сумму квадратов относительных отклонений $\frac{|u-x_k|}{x_k}$, откуда следует обоснованность данного названия.

Неравенства для средних

Теорема 2. Если τ, g, h, v, r, q – среднее относительное, гармоническое, геометрическое, квадрат среднего арифметического квадратных корней, арифметическое и квадратическое соответственно, то $\tau \leqslant g \leqslant h \leqslant v \leqslant r \leqslant q$, где равенства имеют место лишь при $x_1 = x_2 = ... = x_n$.

Отметим, что вывод неравенств $g \leqslant h \leqslant r \leqslant q$ известен (см., [1]). Поэтому теорему 2 достаточно доказать для неравенств $\tau \leqslant g$, $h \leqslant v$ и $v \leqslant r$.

Доказательство.

1) $\tau \leqslant g$. Полагая $\alpha_k = 1/x_k$, $\beta_k = 1$, из неравенства Коши

$$\left(\sum_{k=1}^{m}\alpha_k\beta_k\right)^2 \leq \sum_{k=1}^{m}\alpha_k^2\sum_{k=1}^{m}\beta_k^2$$

получаем

$$\left(\sum_{k=1}^{m}\frac{1}{x_k}\right)^2 \leq m\sum_{k=1}^{m}\frac{1}{x_k^2} \Leftrightarrow \left(\sum_{k=1}^{m}\frac{1}{x_k}\right)\left(\sum_{k=1}^{m}\frac{1}{x_k}\right) \leq m\sum_{k=1}^{m}\frac{1}{x_k^2} \Leftrightarrow \frac{\sum\limits_{k=1}^{m}\frac{1}{x_k}}{\sum\limits_{k=1}^{m}\frac{1}{x_k^2}} \leq \frac{m}{\sum\limits_{k=1}^{m}\frac{1}{x_k}} \Leftrightarrow \tau \leq g.$$

2) $h \leqslant v$. Используя известное неравенство между средним геометрическим и арифметическим $h \leqslant r$ для чисел $\sqrt{x_1}, \sqrt{x_2}, ..., \sqrt{x_m}$ имеем

$$\left(x_1^{1/2}\cdot x_2^{1/2}\cdot ...\cdot x_m^{1/2}\right)^{1/m} \leq \frac{\sqrt{x_1}+\sqrt{x_2}+...+\sqrt{x_m}}{m} \Leftrightarrow$$

$$\Leftrightarrow \left(x_1^{1/m}\cdot x_2^{1/m}\cdot ...\cdot x_m^{1/m}\right)^{1/2} \leq \frac{\sqrt{x_1}+\sqrt{x_2}+...+\sqrt{x_m}}{m} \Leftrightarrow$$

$$\Leftrightarrow x_1^{1/m}\cdot x_2^{1/m}\cdot ...\cdot x_m^{1/m} \leq \left(\frac{\sqrt{x_1}+\sqrt{x_2}+...+\sqrt{x_m}}{m}\right)^2 \Leftrightarrow$$

$$\Leftrightarrow \left(x_1\cdot x_2\cdot ...\cdot x_m\right)^{1/m} \leq \left(\frac{\sqrt{x_1}+\sqrt{x_2}+...+\sqrt{x_m}}{m}\right)^2 \Leftrightarrow h \leq v.$$

3) $v \leqslant r$. Полагая $\alpha_k = x_k^{1/2}$, $\beta_k = 1$, опять же, из неравенства Коши будем иметь

$$\left(\sum_{k=1}^{m}\alpha_k\beta_k\right)^2 \leq \sum_{k=1}^{m}\alpha_k^2\sum_{k=1}^{m}\beta_k^2 \Leftrightarrow \left(\sum_{k=1}^{m}x_k^{1/2}\right)^2 \leq m\sum_{k=1}^{m}x_k \Leftrightarrow \left(\frac{1}{m}\sum_{k=1}^{m}x_k^{1/2}\right)^2 \leq \frac{1}{m}\sum_{k=1}^{m}x_k \Leftrightarrow v \leq r.$$

Из неравенств $g \leqslant h \leqslant r \leqslant q$ и $\tau \leqslant g, h \leqslant v, v \leqslant r$ следуют доказываемые неравенства.

Оценка среднего относительного

Теорема 3. Если τ – среднее относительное чисел (1), то

$$1 \leq \frac{\tau}{x_1} \leq \frac{1+\sqrt{m}}{2}.$$

Доказательство. Исходя из определения среднего относительного, имеем

$$\tau = \frac{\sum_{k=1}^{m}\frac{1}{x_k}}{\sum_{k=1}^{m}\frac{1}{x_k^2}} \Leftrightarrow \tau = \frac{\frac{1}{x_1}}{\frac{1}{x_1^2}} \cdot \frac{1+\frac{x_1}{x_2}+\ldots+\frac{x_1}{x_m}}{1+\frac{x_1^2}{x_2^2}+\ldots+\frac{x_1^2}{x_m^2}} \Leftrightarrow$$

$$\Leftrightarrow \frac{\tau}{x_1} = \frac{1+\frac{x_1}{x_2}+\ldots+\frac{x_1}{x_m}}{1+\frac{x_1^2}{x_2^2}+\ldots+\frac{x_1^2}{x_m^2}} \Leftrightarrow \frac{\tau}{x_1} = \frac{1+t_2+\ldots+t_m}{1+t_2^2+\ldots+t_m^2} \Leftrightarrow$$

$$\Leftrightarrow \frac{\tau}{x_1} = f(t_2,\ldots,t_m),\ t_k = \frac{x_1}{x_k} > 0,\ k = \overline{2,m},\ f = \frac{1+t_2+\ldots+t_m}{1+t_2^2+\ldots+t_m^2}.$$

Функцию $f(t_2,\ldots,t_m)$ исследуем на экстремум.

$$\begin{cases}\dfrac{\partial f}{\partial t_k} = 0,\\ k = \overline{2,m}\end{cases} \Leftrightarrow \begin{cases}1+t_2^2+\ldots+t_m^2-2t_k\left(1+t_2+\ldots+t_m\right)=0,\\ k=\overline{2,m}\end{cases} \Rightarrow$$

$$\Rightarrow \forall k \in \{2,\ldots,m\}\left[t_k = \frac{1+t_2^2+\ldots+t_m^2}{2\left(1+t_2+\ldots+t_m\right)}\right] \Rightarrow t_2 = \ldots = t_m.$$

Пусть $t_2 = ... = t_m = t$. Тогда $f(t_2,..., t_m) = f(t) = \dfrac{1+(m-1)t}{1+(m-1)t^2}$ и

$$f'(t) = 0 \Leftrightarrow \frac{(m-1)\left[1+(m-1)t^2\right]-2(m-1)t\left[1+(m-1)t\right]}{1+(m-1)t^2} = 0 \Leftrightarrow$$

$$\Leftrightarrow (m-1)\frac{1-2t-(m-1)t^2}{1+(m-1)t^2} = 0 \Leftrightarrow t_{1,2} = \frac{-1\pm\sqrt{m}}{m-1} \overset{t>0}{\Rightarrow} t = t^* = \frac{1}{1+\sqrt{m}}.$$

Так как $f''(t^*) < 0$, то $\max f(t) = f(t^*) = \dfrac{1+(m-1)\dfrac{1}{1+\sqrt{m}}}{1+(m-1)\dfrac{1}{\left(1+\sqrt{m}\right)^2}} = \dfrac{1+\sqrt{m}}{2}$.

Из неравенств $1 \le \dfrac{\tau}{x_1}$ и $\dfrac{\tau}{x_1} \le \dfrac{1+\sqrt{m}}{2}$ следуют доказываемые неравенства.

Следствие из теоремы 3. $\forall k = \overline{1,m}\left[\dfrac{\tau}{x_k} \le \dfrac{1+\sqrt{m}}{2}\right]$.

Доказательство. Повторить проведенное выше исследование функции $f(t_2,..., t_m)$ на экстремум для отношения $\dfrac{\tau}{x_k}$.

Закон девяти чисел

Теорема 4 (закон девяти чисел). Для любого распределения положительных действительных чисел x_1, x_2,..., x_9 относительное отклонение каждого из них от их среднего относительного не превосходит 1: $\forall k \in \{1, 2,..., 9\}\left[\dfrac{|\tau - x_k|}{x_k} \le 1\right]$.

Доказательство. При $m = 9$ из следствия 3 имеем

$$\forall k \in \{1, 2,..., 9\}\left[\frac{\tau}{x_k} \le 2\right] \Leftrightarrow \forall k \in \{1, 2,..., 9\}\left[\tau - x_k \le x_k\right]. \qquad (4)$$

Далее от противоположного. Предположим, что

$$\exists k \in \{1, 2,..., 9\}\left[\frac{|\tau - x_k|}{x_k} > 1\right] \Leftrightarrow \exists k \in \{1, 2,..., 9\}\left[|\tau - x_k| > x_k\right].$$

Пусть $\tau - x_k \geqslant 0$. Тогда $\exists k \in \{1, 2,..., 9\}$ $[\tau - x_k > x_k]$. Однако это противоречит (4). Пусть теперь $\tau - x_k < 0$. Тогда $\exists k \in \{1, 2,..., 9\}$ $[x_k - \tau > x_k] \Leftrightarrow \exists k \in \{1, 2,..., 9\}$ $[\tau < 0]$, что невозможно.

Понятие сложного среднего

Пусть $S = \{s_1, s_2,..., s_l\}$ – множество средних чисел (1). И пусть s – некоторое среднее чисел (1).

Определение 3. Функция $f : S \to s$ называется сложным средним для чисел (1).

Примеры.

$$1)\ f(r,h,q) = \frac{r \cdot h^2}{q^2} = \frac{x_1 + x_2}{2} \cdot x_1 x_2 \cdot \frac{1}{\frac{x_1^2 + x_2^2}{2}} = \frac{x_1 x_2 (x_1 + x_2)}{x_1^2 + x_2^2} = \frac{\frac{1}{x_1} + \frac{1}{x_2}}{\frac{1}{x_1^2} + \frac{1}{x_2^2}} = \tau,$$

т. е. произведение среднего арифметического на квадрат среднего геометрического двух чисел x_1, x_2, деленное на квадрат среднего квадратического этих чисел, есть среднее относительное x_1, x_2.

$$2)\ f(r,h) = \frac{r+h}{2} = \frac{1}{2}\left(\frac{x_1 + x_2}{2} + \sqrt{x_1 x_2}\right) = \frac{x_1 + 2\sqrt{x_1}\sqrt{x_2} + x_2}{4} = \left(\frac{\sqrt{x_1} + \sqrt{x_2}}{2}\right)^2 = \nu,$$

т. е. для двух чисел x_1, x_2 среднее арифметическое их среднего арифметического и среднего геометрического равно квадрату среднего арифметического квадратных корней этих чисел.

$$3)\ f\left[g(x_1, x_2,..., x_n),\ g\left(x_1^2, x_2^2,..., x_n^2\right)\right] = \frac{g\left(x_1^2, x_2^2,..., x_n^2\right)}{g(x_1, x_2,..., x_n)} = \frac{\sum\limits_{k=1}^{m} \nu_k}{\sum\limits_{k=1}^{m} \frac{\nu_k}{x_k^2}} \cdot \frac{1}{\frac{\sum\limits_{k=1}^{m} \nu_k}{\sum\limits_{k=1}^{m} \frac{\nu_k}{x_k}}} = \frac{\sum\limits_{k=1}^{m} \frac{\nu_k}{x_k}}{\sum\limits_{k=1}^{m} \frac{\nu_k}{x_k^2}} = \tau,$$

т. е. частное взвешенного среднего гармонического квадратов чисел (1) к взвешенному среднему гармоническому самих чисел (1) равно взвешенному среднему относительному этих чисел.

Понятие оптимального среднего

Существование множества средних для одного и того же набора чисел (1) естественно приводит к понятию об оптимальном среднем. Пусть $S = \{s_1, s_2,..., s_l\}$ – конечное множество средних, $l \in \mathbf{N}$ ($l > 1$). В частности, $S = \{\tau, g, h, v, r, q\}$. Через $\delta_k(s_j) = \dfrac{|s_j - x_k|}{x_k}$ ($k = \overline{1, m}; j = \overline{1, l}$) обозначим относительное отклонение среднего s_j от точки x_k и положим $\delta(s_j) = \max\limits_k \delta_k(s_j)$.

Определение 4. Наименьшее из отклонений $\delta(s_1)$, $\delta(s_2)$,..., $\delta(s_l)$, т. е.

$$s = \min[\delta(s_1), \delta(s_2),..., \delta(s_l)], \tag{5}$$

называется оптимальным средним на множестве средних S.

Второе обобщение средних

Пусть $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$ – детерминированная матрица, такая, что $\forall i \in I\ \forall j \in J[a_{ij} > 0]$, $I = \{1,..., m\}$, $J = \{1,..., n\}$. Введем понятие среднего матрицы A. Пусть $a_1 = \min\limits_{i \in I,\ j \in J} a_{ij}$, $a_2 = \max\limits_{i \in I,\ j \in J} a_{ij}$.

Определение 5. Число a_A, удовлетворяющее условиям 1) $a_A \in [a_1; a_2]$ и 2) a_A, функционально зависит от всех элементов матрицы A, называется средним этой матрицы.

Рассмотрим задачу усреднения матрицы A как задачу на минимум:

$$\mu(u) = \sum_{i=1}^{m}\sum_{j=1}^{n} \rho_{ij}\left(u^\alpha - a_{ij}^\alpha\right)^2 \to \min,\ u \in U = [a_1; a_2], \tag{6}$$

где $\rho_{ij} = \rho(a_{ij})$. Задача (6) имеет единственное решение

$$u_2^* = \left(\frac{\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n} \rho_{ij} a_{ij}^\alpha}{\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n} \rho_{ij}} \right)^{1/\alpha}. \tag{7}$$

Теорема 5 (второе достаточное условие средности). Для того чтобы некоторое число u было средним матрицы A в смысле определения 5, достаточно, чтобы оно было решением задачи (6).

Доказательство. Пусть $u = u_2^*$. Имеем

$$\forall i \in I\ \forall j \in J\left[a_1 \le a_{ij} \le a_2\right] \Leftrightarrow \forall i \in I\ \forall j \in J\left[a_1^\alpha \le a_{ij}^\alpha \le a_2^\alpha\right] \Leftrightarrow$$

$$\Leftrightarrow \forall i \in I\ \forall j \in J\left[a_1^\alpha \rho_{ij} \le \rho_{ij} a_{ij}^\alpha \le a_2^\alpha \rho_{ij}\right] \Rightarrow$$

$$\Rightarrow a_1^\alpha \sum_{i=1}^{m}\sum_{j=1}^{n}\rho_{ij} \le \sum_{i=1}^{m}\sum_{j=1}^{n}\rho_{ij} a_{ij}^\alpha \le a_2^\alpha \sum_{i=1}^{m}\sum_{j=1}^{n}\rho_{ij} \Leftrightarrow$$

$$\Leftrightarrow a_1^\alpha \le \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\rho_{ij} a_{ij}^\alpha}{\sum_{i=1}^{m}\sum_{j=1}^{n}\rho_{ij}} \le a_2^\alpha \Leftrightarrow a_1 \le u_2^* \le a_2.$$

Хотя (7) названо обобщенным средним, из него можно получать лишь те средние, которые выражаются в виде сумм. Так, например, среднее геометрическое $h_A = \prod_{i=1}^{m}\left(\prod_{j=1}^{n} a_{ij}\right)^{1/mn}$ матрицы A не вписывается в структуру (7). С целью получения формулы более высокого порядка обобщения перейдем к третьему обобщению.

Третье обобщение средних

Для всех элементов матрицы рассмотрим задачу на минимум:

$$\mu(u) = \sum_{i=1}^{m}\left\{\sum_{j=1}^{n}\rho_{ij}\left[u^\alpha - \left(\prod_{j=1}^{n} a_{ij}\right)^{\alpha/n}\right]\right\}^2 \to \min,\ u\ \ U = [a_1; a_2], \qquad (8)$$

где $\rho_{ij} = \rho(a_{ij})$. Существует единственное решение задачи (8)

$$u_3^* = \left\{\frac{\sum_{i=1}^{m}\left[\left(\sum_{j=1}^{n}\rho_{ij}\right)\left(\prod_{j=1}^{n} a_{ij}\right)^{\alpha/n}\right]}{\sum_{i=1}^{m}\sum_{j=1}^{n}\rho_{ij}}\right\}^{1/\alpha}. \qquad (9)$$

Теорема 6 (третье достаточное условие средности). Для того чтобы некоторое число u было средним матрицы A в смысле определения 5, достаточно, чтобы оно было решением задачи (8).

Доказательство. Пусть $u = u_3^*$. Имеем

$$\forall i \in I\ \forall j \in J\left[a_1 \le a_{ij} \le a_2\right] \Leftrightarrow \forall i \in I\ \forall j \in J\left[a_1^\alpha \le a_{ij}^\alpha \le a_2^\alpha\right] \Rightarrow$$

$$\Rightarrow \forall i \in I\left[a_1^{\alpha\cdot n} \le \left(\prod_{j=1}^{n} a_{ij}^\alpha\right)^n \le a_2^{\alpha\cdot n}\right] \Leftrightarrow \forall i \in I\left[a_1^\alpha \le \left(\prod_{j=1}^{n} a_{ij}^\alpha\right)^{1/n} \le a_2^\alpha\right] \Leftrightarrow$$

$$\Leftrightarrow \forall i \in I\left[a_1^\alpha \le \left(\prod_{j=1}^{n} a_{ij}\right)^{\alpha/n} \le a_2^\alpha\right] \Leftrightarrow \forall i \in I\left[a_1^\alpha \rho_{ij} \le \rho_{ij}\left(\prod_{j=1}^{n} a_{ij}^{1/n}\right)^\alpha \le a_2^\alpha \rho_{ij}\right] \Rightarrow$$

$$\Rightarrow a_1^\alpha \sum_{j=1}^{n} \rho_{ij} \le \left(\sum_{j=1}^{n} \rho_{ij}\right)\left(\prod_{j=1}^{n} a_{ij}\right)^{\alpha/n} \le a_2^\alpha \sum_{j=1}^{n} \rho_{ij} \Rightarrow$$

$$\Rightarrow a_1^\alpha \sum_{i=1}^{m}\sum_{j=1}^{n} \rho_{ij} \le \sum_{i=1}^{m}\left[\left(\sum_{j=1}^{n} \rho_{ij}\right)\left(\prod_{j=1}^{n} a_{ij}\right)^{\alpha/n}\right] \le a_2^\alpha \sum_{i=1}^{m}\sum_{j=1}^{n} \rho_{ij} \Leftrightarrow$$

$$\Leftrightarrow a_1^\alpha \le \frac{\sum_{i=1}^{m}\left[\left(\sum_{j=1}^{n} \rho_{ij}\right)\left(\prod_{j=1}^{n} a_{ij}\right)^{\alpha/n}\right]}{\sum_{i=1}^{m}\sum_{j=1}^{n} \rho_{ij}} \le a_2^\alpha \Leftrightarrow$$

$$\Leftrightarrow a_1 \le \left\{\frac{\sum_{i=1}^{m}\left[\left(\sum_{j=1}^{n} \rho_{ij}\right)\left(\prod_{j=1}^{n} a_{ij}\right)^{\alpha/n}\right]}{\sum_{i=1}^{m}\sum_{j=1}^{n} \rho_{ij}}\right\}^{1/\alpha} \le a_2 \Leftrightarrow a_1 \le u_3^* \le a_2.$$

Рассмотрим частные случаи (9).

Случай 1. Пусть $n = 1$. Из (9) получим $u_3^* = \left\{ \dfrac{\sum_{i=1}^{m} \rho_i a_i^{\alpha}}{\sum_{i=1}^{m} \rho_i} \right\}^{1/\alpha} = u_1^*$, что есть первое обобщение среднего, где $\rho_i = \rho_{i1}$, $a_i = a_{i1}$.

Случай 2. Пусть $\rho_{ij} = 1$, $m = 1$, $\alpha = n$, $a_j = a_{1j}$. Из (9) получим $h = [a_1 \cdot a_2 \cdot ... \cdot a_n]^{1/n}$, что есть среднее геометрическое n чисел $a_1, a_2, ..., a_n$.

Случай 3. Пусть $\alpha = n$. Из (9) получим

$$u_3^* = \left\{ \frac{\sum_{i=1}^{m} \left[\left(\sum_{j=1}^{n} \rho_{ij} \right) \left(\prod_{j=1}^{n} a_{ij} \right) \right]}{\sum_{i=1}^{m} \sum_{j=1}^{n} \rho_{ij}} \right\}^{1/n}. \qquad (10)$$

Случай 4. Пусть $\rho_{ij} = \mathrm{v}_{ij} = const$. Из (10) получим

$$u_3^* = \left\{ \frac{\sum_{i=1}^{m} \left[\left(\sum_{j=1}^{n} \mathrm{v}_{ij} \right) \left(\prod_{j=1}^{n} a_{ij} \right) \right]}{\sum_{i=1}^{m} \sum_{j=1}^{n} \mathrm{v}_{ij}} \right\}^{1/n}. \qquad (11)$$

В частности, когда $m = 1$, из (11) получаем $u_3^* = h = [a_1 \cdot a_2 \cdot ... \cdot a_n]^{1/n}$. Поэтому среднее, определяемое формулой (11), естественно назвать взвешенным средним геометрическим mn чисел $a_{11}, a_{12}, ..., a_{mn}$ матрицы A.

Таким образом, третье обобщение (9) является наиболее общим, включающим в себя как средние в форме сумм, так и средние в форме произведений. В частности, взвешенные средние арифметическое и геометрическое – частные случаи (9).

Что касается известного среднего геометрического с весом $\left(\prod_{k=1}^{m} x_k^{\mathrm{v}_k} \right)^{1/\sum_{k=1}^{m} \mathrm{v}_k}$, то очевидно, что оно имеет совершенно иную структуру, чем (11). Это среднее есть результат формального обобщения или существует его осмысленный вывод, автору неизвестно.

Усреднение дискретной случайной величины. Новые определения математического ожидания и дисперсии

Рассмотрим закон распределения дискретной случайной величины

$$\begin{array}{cc} x & x_1, x_2, ..., x_m \\ \mathrm{P} & p_1, p_2, ..., p_m, \end{array}$$

где $p_i = \mathbf{P}(x = x_i)$ – вероятность того, что случайная величина x примет значение x_i, $x_i > 0$, $i \in I$. Приведем классические определения числовых характеристик дискретной случайной величины:

$$M(x) = \sum_{i=1}^{m} x_i p_i, \; D(x) = M\left[x - M(x)\right]^2.$$

Отметим два недостатка этих определений:

1) ориентированность на среднего арифметического;

2) закрытость к обобщению.

Ориентированность на среднего арифметического означает, что в определенном смысле математическое ожидание $M(x)$ в самом деле является средним арифметическим значений x_1, x_2,..., x_m случайной величины x. Действительно, используя классическое определение вероятности, имеем

$$\overline{x} = \frac{\mathrm{v}_1 x_1 + \mathrm{v}_2 x_2 + ... + \mathrm{v}_m x_m}{\mathrm{v}} = \frac{\mathrm{v}_1}{\mathrm{v}} x_1 + \frac{\mathrm{v}_2}{\mathrm{v}} x_2 + ... + \frac{\mathrm{v}_m}{\mathrm{v}} x_m = \sum_{i=1}^{m} x_i p_i.$$

Непосредственным следствием 1) является 2). Имея желание обобщить, дадим новое определение $M(x)$ и $D(x)$. Пусть $\overline{x}$ – некоторое среднее значение случайной величины x. Тогда модуль отклонения $\varepsilon_i = |\overline{x} - x_i|$ есть случайная величина. Составим сумму квадратов

$$\mu(u) = \sum_{k=1}^{m} p_k \left(u - x_k\right)^2 \to \min, u \in U = [x_1; x_m] \subset \mathbf{R}_+. \qquad (12)$$

Определение 6. Точка минимума функции (12) называется математическим ожиданием, а минимум функции (12) – дисперсией дискретной случайной величины x.

Задача (12) имеет единственное решение: $\overline{x} = \sum_{i=1}^{m} x_i p_i = M(x)$, при этом $\min \mu(u) = \mu(\overline{x}) = D(x)$.

Обобщение математического ожидания и дисперсии дискретной случайной величины

Вместо функции (12) рассмотрим другую функцию

$$\mu(u)=\sum_{k=1}^{m}\rho_k p_k\left(u^{\alpha}-x_k^{\alpha}\right)^2\to\min,\ \rho_k=\rho(x_k),\ u\in U=[x_1;x_m]\subset\mathbf{R}_+. \quad (13)$$

Определение 7. Точка минимума функции (13) называется обобщенным математическим ожиданием, а минимум функции (13) – обобщенной дисперсией дискретной случайной величины x.

Задача (13) имеет единственное решение:

$$\bar{x}=M\left(x,\alpha,\rho\right)=\left(\sum_{i=1}^{m}\rho_i p_i x_i^{\alpha}\Big/\sum_{i=1}^{m}\rho_i p_i\right)^{1/\alpha},$$

при этом $\min\mu(u)=\mu(x)=D(x,\alpha,\rho)=\sum_{i=1}^{n}\rho_i p_i\left[M^{\alpha}\left(x,\alpha,\rho\right)-x_i^{\alpha}\right]^2$.
В частности,

$$M_r=M\left(x,1,1\right)=\sum_{i=1}^{m}x_i p_i,\ M_g=M\left(x,1,\frac{1}{x}\right)=\frac{1}{\sum\limits_{i=1}^{m}\frac{p_i}{x_i}},\ M_\tau=M\left(x,1,\frac{1}{x^2}\right)=\frac{\sum\limits_{i=1}^{m}\frac{p_i}{x_i}}{\sum\limits_{i=1}^{m}\frac{p_i}{x_i^2}}.$$

В обозначениях M_r, M_g, M_τ индексы r, g, τ инициированы средними арифметическим, гармоническим и относительным.

Обобщение математического ожидания и дисперсии непрерывной случайной величины

Пусть $x\in[a;b]=U, b>a>0$ – непрерывная случайная величина с функцией распределения $F(x)$ и плотностью распределения $f(x)$. Рассмотрим задачу на минимум:

$$\mu(u)=\int_a^b\rho(x)f(x)\left(u^{\alpha}-x^{\alpha}\right)^2dx\ \to\ u\in U. \quad (14)$$

Определение 8. Точка минимума функции (14) называется обобщенным математическим ожиданием, а минимум этой функции – обобщенной дисперсией непрерывной случайной величины x.

Итак, по определению обобщенным математическим ожиданием и обобщенной дисперсией непрерывной случайной величины x являются

$$M(x,\alpha,\rho)=\left(\frac{\int_a^b t^{\alpha}\rho(t)f(t)dt}{\int_a^b \rho(t)f(t)dt}\right)^{1/\alpha},\quad D(x,\alpha,\rho)=\int_a^b \rho(t)f(t)\left[M^{\alpha}(t,\alpha,\rho)-t^{\alpha}\right]^2 dt$$

соответственно. В частности,

1) если $\alpha = 1, \rho_i = 1$, то

$$M(x,1,1)=M_r(x)=\frac{\int_a^b t\,f(t)dt}{\int_a^b f(t)dt},\ D(x,1,1)=D_r(x)=\int_a^b f(t)\left[M(t)-t\right]^2 dt;$$

2) если $\alpha = 1,\ \rho=\frac{1}{x}$, то

$$M\left(x,1,\frac{1}{x}\right)=M_g(x)=\frac{\int_a^b f(t)dt}{\int_a^b \frac{f(t)}{t}dt};\ D(x,1,1)=D_g(x)=\int_a^b \frac{f(t)}{t}\left[M(t)-t\right]^2 dt;$$

3) если же $\alpha = 1,\ \rho=\frac{1}{x^2}$, то

$$M\left(x,1,\frac{1}{x^2}\right)=M_{\tau}(x)=\frac{\int_a^b \frac{f(t)}{t}dt}{\int_a^b \frac{f(t)}{t^2}dt},\ D(x,\alpha,\rho)=D_{\tau}(x)=\int_a^b \frac{f(t)}{t^2}\left[M_{\tau}(t)-t\right]^2 dt.$$

В п. 12 предполагается, что определенные интегралы Римана существуют. Но на условиях их существования не будем останавливаться, так как их без труда можно перечислить.

Гармоническое и относительное распределения непрерывной случайной величины

Применение обобщенного математического ожидания привело к открытию двух новых распределений.

Определение 9. Распределение вероятностей непрерывной случайной величины x называется гармоническим, если

$$f(x)=\begin{cases}0 & \text{при } x\notin U,\\ \dfrac{1}{x\ln(b/a)} & \text{при } x\in U.\end{cases}$$

При этом $M\left(x,1,\dfrac{1}{x}\right)=\dfrac{ab}{b-a}\ln\dfrac{b}{a}$ и $F(x)=\begin{cases}0 & \text{при } x\notin U,\\ \dfrac{\ln\frac{x}{a}}{\ln\frac{a}{b}} & \text{при } x\in[a;x].\end{cases}$

Определение 10. Распределение вероятностей непрерывной случайной величины x называется относительным, если

$$f(x)=\begin{cases}0 & \text{при } x\notin U,\\ \dfrac{ab}{b-a}\cdot\dfrac{1}{x^2} & \text{при } x\in U.\end{cases}$$

При этом

$$M\left(x,1,\frac{1}{x^2}\right)=\frac{3}{2}\cdot\frac{ab(a+b)}{a^2+ab+b^2},\ F(x)=\begin{cases}0 & \text{при } x\notin U,\\ \dfrac{1-\frac{a}{x}}{1-\frac{a}{b}} & \text{при } x\in[a;x].\end{cases}$$

Обобщенные числовые характеристики случайной матрицы

Рассмотрим случайную матрицу $A=\|x_{ij}\|, \forall i\in I\,\forall j\in J\left[x_{ij}>0\right]$, где $I=\{1,...,m\}, J=\{1,...,n\}$. Пусть p_{ij} – вероятность того, что случайный элемент x_{ij} матрицы A примет значение $a_{ij}: p_{ij}=p(x_{i,j}=a_{ij})$. Рассмотрим задачу

$$\mu(u) = \sum_{i=1}^{m}\sum_{j=1}^{n} p_{ij}\rho_{ij}\left(u^{\alpha} - a_{ij}^{\alpha}\right)^2 \to \min,\ u \in U = [a_1; a_2] \qquad (15)$$

где $\rho_{ij} = \rho(a_{ij})$, $a_1 = \min\limits_{i\in I,\ j\in J}\left(a_{ij}\right)$, $a_2 = \max\limits_{i\in I,\ j\in J}\left(a_{ij}\right)$.

Определение 11. Точка минимума функции (15) называется обобщенным математическим ожиданием, а минимум этой функции – обобщенной дисперсией случайной матрицы A.

Итак, согласно определению 11, $M(A, \alpha, \rho) = \left(\dfrac{\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n} p_{ij}\rho_{ij}a_{ij}^{\alpha}}{\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n} p_{ij}\rho_{ij}}\right)^{1/\alpha}$ – обобщенное математическое ожидание случайной матрицы A;

$\mu(u^*) = D(A, \alpha, \rho) = \sum\limits_{i=1}^{n} \rho_i p_i \left[M^{\alpha}(x, \alpha, \rho) - a_{ij}^{\alpha}\right]^2$ – обобщенная дисперсия случайной матрицы A.

По аналогии с (5) для конечного множества математических ожиданий можно ввести понятие оптимального математического ожидания.

Заключение

1. Дано новое определение среднего для конечного набора положительных действительных чисел.
2. Даны три обобщения среднего, причем не как формальное обобщение, а как решение задачи в форме наименьших квадратов. Третье обобщение является наиболее общим и включает в себя средние как в виде сумм, так и в виде произведений.
3. Некоторым средним даны интерпретации через минимум погрешностей.
4. Введено понятие оптимального среднего.
5. Даны новые определения и обобщения математического ожидания и дисперсии.
6. Даны определения среднего детерминированной матрицы и числовых характеристик матрицы со случайными элементами.
7. Определены гармоническое и относительное распределения непрерывной случайной величины.

Обозначения

$\mathbf{N}$, $\mathbf{R}_+$ – множества натуральных и положительных вещественных чисел.

Литература

Галканов 1991 – *Галканов А.Г.* Принцип минимума в теории средних // Известия АН ТССР, серия физико-математических, технических, химических и геологических наук. 1991. № 3. С. 99–100.

Галканов 1995 – *Галканов А.Г.* О некоторых результатах применения модифицированных методов наименьших квадратов к задачам восстановления эмпирических функций // Тезисы докладов конференции с Международным участием «Математические методы распознавания образов», посвященной 60-летию академика Ю.И. Журавлёва, 25–30 сентября, Пущино, 1995. М., 1995. С. 85.

Галканов 2010 – *Галканов А.Г.* Обобщенный принцип наименьших квадратов и новые методы математической обработки опытных данных // G-Global, Japan Science and Technology Agency. 2010. 06月11日.

Ляпин, Евсеев 1974 – *Ляпин Е.С., Евсеев А.С.* Алгебра и теория чисел. Ч. 1. М.: Просвещение, 1974.

Харди, Литлвуд, Полиа 1948 – *Харди Г.Г., Литлвуд Дж.Е., Полиа Г.* Неравенства / Пер. с англ. В.И. Левина. М.: Государственное издательство иностранной литературы, 1948.

References

Galkanov, A.G. (1991), “The minimum principle in the theory of averages”, *Izvestiya AN TSSR, seriya fiziko-matematicheskikh, tekhnicheskikh, khimicheskikh i geologicheskikh nauk, Series*, no. 3, pp. 99–100.

Galkanov, A.G. (1995), “On some results of the application of modified least squares methods to the problems of restoring empirical functions”, *Matematicheskie metody raspoznavaniya obrazov. Tezisy dokladov s Mezhdunarodnym uchastiem, posvyashchennoi 60-letiyu akademika RAN Yu.I. Zhuravleva* [Abstracts of the conference with international participation “Mathematical Methods of Pattern Recognition”, dedicated to the 60th anniversary of Academician Yu.I. Zhuravlev], September 25–30, Pushchino, 1995, Moscow, Russia, p. 85.

Galkanov, A.G. (2010), “The generalized principle of least squares and new methods of mathematical processing of experimental data”, *G-Global, Japan Science and Technology Agency*, 年06月11日.

Khardi G.G., Litlvud, Dzh.E. and Polia, G. (1948), *Neravenstva* [Inequalities], Levina, V.I. (transl. from Engl.), Gosudarstvennoe izdatel'stvo inostrannoi literatury, Moscow, Russia.

Lyapin, E.S. and Evseev, A.S. (1974), *Algebra i teoriya chisel. Ch. 1.* [Algebra and number theory, part 1], Prosveshchenie, Moscow, Russia.

Информация об авторе

Аллаберди Г. Галканов, кандидат технических наук, профессор, Государственный гуманитарно-технологический университет, Орехово-Зуево, Московская обл., Россия; 142600, Россия, Московская обл., Орехово-Зуево, ул. Зеленая, д. 22; agalkanov@yandex.ru

Information about the author

Allaberdi G. Galkanov, Cand. of Sci. (Computer Science), professor, State University of Humanities and Technology, Orekhovo-Zuevo, Moscow Region, Russia; bld. 22, Zelenaya St., Moscow Region, Orekhovo-Zuevo, Russia, 142600; agalkanov@yandex.ru

Дизайн обложки
Е.В. Амосова

Корректор
А.А. Леонтьева

Компьютерная верстка
Н.В. Москвина

Подписано в печать 10.05.2023.
Формат 60×90 1/16.
Уч.-изд. л. 6,3. Усл. печ. л. 6,4.
Тираж 1050 экз. Заказ № 1737

Издательский центр
Российского государственного
гуманитарного университета
125047, Москва, Миусская пл., 6
www.rsuh.ru