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
2025

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; in the List of leading scientific magazines journals and other editions for publishing PhD research findings peer-reviewed publications fall within the following research area:

1.1.6. Computational Mathematics (physical and mathematical sciences)

2.3.6. Information security methods and systems, information security (technical science)

2.3.8. Informatics and information processes (technical science)

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); в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям и соответствующим им отраслям науки:

1.1.6. Вычислительная математика (физико-математические науки)

2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки)

2.3.8. Информатика и информационные процессы (технические науки)

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

Information Science

Valerii M. Kaziev, Bella V. Kazieva
Dynamic testing of computer programs 8

Elena V. Melnikova, Valentina A. Tsvetkova
Analysis of possibilities of artificial intelligence application in modern scientometry and bibliometry 19

Valerii V. Muromtsev, Anna V. Muromtseva
Information interaction in modern distance learning systems 41

Andrei P. Titov
Generative discrimination method for effective retraining of language models 54

Information Security

Mar'yana A. Georgieva, Konstantin S. Barkhatov
Modernized system of generation and management of crypto-resistant keys 69

Airat B. Shukenbaev, Kamilla R. Ziatdinova, Nailya Sh. Shukenbaeva
Development of a methodology for testing the security of IT projects 80

СОДЕРЖАНИЕ

Информатика

Валерий М. Казиев, Бэлла В. Казиева
Динамическое тестирование компьютерных программ 8

Елена В. Мельникова, Валентина А. Цветкова
Анализ возможностей применения искусственного интеллекта в современной наукометрии и библиометрии 19

Валерий В. Муромцев, Анна В. Муромцева
Информационное взаимодействие в современных системах дистанционного обучения 41

Андрей П. Титов
Метод генеративной дискриминации для эффективного предобучения языковых моделей 54

Информационная безопасность

Марьяна А. Георгиева, Константин С. Бархатов
Модернизированная система генерации и управления криптостойкими ключами 69

Айрат Б. Шукенбаев, Камилла Р. Зиатдинова, Наиля Ш. Шукенбаева
Разработка методики тестирования безопасности ИТ-проектов 80

УДК 004.413.4
DOI: 10.28995/2686-679X-2025-2-8-18

Динамическое тестирование компьютерных программ

Валерий М. Казиев
Кабардино-Балкарский государственный университет, Нальчик, Россия, studkvm@mail.ru

Бэлла В. Казиева
Кабардино-Балкарский государственный университет, Нальчик, Россия, bella_kazieva@mail.ru

Аннотация. Эволюция в сфере разработки программных систем и программирования позволяет перейти к постиндустриальному программированию с применением мощных библиотек в различных средах программирования. Тестирование приложений является актуальной задачей в проблеме анализа качества программных комплексов, оценки согласованности с требованиями технического задания по функционалу, комфортности, надежности. Для решения этой задачи требуется системный анализ технологий, методов и задач тестирования с акцентом на определение параметров работы и программного комплекса. Методами анализа и синтеза, имитационного моделирования динамики процессов отладки получены такие результаты, как: 1) аналитика известных подходов и методов тестирования; 2) предложена классификационная схема тестирующих процессов и критериев оценки надежности комплексов программ; 3) на основе вероятностных гипотез распределения программных ошибок исследована дифференциальная динамическая модель снижения ошибок в программе; 4) предложена модель класса «системы с насыщением» (аналог модели типа Джелински-Моранда) с риск-функцией ошибок. Предложенные рекомендации иллюстрируются примером, в котором продемонстрирована возможность ситуационно настраивать темп процесса тестирования. Результаты исследования можно использовать для аудита процесса отладки и особенно для хаос-тестирования.

Ключевые слова: аудит, программный комплекс, качество программ, тестирование, моделирование

Для цитирования: Казиев В.М., Казиева Б.В. Динамическое тестирование компьютерных программ // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 2. С. 8–18. DOI: 10.28995/2686-679X-2025-2-8-18

Dynamic testing of computer programs

Valerii M. Kaziev
Kabardino-Balkarian State University, Nalchik, Russia,
studkvm@mail.ru

Bella V. Kazieva
Kabardino-Balkarian State University, Nalchik, Russia,
bella_kazieva@mail.ru

Abstract. The evolution in the field of software systems development and programming allows us to move to post-industrial programming using powerful libraries in various programming environments. Application testing is an urgent task in the problem of analyzing the quality of software systems, assessing consistency with the requirements of the terms of reference in terms of functionality, comfort, and reliability. To solve this problem, a systematic analysis of testing technologies, methods, and tasks is required, with an emphasis on determining the parameters of the operation and software package. Methods of analysis and synthesis, simulation modeling of the dynamics of debugging processes have obtained such results as: 1) analysis of known testing approaches and methods; 2) a classification scheme of testing processes and criteria for evaluating the reliability of software packages is proposed; 3) based on probabilistic hypotheses of the distribution of software errors, a differential dynamic model for reducing errors in a program is investigated; 4) a model of the "saturation systems" class (analogous to the Jelinsky-Morand type model) with risk is a function of errors. The proposed recommendations are illustrated by an example that shows that it is possible to situationally adjust the pace of the testing process. The results of the study can be used to audit the debugging process and, especially, for chaos testing. The evolution in the field of software systems development and programming allows us to move to post-industrial programming using powerful libraries in various programming environments.

Keywords: audit, software package, software quality, testing, modeling

For citation: Kaziev, V.M. and Kazieva, B.V. (2025), "Dynamic testing of computer programs", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 8–18, DOI: 10.28995/2686-679X-2025-2-8-18

Введение

Разработка компьютерных программ на промышленном уровне требует учета положений стандартизации (например, IEEE 1012) и комплексной оценки их качества, своевременного выявления и устранения латентных ошибок на всех этапах разработки, включая ввод в эксплуатацию и сопровождение программного обеспечения.

Процесс валидации направлен на выяснение соответствия программы или ее модулей заявленным спецификациям (ТЗ), требованиям полноты, функциональности и устойчивости функционирования, а также потребительским ожиданиям. Валидация – процесс более общий, она учитывает соответствие потребительским ожиданиям, но часто сводится к «приземленному» тестированию.

Верификация проводится до начала оценки релевантности программы, в начале разработки [Мерзляков 2023, с. 34]. Она проверяет (по заданным критериям) соответствие разрабатываемого (сопровождаемого) ПО используемым процессам, спецификациям разработки. Верификация, как и валидация, использует активно релевантные критерии соответствия. Хотя верификация базируется на формализации, но редко полностью ею ограничивается.

Тестирование дает возможность априори оценивать количественные и некоторые качественные параметры ПО, идентифицировать их для дальнейшей устойчивой верификации и эксплуатации.

В статье выполнен сравнительный и системный анализ существующих подходов и инструментов (методов) тестирования. Предложены модели, смежные с этой проблемой.

Методы и инструментарий тестирования

Тестирование демонстрирует работоспособность или ее отсутствие на минимальном, но полном наборе тестов, т. е. без дублирования проверки одной и той же ветви логики программы. Все ветви логики (алгоритма) должны быть проверены на соответствующих тестах. Тестирование позволяет оценивать устойчивую работу программ, оптимизировать ресурсы, рыночную и интерфейсную привлекательность.

Тестировщик – профессия востребованная. Его ключевая задача – указать программисту ошибки и уязвимости в программе (их места, причины, возможности исправления) при максимальном количестве возможных ситуациях.

Тестировщику исходный код не нужен, он не получает его от заказчика. Его интересует лишь вход-выход и сам выходной результат, надежность. Последнее часто понимается как устойчивость, работоспособность, непрерывная готовность к использованию программы [Лаврищева 2019, с. 98] или безотказность, предотвращение или быстрое устранение отказа [Карпович 2020, с. 46], восстанавливаемость управления после сбоя с корректной реализацией целевых сценариев и параметров.

Тестирование – способ обеспечения качества и надежности ПО. Оценивание сложности ПО – задача многофакторная и многокритериальная. Тестирование – экспертно-эвристический и статистико-математический процесс, который часто опирается на априорные установки, критерии и полуэмпирические модели надежности.

Тестирование может быть в процессе разработки (цель – обнаружение ошибок), для проверки соответствия требованиям заказчика (стейкхолдера) и приемочное, пользовательское (цель – аудит для маркетинга, запуска продаж). Тестировщик – профессионал, возможно, в прошлом сам программист. Чаще работает тандем программиста и ассоциированного тестировщика (асессора) с общей ответственностью за результативность и надежность.

Результат тестирования комплекса программ зависит от инфологических связей программ (модулей, интерфейса), от системной связности комплекса [Казиев 2007, с. 26].

Тестирование проводят в персональном (автономном) или командном режиме, ручном или автоматизированном, а сейчас и в интеллектуализированном режиме. Есть различные модели оценивания надежности ПО (рис. 1).

Ручное тестирование для расширении функционала тестируемого ПО достаточно и трудоемкое [Nass 2021].

Есть и комбинаторное тестирование, охватывающее всевозможные взаимодействия входных параметров, например, попарное (двухстороннее) тестирование [Шевчук 2023, с. 44].

Несмотря на появление ряда интеллектуальных алгоритмов тестирования, полностью процесс автоматизировать невозможно – слабо формализуемы нестандартные ситуации. Но автоматическое генерирование тестов выполняется достаточно успешно, есть соответствующие инструменты генерации тестов и ввода тестовых заданий в среду тестирования, анализа тестирования и документов.

Автоматизация тестирования минимизирует «дубли» ситуаций (ветвей логики) тестового набора, позволяет тестировать различные ситуации. Можно «самотестировать» – тестировать самим программистом.

Рис. 1. Классы моделей, подходов оценки надежности ПО

Инструментарий тестирования выбирается релевантно цели и сложности ПО, до перехода к автоматизации. Сначала требования, затем анализ инструментов и, наконец, выбор инструментария. Надежность ПО тестируется теоретически, верификацией, доказательным образом или практически, на тестах.

К сожалению, первый, аксиоматический метод, редко используется, он требует, в частности, алгебраических компетенций (теория полугрупп, абстрактные алгебры автоматов и др.). Этому учат в некоторых университетах, на курсах тестировщиков подобные темы не затрагиваются. Часто используют недостаточно формализованный подход к верификации как, например, с применением эвристического подхода [Кашкевич 2023, с. 32] или динамических рядов [Радионова 2018, с. 42].

Тестирование также предполагает наличие компетенций, но им можно научить достаточно быстро. Например, на 2–3-месячных курсах. При базовой естественно-научной подготовке или даже без нее.

Ситуационное (сценарное) тестирование реализуется поэтапно, как и требуется при имитационном моделировании:

– генерация сценария (кластера реальных тестов);
– разработка (выбор, адаптация) нагрузочного сценария;
– тестирование (реализация сценария);
– анализ реакции на сценарии и формирование отчета.

Автоматизацию тестирования (как по «ширине», так и по «глубине») часто сдерживает стоимость автоматизации и его поддержки (по данным аналитиков WorkSoft).

Функциональное тестирование базируется на релевантной программе испытаний и имеет нижеследующие уровни:

1) покомпонентное тестирование (тестирование блочное, модульное, с учетом назначения и функций компоненты);
2) интегрирующее тестирование (тестирование логики взаимодействий, приема-передачи данных и управления).

Подвидом функционального тестирования является тестирование исследовательское. Оно используется для оценки эволюционных возможностей разработки и не предполагает четких, стандартизируемых требований. Это высокоуровневое тестирование профессионалов высокого и творческого уровня, граничащего с искусством (как в программировании, понимаемого уже не так часто как искусство).

Нефункциональное тестирование ПО осуществляется по специальной программе испытаний, в которой соблюдаются все целевые требования конкурентоспособности ПО на рынке, а именно кросс-платформенное и интерфейсное единство требований, применение DevOps, Agile и др. Привлекают QA-специалистов, обладающих компетенциями анализа, моделирования, SoftSkills и др.

Есть и важное для бизнес-компаний мобильное тестирование [Барсуков 2023, с. 5], которое проверяет мобильные приложения на функциональность, согласованность. Такое тестирование зависит от типа приложения – нативное, или гибридное (iOS/Android), прогрессивное (PWA) и др. Есть фреймворки, в частности, кросс-платформенный Appium, «Андроидный» Espresso или XCUITest для iOS.

Для каждого фактора или параметра качества ПО проводят нагрузочное тестирование по изучению реакции на его изменение. Часто с параметрами экстремальных ситуаций, например, высоконагруженных.

Хотя говорят, что каждый может сам же и протестировать свою программу, навыки и команду тестировщиков следует совершенствовать. Есть некоторые ключевые составляющие создания и удержания успешных команд тестирования. Управление командой ориентируется на тип и мотивацию тестировщика.

Чтобы выяснить тип тестировщика есть специальные анкеты «стиля тестировщика». Приведем пример фрагмента анкеты для тестировщиков.

1. Внедрение технологии тестирования сдерживается (проранжируйте указанные факторы):

– квалификацией тестировщика;
– нечеткостью и непониманием целей и задач тестирования;
– недостаточной личной мотивацией;

– отсутствием эффективных подготовительных курсов;
– плохой организацией командной работы, дискомфортом в команде;
– избыточной рутиной;
– постоянными переработками и срочностью проектов;
– требовательностью и негибкостью руководителя;
– подавлением своих потребностей;
– уникальностью программных продуктов.

По аналогичным вопросам выявляют четыре типа тестировщиков: «прагматик»; «фасилитатор»; «аналитик»; «пионер».

Важно признать их различия, чтобы максимально не зацикливаться на слабостях. Анкета анализа также может быть использована для того, чтобы убрать конфликты, разрядить «взрывоопасные» ситуации.

Модели динамики тестирования программ

Тестировщику следует непрерывно и оперативно анализировать динамику программных ошибок (текущих и/или потенциальных) для достижения параметров устойчивости программы.

Для того чтобы построить и исследовать модель надежности ПО, следует определиться с гипотезами статистического характера. В частности, модель типа Джелински-Моранда базируется на гипотезе непрерывного, независимого и равновероятного обнаружения ошибок.

Формализуем наши гипотезы, отражающие процедуру поиска ошибок:

– темп обнаружения ошибок пропорционален с некоторым экспериментально устанавливаемым коэффициентом оставшемуся объему ошибок в ПО;
– все ошибки равновероятны и проявляются независимо;
– при отладке риск внесения иных ошибок нулевой;
– время тестирования распределено по экспоненте;
– темп обнаружения ошибок (функция риска) задается в виде:

$$R(x, t) = R_{ij},$$

$$x \in [x_i; x_{i+1}],\ t \in [t_j; t_{j+1}],\ i = 1, 2, \ldots, m-1, j = 0,1, \ldots, n-1.$$

Рассмотрим следующую модель. Пусть $u_i(x_i)$, $i = 1, \ldots, n$ – показатель надежности программной системы по фактору x_i, который рассматривается, x_{iopt} – оптимальное для устойчивости значение x_i,

k_i – ритмичность по x_i, $s_i(x_i)$ – темп по x_i, $s_i(x_i)$ зависит лишь от x_i (неявно от t), $u_i = u_i(t)$.

Темп $s(x)$ задаем зависимостью вида:

$$s_i(x_i) = \frac{u_i - u_i^{min}}{u_i^{max} - u_i^{min}},$$

где x_i^{max}, x_i^{min} – максимальное, минимальное значения x_i.

При условии:

$$u_i(x_i^{max}) = 1,\ i = 1, \ldots, n$$

запишем систему расщепляющихся уравнений:

$$\frac{du_i}{dx_i} = \frac{a_i}{u_i^{max}} u_i\left(x_i^{opt} - x_i\right), \qquad a_i = \frac{x_i^{max}}{k_i},$$

которая устойчиво разрешима:

$$u_i = exp\left(-\frac{(x_i^{opt} - x_i)^2}{2a_i}\right).$$

Получили, как и ожидаемо по гипотезе, нормальное распределение.

Важно идентифицировать n-мерный куб: $a_{imin} \le a_i \le a_{imax}$, $i = 1,2, \ldots, n$ устойчивости программы.

Пример. Для теста: $n = 1$, $s_1(1) = 4$, $s_1(2) = 5$, $y_1^{min} = 0$, $y_1^{max} = 7$ с дополнительным значением, после идентификации получаем $a_1 = \log_{3,5} 1{,}5 = 0{,}323$.

Рассмотрим вторую модель. Если $u(x, t)$ – объем ошибок, найденных к моменту времени t (включительно) с помощью x тестировщиков, то можно предложить модель типа систем «с насыщением» [Казиев 2024, с. 33]:

$$div\ u = k(x, t)\ (Lu - u\ (x, t)),$$

где $k(x, t)$ – интенсивность тестирования, Lu – оператор насыщения ошибками в программе, этот оператор идентифицируется при решении обратной задачи или задается эвристически, например, $Lu = u_{max}$.

При начально-нелокальных условиях вида:

$$u(x, 0) = \varphi(x),$$
$$u(0, t) = \int_0^t z(x, t)\ u(x, t)\ dx + \psi(t),$$
$$\varphi(0) = \psi(0),$$

где

$$z(x, t) \in C^1(\Omega), \ \psi = C^1]0, T[,$$

получаем модель тестирования.

По непрерывности $u(x, t)$ можно полагать

$$u_{max} = u(x_0, t_0), (x_0; t_0) \in [0; X] \text{ x } [0; T].$$

Как и в модели Джелински-Моранда, риск-функцию ошибок зададим в форме:

$$R(x, t) = k(x, t)(u_{max} - u),$$
$$R_{ij} = R(x_i, t_j) = k_{ij}(u_{max} - u_{ij}),$$
$$u_{ij} = u(x_i, t_j).$$

По значениям u_{ij} идентифицируется диапазон интенсивности $k_{min} \le k \le k_{max}$ и настраивается темп процесса тестирования.

Заключение

Как показали исследования авторов, технология тестирования быстро эволюционирует с учетом новых достижений в области индустриального и веб-ориентированного программирования. С увеличением сложности тестируемых компьютерных программ и закономерного расширения функционала механизма тестирования традиционное ручное тестирование становится все более затратным процессом. В условиях жестких ограничений на привлекаемые ресурсы и вариативности алгоритмических ситуаций актуальными являются задачи автоматизации и прогнозирования процесса отладки. Проведенное исследование является начальным шагом в развитии модельного подхода к тестированию. Наиболее перспективным следует считать адаптацию рассмотренных подходов и моделей к хаос- и бэк-тестингу, которая позволит оптимизировать параметры процесса отладки и оценки эксплуатационных качеств и характеристик программного обеспечения.

Литература

Барсуков 2023 – *Барсуков И.А., Наумова Н.А., Бострикова Д.К., Машина Е.А.* Создание унифицированных механизмов автоматизированного тестирования приложений для мобильных устройств // Инженерный вестник Дона. 2023. № 5. С. 1–19.

Казиев 2007 – *Казиев В.М.* Введение в анализ, синтез и моделирование систем. М.: Бином: Лаборатория знаний, ИНТУИТ, 2007. 244 с.

Казиев 2024 – *Казиев В.М., Казиева Б.В.* Ситуационное моделирование кибератак на инфраструктуру организации в центрах мониторинга инцидентов // «Новые идеи»: труды Региональной научно-практической конференции (г. Ростов-на-Дону, 21–26 октября 2024 г.) / Под ред. Н.Д. Панасенко. Ростов н/Д.: ДГТУ-Принт, 2024. С. 30–34.

Кашкевич 2023 – *Кашкевич А.М., Баданина Ю.В., Филимонов А.С., Долгих А.И.* Верификация программных комплексов на примере статически определимой призматической балки // Известия вузов (сер. «Машиностроение»). 2023. № 5. С. 29–36.

Карпович 2020 – *Карпович Е.Е.* Методы тестирования и отладки программного обеспечения. М.: МИСИС, 2020. 136 с.

Лаврищева 2019 – *Лаврищева Е.М., Зеленов С.В., Пакулин Н.В.* Методы оценки надежности программных и технических систем // Труды ИСПРАН. 2019. Т. 31. № 5. С. 95–108.

Мерзлякова 2023 – *Мерзлякова Е.Ю., Янченко Е.В.* Обзор методов верификации и оценки качества программного обеспечения // Вестник СибГУТИ. 2023. Т. 17. № 1. С. 92–106.

Радионова 2018 – *Радионова Ю.А., Емельянов А.А., Савкин А.Л.* Использование статистических данных в рамках динамической модели оценки надежности программного обеспечения // Автоматизация процессов управления. 2018. № 5 (54). С. 36–47.

Шевчук 2023 – *Шевчук В.И.* Попарное тестирование программного обеспечения // Universum: технические науки. 2023. № 7 (112). С. 44–45.

Nass 2021 – *Nass M., Alegroth E., Feldt R.* Why many challenges with GUI test automation (will) remain // Information and Software Technology. 2021. Vol. 138 (2). P. 106–625.

References

Barsukov, I.A., Naumova, N.A., Bostrikova, D.K. and Mashina, E.A. (2023), “Creating of unified mechanisms for automated testing of applications for mobile devices”, *Engineering Bulletin of the Don*, no. 5, pp. 1–19.

Kaziev, V.M. (2007), *Vvedenie v analiz, sintez i modelirovanie sistem* [Introduction to analysis, synthesis and modeling of systems], Binom: Laboratoriya znanii, INTUIT, Moscow, Russia, 244 p.

Kaziev, V.M. and Kazieva, B.V. (2024), “Situational modeling of cyberattacks against organization’s infrastructure in incident monitoring centers”, in Panasenko, N.D. (ed.), *“Novye idei”: trudy Regional’noi nauchno-prakticheskoi konferentsii* [“New Ideas”. Proceedings of the Regional Scientific and Practical Conference] (Rostov-on-Don, October 21–26, 2024), DSTU-Print, Rostov-on-Don, Russia, pp. 30–34.

Kashkevich, A.M., Badanina, Yu.V., Filimonov, A.S. and Dolgikh, A.I. (2023), "Verification of software systems using the example of a statically definable prismatic beam", *News of universities. Mechanical Engineering*, no. 5, pp. 29–36.

Karpovich, E.E. (2020), *Metody testirovaniya i otladki programmnogo obespecheniya* [Software testing and debugging methods], MISIS, Moscow, Russia, 136 p.

Lavrishcheva, E.M., Zelenov, S.V. and Pakulin, N.V. (2019), "Methods for assessing the reliability of software and technical systems", *Proceedings ISPRAS*, vol. 31, no. 5, pp. 95–108.

Merzlyakova, E.Yu. and Yanchenko, E.V. (2023) "Overview of methods for verifying and assessing the quality of software", *Vestnik SibGUTI*, vol. 17, no. 1, pp. 92–106.

Nass, M., Alegroth, E. and Feldt, R. (2021), "Why many challenges with GUI test automation (will) remain", *Information and Software Technology*, vol. 138 (2), pp. 106–625.

Radionova, Yu.A., Emelyanov, A.A. and Savkin, A.L. (2018), "Use of statistical data within the dynamic model of software reliability assessment", *Automation of control processes*, no. 5 (54), pp. 36–47.

Shevchuk, V.I. (2023), "Pairwise testing of software", *Universum: technical sciences*, no. 7 (112), pp. 44–45.

Информация об авторах

Валерий М. Казиев, кандидат физико-математических наук, доцент, Кабардино-Балкарский государственный университет, Нальчик, Россия; 360004, Россия, Нальчик, ул. Чернышевского, д. 173; studkvm@mail.ru

Бэлла В. Казиева, кандидат экономических наук, доцент, Кабардино-Балкарский государственный университет, Нальчик, Россия; 360004, Россия, Нальчик, ул. Чернышевского, д. 173; bella_kazieva@mail.ru

Information about the authors

Valerii M. Kaziev, Cand. of Sci. (Physics and Mathematics), associate professor, Kabardino-Balkarian State University, Nalchik, Russia; bld. 173, Chernyshevsky Str., Nalchik, 360004, Russia; studkvm@mail.ru

Bella V. Kazieva, Cand. of Sci. (Economics), associate professor, Kabardino-Balkarian State University, Nalchik, Russia; bld. 173, Chernyshevsky Str., Nalchik, 360004, Russia; bella_kazieva@mail.ru

УДК 004.8:001
DOI: 10.28995/2686-679X-2025-2-19-40

Анализ возможностей применения искусственного интеллекта в современной наукометрии и библиометрии

Елена В. Мельникова
Всероссийский институт научной и технической информации Российской академии наук (ВИНИТИ РАН), Москва, Россия, verden.mel@yandex.ru

Валентина А. Цветкова
Всероссийский институт научной и технической информации Российской академии наук (ВИНИТИ РАН), Москва, Россия, vats08@mail.ru

Аннотация. Цель исследования состоит в выявлении и анализе возможностей применения искусственного интеллекта в наукометрии и библиометрии. Искусственный интеллект рассматривается в работе как раздел информатики. Особенностью статьи является ее междисциплинарный характер. К методам исследования относятся: конкретизация границ исследования, теоретический анализ, синтез, сравнение сущностей, систематизация материала, интерпретация и обобщение результатов. Для характеристики области применения искусственного интеллекта представлены и проанализированы общие черты современной наукометрии и библиометрии, выделены их особенности, разработано определение для каждой из двух метрических дисциплин с учетом их различий, рассмотрены их задачи и потребности. Раскрыто основное содержание технологии искусственного интеллекта, представлены его базовые определения, проанализированы сферы возможного применения в наукометрии и библиометрии, включая общие направления использования для двух дисциплин. Выявление основных направлений применения проведено в том числе с привлечением результатов актуальных исследований российских, индийских, иранских, китайских, западных ученых, а также исследователей из Юго-Восточной Азии. Сделаны выводы о том, что на современном этапе искусственный интеллект получает все большее распространение в наукометрии и библиометрии; его инструменты и методы способствуют оптимизации решения метрических задач, обеспечивая повышение скорости и качества обработки, анализа и представления научной информации и данных, включая современную категорию больших данных

Ключевые слова: информатика, искусственный интеллект, алгоритмы глубокого обучения, нейросети, большие языковые модели, интеллектуальный анализ текста, наукометрия, библиометрия, результативность науки, библиометрические показатели, постатейная классификация

Для цитирования: Мельникова Е.В., Цветкова В.А. Анализ возможностей применения искусственного интеллекта в современной наукометрии и библиометрии // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 2. С. 19–40. DOI: 10.28995/2686-679X-2025-2-19-40

Analysis of possibilities of artificial intelligence application in modern scientometry and bibliometry

Elena V. Melnikova
All-Russian Institute for Scientific and Technical Information, Moscow, Russia, verden.mel@yandex.ru

Valentina A. Tsvetkova
All-Russian Institute for Scientific and Technical Information, Moscow, Russia, vats08@mail.ru

Abstract. The purpose of the research work is to identify and analyze the possibilities of the artificial intelligence application in scientometry and bibliometry. Artificial intelligence is considered in the work as a section of informatics. A special feature of the article is its interdisciplinary character. The research methods include: specification of research boundaries, theoretical analysis, synthesis, comparison of entities, systematization of the material, interpretation and generalization of results. To characterize the field of the artificial intelligence application, the general features of modern scientometry and bibliometry are presented and analyzed, their specific features are highlighted, the definition for each of the two metric disciplines is worked out taking into account their differences; their tasks and needs are considered. The main content of artificial intelligence technology is revealed, its basic definitions are presented, spheres of its possible application in scientometry and bibliometry are analyzed, including the common directions of its usage for the two disciplines. The main spheres of application were identified along with using the results of current research by Russian, Indian, Iranian, Chinese, Western scientists, as well as researchers from SouthEast Asia. It is concluded that artificial intelligence nowadays is becoming increasingly widespread; its tools and methods contribute to optimizing the solution of scientometric and bibliometric tasks, providing an increase in the speed and quality of processing, analysis and pre-

sentation of scientific information and data, including the modern category of big data.

Keywords: informatics, artificial intelligence, deep learning algorithms, neural networks, large language models, text mining, scientometry, bibliometry, effectiveness of science, bibliometric indicators, itemized classification

For citation: Melnikova, E.V. and Tsvetkova, V.A. (2025), "Analysis of possibilities of artificial intelligence application in modern scientometry and bibliometry", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 2, pp. 19–40, DOI: 10.28995/2686-679X-2025-2-19-40

Введение

Наукометрические и библиометрические исследования являются значимой составляющей работы с научной и технической информацией в рамках информационного, а также библиотечного дела. Практика последнего десятилетия в области применения технологии искусственного интеллекта (ИИ) в наукометрии и библиометрии демонстрирует существенные изменения в работе научных организаций и коллективов, проводящих исследования в двух названных сферах, а также в целом в деятельности научного и образовательного сообщества, включая те его сегменты, где использование ИИ является непрофильным. Эти изменения выражаются в активизации применения искусственного интеллекта как вспомогательного инструмента в проведении научных исследований [Шрайберг 2024], включая науко/библио-метрический анализ [Li, Duan 2023].

Рост активности применения ИИ в области метрических исследований, как и в других сферах науки, обусловлен тем, что использование ИИ-инструментов и методов приводит к увеличению скорости обработки данных, повышению качества результатов исследований, росту точности научных прогнозов. При этом наибольшего позитивного эффекта добиваются коллективы, учитывающие определенные ограничения в использовании инструментария искусственного интеллекта, которые требуют проверки надежности ИИ-алгоритмов и адекватности их действия. Важным фактором также является степень подготовленности научных коллективов, включая сферу гуманитарных и общественных наук, к использованию новых технологических ИИ-инструментов.

В наукометрии и библиометрии, как и в ряде других наук, одним из сдерживающих факторов в развитии ИИ-практики является

предвзятое отношение со стороны некоторых ученых к ИИ-нововведениям, к использованию науко/библиометрических показателей, полученных с привлечением искусственного интеллекта, для подготовки отчетов о результативности научной деятельности или рейтингов. С учетом этого обстоятельства необходимым условием, по мнению ученых [Столяров 2022; Шталь, Шредер, Родригес 2024], становится обеспечение адекватного по скорости, нефорсированного внедрения ИИ-технологии, соблюдающего в том числе условие этичности как по отношению к пользователям метрической информации, так и по отношению к членам науко/бибилиометрических коллективов.

Характерные черты и особенности современных наукометрии и библиометрии

Логика возникновения и эволюции исследуемых нами метрических дисциплин и последовательности операций в рамках метрического анализа обусловливает рассмотрение их характерных черт и особенностей, начиная с библиометрии.

Библиометрия и ее особенности

Библиометрия – это научная дисциплина, в рамках которой разработан набор специализированных статистических и математических инструментов для исследования документальных потоков и массивов информации на основе их количественной оценки. Библиометрия занимается детальной обработкой и анализом данных, касающихся научных публикаций, их авторов, ссылок, ключевых слов и другой библиографической информации. На современном этапе библиометрия является одним из наиболее распространенных методов оценки публикационной активности ученых и важным вспомогательным средством в анализе их деятельности группами признанных в научном мире экспертов [Гиляревский 2022а; Mitha, Omarsaib 2024]. Библиометрия содействует ученым в поиске и подборе для их исследований наиболее востребованных и актуальных научных работ наиболее авторитетных авторов.

Базовым библиометрическим методом, как известно, является анализ пристатейных ссылок, который также называют методом научного цитирования. Метод пристатейных ссылок базируется на идее Ю. Гарфилда [Garfild E. 1964] об использовании количества ссылок на статьи в научных журналах как средства количествен-

ной оценки результатов деятельности ученого[1]. Метод основан на предложенном Ю. Гарфилдом показателе – индексе научного цитирования (*Science Citation Index (SCI)*). На основе индекса научного цитирования разработано большое количество производных метрических показателей, которые входят в сферу компетенции наукометрии.

Одним из значимых методов библиометрии, помимо вычисления индекса научного цитирования, также является метод библиографического сочетания документов (или библиографической связанности). Метод предусматривает поиск связанных по смыслу документов, авторы которых ссылаются на одни и те же работы. Числом совпадающих ссылок измеряется степень смысловой и тематической связанности документов, что важно для пользователей, осуществляющих поиск публикаций по интересующей их проблематике.

Наукометрия и ее отличия от библиометрии

Наукометрия – это научная дисциплина, которая на основе метрических исследований изучает «развитие науки как информационного процесса» [Налимов 1969], проявляющего себя через систему научных коммуникаций. Наукометрия использует совокупность методов, основанных на разработке и применении особых числовых показателей (метрик) для исследования процесса развития науки в целом и ее отдельных направлений, анализа перспективности научных исследований в конкретной предметной области, определения структуры науки, взаимосвязей между научными областями, тенденций и перспектив развития науки, решения задач по оценке результативности научной деятельности [Melnikova 2024], определения «веса» ученого и его идей в научном сообществе.

Для решения перечисленных задач наукометрия активно использует методы, применяемые в библиометрии, альтметрии, вебометрии, медиаметрии и ряде других современных метрических дисциплин. Метрические методы основываются на формальных количественных показателях. Из представленного комплекса в наукометрии наиболее широко используются библиометрические

[1] Ю. Гарфилд также рассматривал возможность использования индекса научного цитирования для оценки научного «веса» конкретного автора и его идей и как возможного инструмента изучения структуры науки. Эти показатели вошли в сферу действия наукометрии. – *Примеч. авт.*

методы. Они предполагают первоначальное проведение мониторинга и анализа документопотоков научных, образовательных организаций и учреждений и получение библиометрических показателей [Лазарев 2022; Цветкова, Мохначева 2021]. Затем на их основе в рамках наукометрии производится анализ публикационной активности ученых/преподавателей, информационно-документального сопровождения НИОКР, исследуются информационные потребности научно-образовательного сообщества, структура сети научных коммуникаций, даются оценки результативности научно-исследовательской деятельности.

Для решения перечисленных и некоторых других задач в наукометрии разрабатываются собственные, специализированные метрические показатели/индексы. Они позволяют дать оценку не только количества, но и качества научной деятельности. В их основе, как было отмечено, лежит индекс научного цитирования. К основным наукометрическим показателям относятся: 1) индекс Хирша – характеризует научную активность исследователя и востребованность его идей; индекс Хирша ученого равен h, если ученый опубликовал h статей, на каждую из которых сослались как минимум h раз; 2) i-индекс – позволяет выделить в научной организации или области исследований ядро наиболее научно активных и востребованных авторов, имеющих наиболее высокий индекс Хирша; 3) g-индекс – отражает авторитетность и «вес» сотрудников организации в научном мире и вычисляется как корень из суммарного цитирования работ ученого или сотрудников организации; 4) импакт-фактор (для научных журналов) и некоторые другие показатели.

Общая для двух дисциплин основа исследования

Широкое использование библиометрических методов как в самой библиометрии, так и в наукометрии закладывает логическую основу для исследования общих черт и особенностей применения искусственного интеллекта в этих двух взаимосвязанных метрических дисциплинах. Для обеих дисциплин потребность в применении ИИ имеет объективный характер: она обусловлена необходимостью обработки и анализа непрерывно поступающих и стремительно растущих потоков разнородной информации с акцентом на обработку современной информационной категории – «больших данных». Эти обстоятельства требуют применения специальных высокопроизводительных автоматизированных инструментов [Asiakin N. 2021; Каптерев 2023], без которых человек самостоятельно справиться уже не может.

Применение искусственного интеллекта в наукометрии и библиометрии

Основное содержание технологии искусственного интеллекта[2]. Проблематика искусственного интеллекта с начала XXI в. прочно закрепилась в центре внимания информатики как науки о свойствах информации, процессах и методах ее сбора, хранения, обработки, передачи, анализа и оценки с применением компьютерных технологий, обеспечивающих возможность ее использования в различных сферах человеческой деятельности. Отдельные аспекты ИИ-проблематики также рассматриваются в рамках нейроинформатики, кибернетики, науки о данных. Каждая из дисциплин исследует ИИ со своего ракурса и своими средствами развивает его теорию и практику.

Искусственный интеллект – это раздел информатики, в котором разрабатываются методы и средства компьютерного решения интеллектуальных задач, традиционно решаемых человеком, включая, в том числе, анализ имеющейся и генерацию новой информации. Существуют и другие определения искусственного интеллекта. Так, соответствующий данной тематике российский ГОСТ[3] определяет ИИ как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека... и получать при выполнении конкретных практически значимых задач обработки данных результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека».

С учетом вышеизложенного допустимо считать, что механизм искусственного интеллекта строится на имитации нейронных процессов в биологическом мозге. На современном этапе ИИ-разработки далеки от биологического оригинала[4], но процесс

---

[2] В данном параграфе авторы не ставят задачу дать развернутую характеристику ИИ-технологии, а отражают базовые актуальные моменты, которые могут иметь отношение к метрическим дисциплинам.

[3] ГОСТ Р 59277-2020 «Системы искусственного интеллекта. Классификация систем искусственного интеллекта». Раздел 3, пункт 18 / Федеральное агентство по техническому регулированию и метрологии. М.: Стандартинформ, 2021. 16 с.

[4] Стремление разработчиков искусственного интеллекта создать полное подобие естественного интеллекта сходно со стремлением к абсолютной истине, к которой можно приближаться бесконечно, но полностью достичь ее невозможно. Об этом свидетельствуют законы классической логики. Об этом говорит философия, которая обозначает методологические рамки для развития всех наук и технологий. – *Примеч. авт.*

совершенствования технологии продолжается. В рамках ИИ-технологии последовательно решаются две базовые рабочие задачи: 1) классифицировать входные данные на основе соответствующим образом разработанных и реализованных в рамках компьютеров виртуальных моделей и 2) на базе этих моделей делать прогнозы результатов, вырабатывать оптимальные прогнозные решения по изначально заданным вопросам или проблемам, под которые создавались модели.

На современном этапе существуют две основные формы искусственного интеллекта – дискриминативный ИИ и генеративный ИИ, который появился и развивается в последние несколько лет. Обе формы ИИ дополняют друг друга. Дискриминативный ИИ (ДИИ) специализируется на операциях анализа данных, интерпретации, классификации и прогнозирования. Главное отличие генеративного ИИ (ГИИ) состоит в том, что он нацелен на генерацию новых данных и новой информации (в виде текста, видеоряда и др.) с ориентацией на заданные шаблоны/образцы; он также способен обеспечивать классификацию, прогнозирование, но менее эффективно, чем ДИИ. Одним из характерных примеров практического применения возможностей ГИИ в создании нового контента является *ChatGPT* [Родионов, Цветкова, Калашникова 2025], представляющий собой большую языковую модель *(LLM)*, обученную на базе архитектуры *GPT*. Другой пример в этой области – последняя китайская разработка *DeepSeek R-1,* которая также функционирует на базе больших данных.

В науко/библиометрической сфере ИИ может решать вопросы оценки публикационной активности отдельных ученых, научных организаций, обеспечивать анализ развития научных областей, национальной науки в целом [Gowri 2019], содействовать определению других, приведенных выше, параметров развития науки. При решении этих задач и генерации прогнозных решений ИИ-технология основывается на функциональной связке алгоритмов глубокого машинного обучения и искусственных нейронных сетей. Чем более многослойной является структура нейросети, тем более глубоко может обучаться компьютерная система для реализации метрических задач и тем более эффективные прогнозные решения она способна выдавать. Эти преимущества глубокого обучения как одной из базовых составляющих ИИ-технологии приводят к тому, что искусственный интеллект приобретает все более широкое распространение во многих сферах общественной жизни и областях науки, включая рассматриваемые метрические дисциплины.

Проанализируем современные возможности использования искусственного интеллекта в наукометрии и библиометрии и

выделим основные направления его практического применения в рамках этих научных дисциплин.

Общие направления применения искусственного интеллекта в наукометрии и библиометрии

Автоматизированная обработка и анализ данных. Применение ИИ в обработке и интеллектуальном анализе огромных массивов разнородных научных данных для проведения науко/бибилиометрических исследований, как было отмечено выше, реализуется на основе глубокого машинного обучения [Gowri 2019]. Глубокое обучение в связке с нейросетями основывается на математических и вычислительных методах особой сложности, что в совокупности делает возможным обработку и анализ категории «больших данных», обладающих существенным потенциалом научной и общественной полезности. ИИ помогает выявлять в обрабатываемых массивах больших данных скрытые (часто – неожиданные) значимые смысловые закономерности, несущие новое знание.

Обработка естественного языка (NLP – Natural Language Processing) – это научное направление, объединяющее возможности ИИ (в лице глубокого обучения) и математической лингвистики; с использованием специализированного программного обеспечения *NLP* решает задачи компьютерного анализа и синтеза текстов на естественном языке [Bircan, Salah 2022]. Среди функций *NLP*, имеющих прямое отношение к метрическим дисциплинам и информационным ресурсам, на основе которых они проводят свои исследования, необходимо указать: *определение значения и смысла слов* – в результате семантического анализа предложений, из которых состоит текст; *распознавание именованных сущностей* (имени человека, названий организаций, городов, стран и т. д.) – путем их правильного выявления и корректного использования при обработке текста или генерации ответа на запрос; *определение и сохранение перекрестных ссылок* – в результате учета взаимосвязей между токенами (небольшими фрагментами), на которые разбивается текст при анализе; *генерирование текста на естественном языке* – путем перевода в формат текста структурированных (табличных) данных или голосовой речи (на основе распознавания речи), например, при подготовке информационных материалов для метрического анализа.

Распознавание рукописных текстов реализуется ИИ-технологией на основе специальной программы распознавания основных

структурных элементов рукописного текста. В результате этих операций искусственный интеллект упрощает и расширяет доступ к научным данным за счет их архивированной рукописной части, которая может содержать значимую информацию для решения некоторых современных науко/библиометрических задач в сравнении с публикационным материалом, относящимся к прошлому.

Вопросы индексации данных занимают важное место в работе баз данных, а также систем индексации и цитирования научной информации. Искусственный интеллект позволяет существенно ускорить процессы индексации данных и снизить количество ошибок в работе инструментов индексации. Увеличение скорости и безошибочности в работе систем индексации обеспечивает, например, повышение темпов классификации книг в библиотеках и качества их каталогизации [Waltman, Boyack 2020], что создает более благоприятную информационную основу для получения в дальнейшем адекватных метрических результатов. Совершенствование процедур индексации, кроме того, ускоряет поиск цифровых ресурсов в научных базах данных, обеспечивает предоставление по запросам пользователей более конкретного и точного информационного материала для проведения науко/библиометрического анализа, что способствует повышению качества метрических исследований.

Проблемы классификации

Классификация научных публикаций, книг имеет для наукометрии и библиометрии большое значение. Классификация может производиться на основе традиционных методов, включая регрессионный, байесовский и т. п. В других случаях, например, в рамках тематической классификации [Гиляревский 2022с], нацеленной на определение тематики научных текстов, также достаточно широко используются подходы на основе цитирования – прямого цитирования, ко-цитирования, библиографического сочетания документов, изучения сетей цитирования [Zhao, Feng 2022], а также комбинации этих подходов и показателей. Адекватное распределение публикаций и книг по классам определяет корректность обработки накопленного информационного массива и последующего вычисления метрических показателей.

В процессе классификации могут возникать операционные сложности, обусловленные: 1) ошибками при связывании – установлении идентифицирующих связей между объектами в информационной системе или между системами (публикация-автор, автор-аффилиация и т. д.); 2) изменчивостью структуры науки,

появлением новых научных дисциплин (биотехнологии, нанотехнологий, нейроинформатики и др.), что приводит к необходимости периодической корректировки и актуализации структуры классификаторов, предполагающих трудоемкую повторную классификацию всего массива научных публикаций. Подобные операционные проблемы приводят к достаточно часто возникающим сложностям в поиске публикаций.

Рациональность и правильность классификации по конкретному основанию, ее соответствие текущим реалиям развития науки являются одним из ключевых факторов, определяющих точность результатов науко/библиометрических исследований [Мельникова 2023], проводимых на базе современных информационных систем.

Технология искусственного интеллекта позволяет в автоматизированном режиме производить классификацию данных, существенно сокращая при этом сроки классификации и повышая степень ее адекватности за счет применения различных наборов высокотехнологичных ИИ-инструментов [Ma, Liu, Xu 2021]. ИИ-технология генерирует новые подходы, позволяющие производить *постатейную* тематическую классификацию научных публикаций, что является чрезвычайно значимым фактором для современных систем индексации и цитирования научной информации. Постатейная классификация на основе искусственного интеллекта существенно повышает эффективность метрических операций и точность вычисляемых показателей, запросы по которым пользователи могут реализовать через аналитические платформы-приложения указанных систем (рис. 1).

Визуализация метрических результатов – это эффективный способ простого для восприятия автоматического представления итоговых метрических данных и лаконичного доведения до пользователя результатов метрического анализа. На современном этапе визуализацию предваряет комплексный процесс, включающий поиск, добычу, обработку и анализ больших данных, что невозможно реализовать без применения технологии искусственного интеллекта. ИИ способен представить результаты метрического анализа огромных объемов разнородных данных в виде четких и кратких визуальных графиков знаний, содержащих статические, динамические или интерактивные визуальные элементы.

Перечисленные возможности позволяют пользователям, которые обращаются к приложениям визуализации (построенным, например, на генеративных состязательных сетях *(GAN)*), получать понятное, лаконичное и при этом детальное представление: – о библиометрической информации, относящейся к публикациям,

авторам, журналам, странам, учреждениям, цитируемым ссылкам, ключевым словам и другим библиографическим категориям; – о наукометрической информации, касающейся результативности публикационной деятельности ученых, продуктивности отраслевой и национальной науки, современных и прогнозируемых трендах в науке и т. д. Следует отметить, что обращение к генеративному ИИ становится оправданным, когда речь идет об обработке больших и сверхбольших объемов данных.

Генерирование библиографии (списка литературы) – важный этап работы ученого в рамках любого исследования, включая науко/библиометрический анализ. Специализированные *генераторы библиографии (менеджеры ссылок) на основе ИИ* обладают расширенными функциями и удобным интерфейсом. Они облегчают поиск релевантных статей в базах данных и составление итоговой библиографии в конце исследования с ее форматированием в соответствии с академическими требованиями. К особенностям некоторых генераторов библиографии относится их бесшовная интеграция с рабочим процессом исследования: на одной платформе ученый может писать текст своей статьи и одновременно получать доступ к интересующим его источникам, которые автоматически заносятся в формируемую библиографию. К наиболее эффективным генераторам относят *CoWriter, Zotero, EndNote, Citation Machine, CiteMaker* и некоторые другие.

Применение искусственного интеллекта в библиометрии

Определение количества публикаций и ссылок. Показатели количества статей и цитирований (*citations*), или количества ссылок на статьи конкретного автора, являются для библиометрии основополагающими. Как было отмечено, на основе количества статей, цитирований, их сочетаний и отношений формируются различные метрические показатели и индексы. Искусственный интеллект способен помочь в оперативном определении количества публикаций и цитирований по их видам (прямых цитирований, перекрестных, самоцитирований), в поиске взаимосвязей между ними [Гиляревский 2022b; Боргоякова 2021; Арутюнов 2020] и в итоговом вычислении на базе полученных данных требуемых метрических показателей и индексов.

Идентификация авторов является одной из не решенных до конца проблем современной библиометрии. Адекватная идентификация затруднена нередко встречающимися различиями в напи-

сании имен авторов и другой информации о них в различных видах источников опубликованной научной информации, в различных базах данных, системах индексации и цитирования. Отсутствие унифицированности приводит к ошибкам в идентификации авторов и как следствие – публикаций [Abramo, D'Angelo 2023; Hain, Jurowetzki, Lee, Zhou 2023], снижая надежность и достоверность информационных подборок, формируемых для проведения библиометрического анализа.

К числу решений проблемы относится расширяющаяся практика применения глубокого машинного обучения с внешним учителем или без него. Обучение строится на принципах оптимизации исходной модели, которая является математически обобщенным представлением исследуемого массива библиометрических данных. Применение инструментов искусственного интеллекта позволяет существенно уменьшить остроту проблемы идентификации авторов и повысить адекватность информационного материала, саккумулированного для решения библиометрических задач.

Перспективные направления применения. В качестве наиболее перспективных направлений применения ИИ в библиометрии на данном этапе рассматриваются: интеллектуальный анализ текста, семантический анализ сетей соавторов, смарт-индекс цитирования и рекомендательные системы. Рекомендательные системы последнего поколения способны работать на основе специальных программ с привлечением инструментов ИИ [Hain, Jurowetzki, Lee, Zhou 2023], осуществляющих оперативное формирование адекватных, качественных выборок научных публикаций из баз данных в соответствии с запросами пользователей, в том числе – для решения библиометрических задач. Такие системы могут анализировать конкретные научные предпочтения пользователей и строить семантические прогнозы по поводу того, какие вопросы может быть рекомендовано охватить пользователям в их следующем тематически связанном запросе/исследовании.

Что касается интеллектуального анализа текста [Saeidnia, Hosseini, Abdoli 2023], то он проводится на базе ИИ-алгоритмов, которые с высокой степенью точности вычленяют в научных публикациях ключевые слова, соответствующие пользовательскому запросу, улучшая тем самым поиск адекватного информационного материала и формируя более широкую и содержательную основу для библиометрического анализа.

Применение смарт-индекса цитирования является еще одним перспективным направлением, связанным с работой алгоритмов искусственного интеллекта. В смарт-индекс встроены две интеллектуальные функции: 1) функция отображения контекста

цитирования и 2) функция классификации цитирований по их тематическому содержанию [Nicholson, Mordaunt, Lopez 2021]. Эти возможности, реализуемые на ИИ-базе, обусловливают эффективность применения смарт-индекса для оптимизации метрических исследований.

Общим для всех направлений является тезис о том, что использование инструментов и методов искусственного интеллекта приводит к совершенствованию поиска необходимой информации в базах данных, повышению ее доступности и качества обработки и в целом – к формированию более благоприятной среды для решения задач библиометрического анализа.

Применение искусственного интеллекта в наукометрии

Количественный и качественный анализ науки. Помимо областей применения ИИ, которые являются общими для двух рассматриваемых метрических дисциплин, непосредственно в наукометрии искусственный интеллект может использоваться на таких направлениях, как оценка результативности науки в целом и научной деятельности отдельных ученых. Обрабатывая массивы больших данных, искусственный интеллект на базе определения количества статей, цитирований и производных показателей способен оперативно осуществлять *качественную* оценку работы ученых – например, на основе отношения количества статей к количеству ссылок проводить анализ востребованности научных журналов, вычислять рейтинговые показатели учебно-научных заведений.

ИИ также может содействовать решению более общих наукометрических задач. С использованием инструментов глубокого обучения искусственный интеллект способен выявлять в текстовых массивах «горячие» информационные направления и темы, в рамках которых обнаруживается повышенная концентрация цитирований, свидетельствующая об особом научном интересе к ним [Saeidnia, Hosseini, Abdoli 2023]. На основании определения плотности научных коммуникаций и ее изменений ИИ также способен давать оценку прогресса или стагнации существующих и появления новых научных направлений. С использованием результатов этой оценки искусственный интеллект может создавать карты знаний. На базе анализа сети научных коммуникаций и анализа цитирований ИИ может строить прогнозы, на каких научных направлениям будет наиболее активно развиваться международное сотрудни-

чество. При этом с использованием искусственного интеллекта значительно возрастают скорость и качество обработки данных, а также формируется более объективная и надежная информационная основа для проведения наукометрических исследований.

Перспективные направления применения. Рассмотренные возможности ИИ имеют большое значение для решения таких важных задач наукометрии, как анализ актуальных трендов в развитии науки, а также – для разработки решений в сфере управления наукой, включая своевременную финансовую поддержку передовых научных направлений и идей. Оценка состояния и динамики развития сети научных коммуникаций, поиск перспективных научных направлений на основе анализа активности ученых в исследованиях по конкретным проблемам, картирование науки, прогноз ее развития и решение некоторых других комплексных наукометрических задач формируют содержание наиболее перспективных направлений применения ИИ в наукометрии, включая в том числе интеллектуальный анализ текста с использованием больших языковых моделей и обработку больших данных на основе связки глубокого обучения с состязательными и другими видами генеративных нейросетей.

Общие для наукометрии и библиометрии перспективные направления применения искусственного интеллекта, нацеленные на оптимизацию решения науко/библиометрических задач, представлены на рис. 1.

Рис. 1. Общие для наукометрии и библиометрии перспективные направления применения искусственного интеллекта

Научные разработки в области приложений искусственного интеллекта для наукометрии и библиометрии

Одна из перспективных разработок в области искусственного интеллекта, созданная индийскими учеными, посвящена автоматической классификации категории цитирования. Методика предназначена для работы с большими данными и основывается на применении глубокого машинного обучения в связке с искусственными нейросетями [Gowri 2019]. Позволяет извлекать ссылки из научных публикаций по конкретной тематике, содержащихся в какой-либо базе данных.

При разработке автоматической классификации учитывалось, что на использование в своих статьях конкретной ссылки ученых могут мотивировать разные целевые установки: подтвердить собственную гипотезу, согласиться с результатами исследования других ученых, подтвердить обоснованность постановки научной проблемы и т. д. Таких категорий может быть несколько десятков. С их учетом создаются автоматические классификаторы, функционирующие на основе специально разработанных правил для маркировки категорий цитирования с помощью меток, каждая из которых обозначает подмножество наиболее схожих признаков. Разбиение категории цитирования на классы позволяет провести более тщательный анализ ссылок, которые сделали ученые в своих статьях по конкретной тематике, оценить реальную научную значимость ссылок и влияние научных идей (на которые ссылки указывают) на развитие рассматриваемой концепции или научного направления. Результаты этих оценок позволяют сделать вывод о перспективности данного научного направления.

Другой тип ИИ-приложений для науко/библиометрических исследований основан на сравнительном анализе моделей исследуемого объекта, например, научной организации. Приложение может ответить на вопрос, какие параметры своей деятельности должна изменить организация, чтобы добиться более высокого рейтинга. Сравниваются параметры (признаки), отражающие текущее состояние организации (текущая модель), и ее возможное будущее, прогнозное состояние, к которому организация должна стремиться (прогнозная модель). Текущая модель представляет собой «взвешенную» функцию основных текущих данных (признаков), характеризующих организацию. Строится несколько прогнозных моделей до получения оптимального значения целевой переменной. Оптимизация прогнозных моделей происходит на основе анализа корреляций между признаками, влияющими на результат целевой переменной.

Заключение

В заключение следует констатировать, что широкий перечень задач наукометрического и библиометрического анализа, а также непрерывный стремительный рост массивов научной информации и формирование категории больших данных приводит к появлению объективной необходимости в новых технологических инструментах, способных предоставить поддержку решению науко/библиометрических задач в новых условиях.

К таким высокоэффективным инструментам относится искусственный интеллект, сфера применения которого неуклонно расширяется. Он обеспечивает более оперативную и качественную обработку данных, их интеллектуальный анализ, более эффективный и адекватный поиск необходимой информации в научных базах данных, более высокую точность вычисления метрических показателей и, как следствие, более надежные и содержательные результаты науко/библиометрического анализа. При этом не следует переоценивать роль искусственного интеллекта в наукометрии и библиометрии: он не может решить все проблемы, существующие в этих метрических дисциплинах, но вполне способен оптимизировать решение немалого их числа.

Благодарности

Статья выполнена в рамках исследования по теме FFFU-2021-0007 Государственного задания ВИНИТИ РАН.

Acknowledgements

The article was carried out in the framework of the research on topic FFFU-2021-0007 of the State Assignment of VINITI RAS.

Литература

Арутюнов 2020 – *Арутюнов В.В.* Наукометрические показатели исследователей-лидеров научной деятельности в области информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2020. № 2. С. 46–56.

Боргоякова 2021 – *Боргоякова К.С.* Наукометрические показатели публикационной активности российских ученых в области экологии (2016–2020 гг.) // Вестник

РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 3. С. 8–27.

Гиляревский 2022a – *Гиляревский Р.С.* Библиометрия как понимание социальных закономерностей научных коммуникаций // Труды Санкт-Петербургского гос. ин-та культуры. СПб.: СПбГИК, 2022. Т. 226. С. 15–23.

Гиляревский 2022b – *Гиляревский Р.С.* Наукометрия в научной журналистике. М.: МГУ, 2022. 134 с.

Гиляревский 2022c – *Гиляревский Р.С.* О некорректности использования индексов цитирования для вычислений по сопоставлению разделов науки // Научно-техническая информация. Сер. 2. 2022. № 2. С. 21–24.

Каптерев 2023 – *Каптерев А.И.* Когнитивный менеджмент и искусственный интеллект в библиотеках: возможности и особенности // Научные и технические библиотеки. Сер. 1. 2023. № 6. С. 113–137.

Лазарев 2022 – *Лазарев* В.С. Библиометрия, наукометрия и информетрия. Методы // Управление наукой: теория и практика. 2022. Т. 4. № 1. С. 180–201.

Мельникова 2023 – *Мельникова Е.В.* Глубокое машинное обучение в оптимизации научно-исследовательской деятельности // Научно-техническая информация. Сер. 1. 2023. № 2. С. 8–13.

Налимов 1969 – *Налимов В.В.* Наукометрия: изучение развития науки как информационного процесса. М.: Наука, 1969. 192 с.

Родионов, Цветкова, Калашникова 2025 – *Родионов И.И., Цветкова В.А., Калашникова Г.В.* Перспективы искусственного интеллекта в информационной деятельности – мнение ChatGPT / Научно-техническая информация. Сер. 1. 2025. № 1. С. 17–25.

Столяров 2022 – *Столяров Ю.Н.* Искусственный интеллект и книжная библиотечная отрасль: направления разработки проблемы // Научные и технические библиотеки. 2022. № 1. С. 17–34.

Шталь, Шредер, Родригес 2024 – *Шталь Б.К., Шредер Д., Родригес Р.* Этика искусственного интеллекта / Пер. с англ. под науч. ред. А. Павлова. М.: НИУ ВШЭ, 2024. 200 с.

Шрайберг 2024 – *Шрайберг Я.Л.* Искусственный интеллект: прошлое, настоящее и будущее – что ждет научно-образовательное и библиотечно-информационное сообщество. Пленарный доклад // 28-я Межд. конф. «LIBCOM-2024», г. Суздаль, 19–23 нояб. 2024 г. М.: ГПНТБ России, 2024. 21 с.

Цветкова, Мохначева 2021 – *Цветкова В.А., Мохначева Ю.В.* Влияние качества библиографического описания на библиометрические оценки // Библиосфера. 2021. № 2. С. 59–64.

Abramo, D'Angelo 2023 – *Abramo G., D'Angelo C.A.* How reliable are unsupervised author disambiguation algorithms in the assessment of research of organisation performance? // Quantitative Science Studies. 2023. Vol. 4. № 1. P. 1–26.

Asiakin 2021 – *Asiakin N. et al.* Exploring big data traits and data quality dimensions for big data analytics application // Journal of Big Data. Springer Science and Business Media. 2021. № 8. P. 1–15.

Bircan, Salah 2022 – *Bircan T., Salah A.A.* Bibliometric Analysis of the Use of Artificial Intelligence Technologies for Social Sciences // Mathematics. 2022. Vol. 10. № 23. P. 43–54.

Garfild 1964 – *Garfild E.* "Science citation index" – a new dimension in indexing // Science. 1964. Vol. 144. P. 649–654.

Gowri 2019 – *Gowri.S.* Relevance of Innovations in Machine Learning to Scientometrics // Journal of Scientometric Research. 2019. № 8 (2). P. 39–43.

Hain, Jurowetzki, Lee, Zhou 2023 – *Hain D, Jurowetzki R, Lee S, Zhou* Y. Machine learning and artificial intelligence for science, technology, innovation mapping and forecasting: Review, synthesis, and applications // Scientometrics. 2023. Vol. 128. № 3. P. 1465–1472.

Li, Duan 2023 – *Li M, Duan W. et al.* The Evolution of AI Dependency in Scientometric Research // University of Illinois Digital Library (IDEALS Library), 2023. 11 p. URL: https://www.ideals.illinois.edu/ (дата обращения 14.01.2025).

Ma, Liu, Xul 2021 – *Ma A, Liu Y, Xu X et al.* A deep-learning based citation count prediction model with paper metadata semantic features // Scientometrics. 2021. Vol. 26. № 8. P. 6803–6823.

Melnikova 2024 – *Melnikova E.V.* Relevance of Application of Artificial Intelligence Toolkit in Modern Scientometric Research // Scientific and Technical Information Processing. 2024. Vol. 51. № 1. P. 57–63.

Mitha, Omarsaib 2024 – *Mitha S.B., Omarsaib M.* Emerging technologies and higher education libraries: a bibliometric analysis of the global literature // Library Hi Tech (LHT). Leeds: Emerald Publishing Ltd., 2024. DOI: 10.1108/LHT-02-2024-0105.

Nicholson, Mordaunt, Lopez 2021 – *Nicholson J.M., Mordaunt M., Lopez P. et al.* A smart citation index that displays the context of citations and classifies their intent using deep learning // Quantitative Science Studies. 2021. Vol. 2. № 3. P. 882–898.

Saeidnia., Hosseini, Abdoli 2023 – *Saeidnia H.R., Hosseini E., Abdoli S. et al.* Unleashing the power of AI: a systematic review of cutting-edge techniques in AI-enhanced scientometrics, webometrics and bibliometrics // Library Hi Tech (LHT). Leeds: Emerald Publishing Ltd., 2023. DOI: 10.1108/LHT-10-2023-0514.

Waltman, Boyack 2020 – *Waltman L., Boyack K.W., Colavizza G., van Eck N.J.* A principled methodology for comparing relatedness measures for clustering publications // Quantitative Science Studies. 2020. Vol. 1 (2). P. 691–713.

Zhao, Feng 2022 – *Zhao Q, Feng X.* Utilizing citation network structure to predict paper citation counts: A Deep learning approach // Journal of Informetrics. 2022. Vol. 16. № 2. P. 1012–1035.

References

Abramo, G. and D'Angelo, C.A. (2023), "How reliable are unsupervised author disambiguation algorithms in the assessment of research of organisation performance?", *Quantitative Science Studies*, vol. 4, no. 1, pp. 1–26.

Arutyunov, V.V. (2020) "Scientometric indicators for leaders in the scientific research of the information security", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 46–56.

Asiakin, N. (2021), "Exploring big data traits and data quality dimensions for big data analytics application", *Journal of Big Data, Springer Science and Business Media*, no. 8, pp. 1–15.

Bircan, T. and Salah, A.A. (2022), "Analysis of the Use of Artificial Intelligence Technologies for Social Sciences", *Mathematics*, vol. 10, no. 23, pp. 43–54.

Borgoyakova, K.S. (2021), "Scientometric indices of the publication activity of Russian scientists in the field of ecology (2016–2020)", *RSUH/RGGU Bulletin. "Informatics. Information Security. Mathematics" Series*, no. 3, pp. 8–27.

Garfild, E. (1964), "Science citation index" – a new dimension in indexing", *Science*, vol. 144, pp. 649–654.

Gilyarevskii, R.S. (2022a), "Bibliometrics as an understanding of the social patterns of scientific communications", *Proceedings of the St. Petersburg State Institute of Culture*, vol. 226, pp. 15–23.

Gilyarevskii, R.S. (2022b), *Naukometriya v nauchnoi zhurnalistike* [Scientometrics in Science Journalism], MSU, Moscow, Russia, 134 p.

Gilyarevskii, R.S. (2022c), "On the incorrectness of using citation indexes for calculations comparing sections of science", *Scientific and Technical Information. Ser. 2*, no. 2, pp. 21–24.

Gowri, S. (2019), "Relevance of Innovations in Machine Learning to Scientometrics", *Journal of Scientometric Research*, no. 8 (2), pp. 39–43.

Hain, D., Jurowetzki, R., Lee, S. and Zhou, Y. (2023), "Machine learning and artificial intelligence for science, technology, innovation mapping and forecasting: Review, synthesis, and applications", *Scientometrics*, vol. 128, no. 3, pp. 1465–1472.

Kapterev, A.I. (2023), "Cognitive management and artificial intelligence in libraries: opportunities and features", *Scientific and Technical Libraries*, no. 6, pp. 113–137.

Lasarev, V. (2022), "Bibliometrics, scientometrics, and informetrics. Methods", *Management of science: theory and practice*, vol. 4, no. 1 pp. 180–201.

Ma, A., Liu, Y. and Xu, X. et al (2021), "A deep-learning based citation count prediction model with paper metadata semantic features", *Scientometrics*, vol. 26, no. 8, pp. 6803–6823.

Melnikova, E.V. (2023), "Deep machine learning in optimizing research activities", *Scientific and Technical Information. Ser. 1*, no. 2, pp. 8–13.

Melnikova, E.V. (2024), "Relevance of Application of Artificial Intelligence Toolkit in Modern Scientometric Research", *Scientific and Technical Information Processing, Springer Nature*, vol. 51, no. 1, pp. 57–63.

Mitha, S.B. and Omarsaib, M. (2024), "Emerging technologies and higher education libraries: a bibliometric analysis of the global literature", *Library Hi Tech (LHT)*, Emerald Publishing Ltd, February, Leeds, UK, DOI: 10.1108/LHT-02-2024-0105.

Li, M. and Duan, W et al. (2023), "The Evolution of AI Dependency in Scientometric Research", *University of Illinois Digital Library (IDEALS Library), 11 p*, available at: https://www.ideals.illinois.edu/ (Accessed 14.01.2025).

Nalimov, V. (1969), *Naukometriya: izuchenie razvitiya nauki kak informatsionnogo protsessa* [Scientometry: the study of the development of science as an information process], Nauka, Moscow, Russia, 192 p.

Nicholson, J.M., Mordaunt, M. and Lopez P. et al. (2021), "A smart citation index that displays the context of citations and classifies their intent using deep learning", *Quantitative Science Studies*, vol. 2, no. 3, pp. 882–898.

Rodionov, I.I. Tsvetkova, V.A. and Kalashnikova, G.V. (2025), "Prospects of artificial intelligence in information activity – opinion of ChatGPT", *Scientific and Technical Information. Ser. 1*, no. 1, pp. 17–25.

Saeidnia, H.R., Hosseini, E. and Abdoli, S. (2023), "Unleashing the power of AI: a systematic review of cutting-edge techniques in AI-enhanced scientometrics, webometrics and bibliometrics", *Library Hi Tech (LHT)*, Emerald Publishing Ltd, Leeds, UK, DOI: 10.1108/LHT-10-2023-0514.

Shraiberg, Ya.L. (2024), "Artificial intelligence: past, present and future – what awaits the scientific, educational, library and information community", *28th International Conference "LIBCOM-2024"*, Suzdal', 19–23 Nov., Russian National Public Library for Science and Technology, Moscow, Russia, 21 p.

Stahl, B.K., Schroeder, D. and Rodriguez, R. (2024), *Etika iskusstvennogo intellekta* [Ethics of Artificial Intelligence], Pavlov, A. (transl. from English, ed.), National Research University "Higher School of Economics", Moscow, Russia, 200 p.

Stolyarov, Y. (2022), "Artificial intelligence and the book library industry: areas of problem development ", *Scientific and Technical Libraries*, no. 1, pp. 17–34.

Tsvetkova, V.A and Mokhnacheva, Y.V. (2021), "The influence of the quality of the bibliographic description on bibliometric estimates", *Bibliosphere*, no. 2, pp. 59–64.

Waltman, L. and Boyack, K.W. (2020), "A principled methodology for comparing relatedness measures for clustering publications", *Quantitative Science Studies*, no. 1 (2), pp. 691–713.

Zhao, Feng (2022), "Utilizing citation network structure to predict paper citation counts: A Deep learning approach", *Journal of Informetrics*, vol. 16, no. 2, pp. 1012–1035.

Информация об авторах

Елена В. Мельникова, кандидат технических наук, старший научный сотрудник, ВИНИТИ РАН, Москва, Россия; 125315, Россия, Москва, ул. Усиевича, д. 20; verden.mel@yandex.ru

Валентина А. Цветкова, доктор технических наук, профессор, главный научный сотрудник, ВИНИТИ РАН, Москва, Россия; 125315, Россия, Москва, ул. Усиевича, д. 20; vats08@mail.ru

Information about the authors

*Elena V. Melnikov*a, Cand. of Sci. (Mechanical Engineering), senior researcher, VINITI RAS, Moscow, Russia; bld. 20, Usievich Str., Moscow, 125315, Russia; verden. mel@yandex.ru

Valentina A. Tsvetkova, Dr. of Sci. (Mechanical Engineering), professor, chief resear-cher, VINITI RAS, Moscow, Russia; bld. 20, Usievich Str., Moscow, 125315, Russia; vats08@mail.ru

УДК 004:37.018
DOI: 10.28995/2686-679X-2025-2-41-53

Информационное взаимодействие в современных системах дистанционного обучения

Валерий В. Муромцев
Национальный исследовательский технологический университет «МИСИС», Москва, Россия,vvm44@inbox.ru

Анна В. Муромцева
Российский государственный гуманитарный университет, Москва, Россия;
Национальный исследовательский технологический университет «МИСИС», Москва, Россия, anmur37@yandex.ru

Аннотация. Дистанционное обучение (ДО) сегодня стало естественной частью всей системы образования и активно используется как форма обучения на всех ее уровнях. В высшей школе она применяется при повышении квалификации, дополнительных курсах, и все больше вузов предлагают ее как один из вариантов заочного обучения. Виртуальное пространство, в котором собственно и проводится ДО, сформировалось буквально за одно десятилетие и сегодня невозможно представить мир без него. Изменения коснулись практически всей жизни человека. Это повседневная деятельность, обучение, работа и практически все сегодня охвачено виртуальным пространством, в котором мы живем наряду с реальным физическим пространством, окружающим нас. Современные технологии ДО активно используют новую технологическую базу и открывающиеся в связи с этим возможности. Актуальность рассмотрения сегодняшнего состояния ДО связана прежде всего с новыми информационными технологиями представления информации и с использованием в процессе обучения искусственного интеллекта, применение которых формирует как новые возможности, так и информационные риски. Авторы неоднократно обращались к тематике ДО и результаты этой работы представлены в целом ряде публикаций.

Ключевые слова: дистанционное обучение (ДО), нейросети, искусственный интеллект, виртуальная коммуникация, экранное восприятие информации, видеообраз, эффективность обучения

Для цитирования: Муромцев В.В., Муромцева А.В. Информационное взаимодействие в современных системах дистанционного обучения // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 2. С. 41–53. DOI: 10.28995/2686-679X-2025-2-41-53

Information interaction in modern distance learning systems

Valerii V. Muromtsev
National University of Science and Technology "MISIS", Moscow, Russia, vvm44@inbox.ru

Anna V. Muromtseva
Russian State University for the Humanities, National University of Science and Technology "MISIS", Moscow, Russia, anmur37@yandex.ru

Abstract. Distance learning (DL) has become a natural part of the entire educational system and is actively used as a form of training at all its levels. In higher education, it is used for advanced training, additional courses, and more and more universities offer it as one of the options for correspondence courses. The virtual space in which DL is actually conducted has formed in literally one decade and today it is impossible to imagine a world without it. Changes have affected almost all of a person's life. That is everyday activity, training, work and almost everything today is covered by the virtual space in which we live along with the real physical space surrounding us. Modern DL technologies actively use the new technological base and the opportunities that open up in that regard. The relevance of considering the current state of DL is primarily associated with new information technologies for presenting information and with the use of artificial intelligence in the learning process, the use of which creates both the new opportunities and information risks. The authors have repeatedly addressed the topic of DL and the results of that work are presented in a number of publications.

Keywords: distance learning (DL), neural networks, artificial intelligence, virtual communication, screen-based information perception, video image, learning efficiency

For citation: Muromtsev, V.V. and Muromtseva, A.V. (2025), "Information interaction in modern distance learning systems", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 2, pp. 41–53, DOI:

Дистанционное обучение (ДО) сегодня довольно популярно. Оно активно применяется как форма обучения при повышении квалификации, дополнительных курсах, и все больше вузов предлагают ее как один из вариантов заочного обучения. ДО используется давно и сегодня претерпело существенные изменения, связанные с новой технологической базой и открывающимися благодаря

этому возможностями. Актуальность рассмотрения сегодняшнего состояния ДО связана прежде всего с новыми информационными технологиями предоставления информации и с использованием в процессе обучения систем искусственного интеллекта, применение которых формирует новые информационные риски.

Основной целью настоящего исследования является анализ современного состояния ДО и, прежде всего, тех изменений, которые в последнее время возникли под влиянием стремительно развивающихся информационных технологий, прежде всего систем искусственного интеллекта (ИИ).

В своей основе ДО содержит как гуманитарный, так и технический аспекты, что требует использование при анализе междисциплинарного системного подхода, в рамках которого следует обратить внимание на их взаимное влияние. Так, например, использование видеоконференций расширило возможности представления информации и, как следствие, повысило эффективность обучения. Применение систем ИИ позволит проводить занятия с учетом индивидуальных особенностей студентов [Муромцев 2010] и т. д.

Дистанционное обучение сегодня обладает рядом особенностей, которые позволяют выделить его в особую группу. Сочетание традиционных форм обучения и современных технических средств, а также взаимодействие между объектами в виртуальном пространстве с использованием виртуальных коммуникаций дает ему довольно широкие возможности как в рамках взаимодействия между участниками, так и в рамках воздействия на них.

Объектом управления при любом виде обучения является коллектив обучаемых, который представляет собой динамическую систему с изменяющимися характеристиками, причем в начальный момент эти характеристики, как правило, не известны. Изменения характеристик системы зависит от целого ряда факторов: состава обучаемых, качества виртуальной коммуникации, вида представляемой информации и т. д.

Дистанционное обучение, как и традиционная форма обучения, реализует процесс информационного управления, т. е. формирует отношение обучаемого к представляемой информации [Архипова 2013]. Данный процесс является очень важным, без него невозможно реализовать качественное обучение.

Так как ДО сегодня является обучением в виртуальном пространстве с использованием виртуальной коммуникации, следовательно, необходимо учитывать законы виртуального пространства.

Основные свойства виртуальной коммуникации были определены авторами в работе [Муромцев, Муромцева 2010]. При этом необходимо отметить, что ДО осуществляет снижение объемов

предоставляемой информации[1] [Муромцев, Муромцева 2010], которое может быть частично компенсировано за счет использования дополнительных информационных технологий.

Для современного молодого поколения характерно экранное восприятие информации[2] [Муромцев, Муромцева 2010]. Информация, представленная не в виде видеообраза, воспринимается с трудом. Чтение и речь перестают играть ведущую роль при восприятии и обработке (обдумывании) информации. Для них видеообраз – основной источник информации, который и остается в памяти. Если требуется, используя логическое мышление, сформировать образ объекта, часто возникают затруднения.

Из-за отсутствия вариативности появляется четкая однозначная трактовка представляемой информации. Этому способствуют и социальные сети, которые поддерживают такую направленность, завлекая молодежь интересными, смешными, шокирующими и подобными роликами[3].

Возможность оперативно получать информацию из сети Интернет приводит к нежеланию запоминать информацию, с одной стороны. С другой – при большом потоке информации, который обрабатывает сегодня мозг современного человека, происходит когнитивная его перегрузка, что приводит к различным видам истощения человека (физическому, психологическому)[4] и к снижению работоспособности, а иногда и выгоранию.

Привычка к доступности информации уменьшает объем памяти и снижает мыслительные способности человека [Сердюкова 2021]. Это приводит к лавинообразным процессам изменения роли человека как лидера современного социума, который сегодня состоит не только из людей реального мира, но и из виртуальных сущностей, которые становятся идеалами для молодежи. На них стремятся походить, несмотря на то, что они существуют только в виртуальном пространстве или являются героями мультфильмов. Не задумываются и о том, что многое невозможно сделать в реальной жизни или такого просто не существует.

---

[1] Обучение в новой нормальности: вызовы и ответы. Аналитический отчет, (2020). М.: АНО ДПО «Корпоративный университет Сбербанка», 2020. С. 71: ил., табл.

[2] Там же.

[3] Зависимость от социальных сетей: что это и как с ней бороться (2022) // Макхост. URL: https://mchost.ru/articles/zavisimost-ot-socialnyh-setej/ (дата обращения 24.10.24).

[4] Когнитивная перегрузка (2024) // Википедия. URL: https://ru.wikipedia.org/wiki/Когнитивная_перегрузка (дата обращения 24.10.2024).

Коммуникация между учителем и учениками в традиционном обучении, которое реализуется в реальном пространстве, осуществляется с помощью органов чувств человека при восприятии информации, а также вербальными и не вербальными символами при представлении информации. При ДО в традиционную схему коммуникации включается дополнительный элемент в виде специального не контролируемого технического канала связи. Он и вносит те изменения, которые приводят за счет технических особенностей к снижению качества коммуникации и невозможности трансляции части информации от других органов чувств (запах, тактильные ощущения).

Стремление устранить этот недостаток привело к созданию новых информационных технологий, которые обеспечили целый ряд возможностей представления и восприятия информации[5] [Kononov, Muromtsev, Murontseva 2022; Khomich 2022].

Прежде всего это системы видеоконференций, такие как Zoom, MS Teams, Skype, Videomost, ClickMeeting и другие, позволяющие реализовать звуковой и визуальный контакт между преподавателями и обучаемыми, возможность использовать презентации и осуществлять контроль за процессом обучения.

В свою очередь, использование новых информационных технологий в ДО приводит к зависимости предоставляемой информации от пожеланий создателей этих технологий и часто не зависит от обучающего. Это создает определенные угрозы информационному управлению обучением.

Необходимо отметить, что большинство открыто используемых современных систем ДО (Zoom, MS Teams, Skype, Videomost, ClickMeeting и другие) работают в сети Интернет и практически не защищены от несанкционированного доступа как владельцев или правообладателей, так и из вне [Гришина 2022; Гришина 2024]. Часть из них открыто декларируют, что вся информация записывается в западных облачных хранилищах. На основе этих данных легко просчитать, смоделировать любого человека, участвующего в сеансе ДО. Разработанные алгоритмы для обработки больших данных позволяют это сделать. А современные моде-

[5] Обучение во времена ИИ: какие нейросети использовать в образовании (2023) // АНО ДПО «Корпоративный университет Сбербанка». URL: https://sberuniversity.ru/edutech-club/pulse/tekhnologii/36438/ (дата обращения 27.07.2023); Журнал EduTech. Групповая работа: как обеспечить эффективное взаимодействие? (2024) // АНО ДПО «Корпоративный университет Сбербанка». URL: https://sberuniversity.ru/edutech-club/journals/32924/ (дата обращения 27.07.2023).

лирование с помощью нейронных сетей и видеозаписей создать видео-двойника. Он будет говорить вашим голосом, держаться и двигаться так, как вы, но при этом транслировать информацию, необходимую заказчику[6].

Известно, что эффективность обучения зависит от подготовленности аудитории к восприятию информации. Что касается очного обучения, то происходит постоянная корректировка тезауруса обучаемых преподавателем, который в процессе занятия контролирует усвоение материала. В ДО это организовать сложно. На подготовленность студентов повлияли не только те знания, что они получили ранее, но и их общение в социальных сетях, мессенджерах и т. д. То есть здесь можно говорить обо всем опыте их взаимодействия в виртуальном пространстве. Привычка получать информацию и не акцентировать свое внимание на ней делает процесс обучения весьма сложным и не всегда продуктивным.

В настоящее время активно реализуется внедрение искусственного интеллекта в процессы обучения.

Создание сильного искусственного интеллекта приведет к еще большему уменьшению роли человека в современном мире. Уже сегодня нейронные сети активно используются студентами при подготовке текстов курсовых и дипломных работ, политические деятели используют нейросети для написания текстов выступлений, многие применяют нейросети при создании научных публикаций и т. д. Интернет пестрит предложениями создания различных рисунков и образов на основе словарного описания[7]. Человек перестает мыслить, фантазировать. За него предлагают это сделать. Кроме всего прочего, современная реклама, телевидение, социальные сети подсказывают ему модель поведения.

Платформа Omdena опубликовала исследование «Лидеры по внедрению искусственного интеллекта», в котором представлены платформы онлайн-обучения с курсами ведущих университетов и преподавателей со всего мира – 50 EdTech-платформ[8], активно

---

[6] Не верь глазам своим. Специальный репортаж ТВЦ. К чему приведет развитие нейросетей? 27.02.2023 // ТВЦ. URL: https://yandex.ru/video/touch/preview/1363407030013542256 (дата обращения 03.09.2024).

[7] *Кульгин М.* 13 Лучших ИИ программ для написания текстов в 2023 году (сравнение) // Дзен. URL: https://dzen.ru/a/ZGOLJIGbjDXQzA8M (дата обращения 14.11.2024).

[8] Групповая работа: как обеспечить эффективное взаимодействие? (2024) // Журнал EduTech. URL: https://sberuniversity.ru/edutech-club/journals/32924/ (дата обращения 27.07.2023).

использующие ИИ-технологии. Наиболее интересные из них представлены в табл. 1.

Таблица 1

Лидеры по внедрению искусственного интеллекта

Наименование	Назначение платформы	Использование ИИ
Carnegie Mellon University	Платформа для обучения Университета Карнеги–Меллона	Содержит учебные курсы на базе ИИ для персонализации обучения
Packback	Дискуссионная платформа для курсов в колледже	Управляется ИИ, обеспечивает персонализированную обратную связь
Cognii	Платформа-помощник	Использует ИИ, предоставляет персонализированную обратную связь и коучинг
Amira Learning	Помощник обучения чтению	Реализована на базе ИИ. Слушает чтение вслух, оценивает уровень и дает отклик
Classcraft	Образовательная онлайн-игра для любой программы, в которую учителя и ученики играют вместе	Использует ИИ
Osmo	Система ускоренного обучения на основе игр	Использует ИИ. Сочетает физическое взаимодействие с цифровым опытом

Развитию ДО уделяет большое внимание Сбер. Журнал Edu Tech, выпускаемый Сбером, затрагивает различные аспекты обучения, а первые номера 2023 г. были посвящены обеспечению эффективного взаимодействия между преподавателем и студентами и между членами виртуального обучения. Кроме того, Сбер Университет предлагает в обучении использовать различные нейросети (Yandex GPT, Humata AI, Kandinsky 3.1 by Sber, Curipod AI и др.)[9], дополненную или виртуальную реальность для повышения эффек-

[9] Обучение во времена ИИ: какие нейросети использовать в образовании (2023) // Журнал EduTech. URL: https://sberuniversity.ru/edutech-club/pulse/tekhnologii/36438/ (дата обращения 27.07.2023).

тивности обучения и для облегчения ряда рутинных процессов[10] [Khomich 2022]. Однако с точки зрения организаторов и создателей этих сетей процесс работы над презентацией может казаться рутиной, как и поиск ответов на поставленный вопрос, а с точки зрения обучения это те элементы, которые помогают ученику глубже понять тему, разобраться в ней. Поэтому использование нейросетей в обучении необходимо для изучения их возможностей, в качестве отработки ряда практических навыков, но не как инструмент для уклонения от самостоятельной исследовательской и творческой деятельности.

Отметим, что в настоящее время в ДО используются западные платформы с ИИ. В России имеются определенные наработки в этой области, но широкого применения они не нашли. Это положение создает определенные риски в области информационной безопасности и рыночных предложений.

Сегодня есть большой срез нейронных сетей, которыми мы пользуемся и не задумываемся о достоверности информации. Имеется в виду – рекомендательные системы, которые предлагают те или иные товары или услуги на основе рекомендаций, полученных поисковыми системами на сайтах организаций-продавцов. Эти системы действуют и при поиске информации об обучении.

Другим важным элементом нейронных сетей, на который следует обратить внимание, является достоверность информации, внедренной в систему. Конечно, Интернет является достаточно большой базой с текстовой, звуковой и видеоинформацией. Однако неизвестно, на какой части этой базы обучалась та или иная нейросеть. Соответственно, какие посылы получат учащиеся, что за информация будет внедрена в их умы – неизвестно. Поэтому прежде чем использовать технологии ИИ, следует внимательно изучить базы данных, на основании которых они были созданы.

В настоящее время осуществляется переход с зарубежного программного обеспечения на отечественное. Это направление является одним из приоритетных при переходе к цифровой экономике. Из существующих российских ОС можно выделить Astra Linux с различными степенями защиты, РОСА, для поддержки серверов, рабочих станций и создания серверных программных продуктов, Uncom OS, Альт (Alt Linux), интеграция с большим количеством

[10] На чем строится совместное обучение в виртуальном пространстве – EduTech Club, (2024) // Журнал EduTech. URL: https://sberuniversity.ru/edutech-club/pulse/tekhnologii/42177/?utm_source=email&utm_medium=organic&utm_campaign=edutech-digest&utm_content=edutech-digest&utm_term=06-05-2024 (дата обращения 06.05.2024).

разных устройств, AlterOS и др. Выделяют еще целый блок систем, который позволяет решать задачи с помощью облачных технологий за счет виртуальных ОС, рабочих столов, корпоративных ИТ-платформ (RAIDIX, VeiL от НИИ «Масштаб»)[11]. С точки зрения авторов наиболее интересной представляется ОС Astra Linux за счет продуманной защиты данных, встроенного офиса и компиляции со многими российскими СЭД.

Кроме того, основываясь на существующих кросс-платформенных решениях[12], можно сказать, что часто неважно, какая ОС используется в ДО как с передающей, так и с получающей стороны, важно ее наличие и имеющийся выход в Интернет. Далее в рамках либо платформы обучения, либо облачных технологий возможно получить требуемое программное обеспечение.

Отметим, что в настоящее время осуществляется цифровое давление на социум во всех его проявлениях. Это представляет собой новый этап в формировании современного информационного пространства, в котором сочетаются формы психоинформационного воздействия с психологией толпы и прямым технологическим терроризмом. Поэтому с позиций информационной безопасности [Kononov, Muromtsev, Murontseva 2022; Муромцев, Немцова 2014; Макаренко 2017][13] следует осмотрительно использовать современные информационные технологии для студентов первых курсов, а особенно школьников. У большинства из них еще не сформирована жизненная позиция, основные ценности. С помощью информации, получаемой по различным виртуальным каналам, им может быть предоставлены недостоверные сведения или скрытно реализовано информационное воздействие, что в результате может привести к различным деструктивным последствиям, примером которых являются события, происходящие на Украине.

В заключение обратим внимание на то, что сегодня настало время разрабатывать новые подходы к эффективному и безопасному обучению, развивая междисциплинарные инновационные комплексы, ориентированные на последние достижения науки

---

[11] Российское ПО и отечественные операционные системы (2024) // Сайт АО «Карма Групп». URL: https://www.karma-group.ru/import-substitution/russian-software/ (дата обращения 11.04.2024).

[12] Там же.

[13] *Витер М.* Информационная безопасность при дистанционном обучении // Студенческий справочник. URL: https://spravochnick.ru/informacionnaya_bezopasnost/informacionnaya_bezopasnost_pri_distancionnom_obuchenii/#informacionnaya-bezopasnost-pri-distancionnom-obuchenii (дата обращения 21.04.2024).

в области коммуникаций человек – человек, человек – машина и направленные на эффективную подготовку специалистов в передовых областях науки и производства.

Появление и активное продвижение систем ИИ во все области деятельности человека, в частности в ДО, требуют изменений всех подходов к технологиям обучения. Прежде всего это учет новых возможностей систем ДО и новых условий, которые сегодня выдвигает окружающая среда.

Подводя итоги, при подготовке и проведении ДО следует обратить внимание на следующие факторы:

- обучение ведется в виртуальном пространстве и следует учитывать законы этого пространства;
- у большинства обучающихся преобладает экранное восприятие информации;
- большой поток информации может привести к когнитивной перегрузке человека;
- привычка к доступности информации уменьшает объем памяти и снижает мыслительные способности человека, что влияет на его способность к принятию решений;
- при ДО включается дополнительный элемент в виде специального не контролируемого технического канала связи;
- большинство открыто используемых современных систем ДО практически не защищены от несанкционированного доступа как владельцев или правообладателей, так и из вне;
- современные моделирование с помощью нейронных сетей и видеозаписей позволяет создать видеодвойника. Поэтому видеозаписи сеансов должны храниться специальным образом.

При использовании нейронных сетей следует обратить внимание на достоверность информации, на которой обучалась система.

С помощью инструментов, используемых в ДО, возможно как психоинформационное воздействие на человека, так и прямой технологический терроризм.

Новые технологии несут не только положительные изменения, но и угрозы, связанные с негативным информационном управлении. Знания, умения, настрой и посылы, которые получат ученики, будет переданы следующим поколениям. Поэтому к применению тех или иных новых технологий в обучении, в частности систем ИИ, нужно относится с должным вниманием и осторожностью.

Литература

Архипова 2013 – *Архипова Н.И., Кульба В.В., Косяченко С.А., Шелков А.Б.* Информационный менеджмент: учебное пособие для вузов. М.: Экономика, 2013. 749 с.

Гришина 2022 – *Гришина Н.В.* Анализ динамики утечки персональных данных в условиях реализации программы «Цифровая экономика Российской Федерации» // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 4. С. 34–43.

Гришина 2024 – *Гришина Н.В.* Анализ подходов к расследованию инцидентов информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 2. С. 73–82.

Макаренко 2017 – *Макаренко С.И.* Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века: Монография. СПб.: Наукоемкие технологии, 2017. 546 с.

Муромцев 2010 – *Муромцев В.В.* Использование информационных психотехнологий в дистанционном обучении // Проблемы управления безопасностью сложных систем: Труды XVIII Международной конференции, Москва, декабрь 2010 г. / Под ред. Н.И. Архиповой, В.В. Кульбы. М.: РГГУ, 2010. С. 531–533.

Муромцев, Муромцева 2010 – *Муромцев В.В., Муромцева А.В.* Основные свойства виртуальных коммуникаций // Проблемы регионального и муниципального управления. Сборник докладов международной научной конференции. М.: РГГУ, 2010. С. 51–53.

Муромцев, Немцова 2014 – *Муромцев В.В., Немцова С.Р.* Проблемы психоинформационной безопасности в современном информационном пространстве // Информационные войны. 2014. № 2. С. 73–80.

Сердюкова 2021 – *Сердюкова Е.А.* Влияние интернета и социальных сетей на жизнь современного человека // Science Time. 2021. № 12 (96). С. 57–61.

Khomich 2022 – *Khomkich A.* The Future Of VR In Education: Full Immersion In Learning // ARPost. URL: https://arpost.co/2022/04/28/vr-in-education-full-immersion-learning/ (дата обращения 23.08.2023).

Kononov, Muromtsev, Murontseva 2022 – *Kononov D., Muromtsev V., Murontseva A.* Telecommunication Distance Education Systems: New Perspectives // Proceedings of the 2nd International Conference on Technology Enhanced Learning in Higher Education (TELE 2022), Lipetsk, Russia. New York, NY: IEEE, 2022. P. 83–87.

References

Arhipova, N.I., Kulba, V.V., Kosyachenko, S.A. and Shelkov, A.B. (2013), *Informatsionnyi menedzhment: uchebnoe posobie dlya vuzov* [Information management. A textbook for universities], Ekonomika, Moscow, Russia, 749 p.

Grishina, N.V. (2022), "Analysis of the dynamics of personal data leakage in the context of the implementation of the program 'Digital Economy of the Russian Federation' ", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 4, pp. 34–43.

Grishina, N.V. (2024), "Analysis of approaches to investigating information security incidents", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 73–82.

Khomich, A. (2022), "The Future Of VR In Education: Full Immersion In Learning", *ARPost,* available at: https://arpost.co/2022/04/28/vr-in-education-full-immersion-learning/ (Accessed 23 August 2023).

Kononov, D., Muromtsev, V. and Muromtseva, A. (2022), "Telecommunication Distance Education Systems: New Perspectives", *Proceedings for the 2nd International Conference on Technology Enhanced Learning in Higher Education (TELE 2022),* Lipetsk, Russia, IEEE, New York, NY, USA, pp. 83–87.

Makarenko, S.I. (2017), *Informatsionnoe protivoborstvo i radioelektronnaya bor'ba v setetsentricheskikh voinakh nachala XXI veka: Monografiya* [Information warfare and electronic warfare in the network-centric wars of the early 21st century. Monograph], Naukoemkie tehnologii, St. Petersburg, Russia, p. 546.

Muromtsev, V.V. (2010), "The use of information psychotechnologies in distance learning", *Proc. of the 18th International Conference "Security management issues of complex systems"*, December 2010, RSUH, Moscow, Russia, pp. 531–533.

Muromtsev, V.V. and Muromtseva, A.V. (2010), "Basic properties of virtual communications", *Coll. of reports of the International Scientific Conference "Issues of regional and municipal management"*, RSUH, Moscow, Russia, pp. 51–53.

Muromtsev, V.V. and Nemtsova, S.R., (2014), "Issues of psychoinformation safety in modern information space", *Information Wars*, no. 2, pp. 73–80.

Serdyukova, E.A., (2021), "The influence of the Internet and social networks on the life of a modern person", *Science Time,* no. 12 (96), pp. 57–61.

Информация об авторах

Валерий В. Муромцев, кандидат технических наук, Национальный исследовательский технологический университет «МИСИС», Москва, Россия; 119049, Россия, Москва, Ленинский пр-кт, д. 4, стр. 1; vvm44@inbox.ru

Анна В. Муромцева, кандидат филологических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6;

Национальный исследовательский технологический университет «МИСИС», Москва, Россия; 119049, Россия, Москва, Ленинский пр-кт, д. 4, стр. 1; anmur37@yandex.ru

Information about the authors

Valerii V. Muromtsev, Cand. of Sci. (Mechanical Engineering), National University of Science and Technology "MISIS", Moscow, Russia; bldg. 1, bld. 4, Leninsky Av., Moscow, 119049, Russia; vvm44@inbox.ru

Anna V. Muromtseva, Cand. of Sci. (Philology), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, 125047, Russia;

National University of Science and Technology "MISIS", Moscow, Russia; bldg. 1, bld. 4, Leninsky Av., Moscow, 119049, Russia; anmur37@yandex.ru

УДК 004.925
DOI: 10.28995/2686-679X-2025-2-54-68

Метод генеративной дискриминации для эффективного предобучения языковых моделей

Андрей П. Титов
МИРЭА – Российский технологический университет,
Москва, Россия, titov_and@mail.ru

Аннотация. В статье представлен исследовательский подход к задачам обработки естественного языка (NLP), который позволяет существенно снизить затраты на вычислительные ресурсы. Основной инновацией этого метода является обучение модели не только умению заполнять пробелы, но и анализу ошибок подставляемого текста, что способствует более глубокому пониманию языковых структур и нюансов. Предобучение языковых моделей стало одним из ключевых направлений в области обработки естественного языка, что существенно улучшило качество выполнения задач, таких как классификация текста, ответы на вопросы и генерация текста. В статье представлен подробный анализ метода ELECTRA (Efficiently Learning an Encoder that Classifies Token Replacements Accurately), рассмотрены его особенности и преимущества по сравнению с традиционными методами предобучения BERT и GPT. Метод ELECTRA представляет собой инновационный подход к задаче предобучения, который опирается на концепцию генеративной дискриминации. Предлагаемый подход позволяет модели получить глубокие представления из данных, поскольку обучение дискриминатора происходит на уровне токенов, что делает его более чувствительным к контексту. Главным преимуществом ELECTRA является рациональное использование вычислительных ресурсов. Генеративный подход и способность дискриминатора учиться на больших объемах данных позволяют методу достигать результаты, используя меньшие вычислительные затраты по сравнению с другими моделями. Это делает его более доступным для исследователей и разработчиков, у которых могут быть ограничения по аппаратному обеспечению. Метод эффективно использует контекстные зависимости, что позволяет учитывать семантические связи между словами и фразами. В отличие от других моделей при обучении на ограниченных наборах данных, ELECTRA, за счет своего уникального подхода к дискриминации, помогает сохранять баланс между обучением и проверкой. В статье исследуются перспективы дальнейшего развития метода ELECTRA, рассматриваются возможности его интеграции с другими подходами к обучению, такими как трансферное обучение и

мета-обучение, а также выделены вопросы, связанные с его адаптацией для работы с многоязычными текстами и специфическими доменными задачами. Статья направлена на демонстрацию метода ELECTRA и раскрытие потенциала для будущих исследований и практического использования в области обработки естественного языка.

Ключевые слова: метод ELECTRA, генеративный подход, дискриминатор, обработка естественного языка

Для цитирования: Титов А.П. Метод генеративной дискриминации для эффективного предобучения языковых моделей // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 2. С. 54–68. DOI: 10.28995/2686-679X-2025-2-54-68

Generative discrimination method for effective retraining of language models

Andrei P. Titov
MIREA – Russian Technological University,
Moscow, Russia, titov_and@mail.ru

Abstract. The article presents a research approach to natural language processing (NLP) tasks, which significantly reduces the cost of computing resources. The main innovation of that method is to teach the model not only the ability to fill in blanks, but also to analyze errors in the inserted text, which contributes to a deeper understanding of language structures and nuances. The pre-learning of language models has become one of the key areas in the field of natural language processing, which has significantly improved the execution quality of tasks such as text classification, answering questions, and text generation. The article presents a detailed analysis of the ELECTRA (Efficiently Learning an Encoder that Classifies Token Replacements Accurately) method, and considers its features and advantages over traditional BERT and GPT prelearning methods. The ELECTRA method is an innovative approach to the task of pre-education, which is based on the concept of generative discrimination. The proposed approach allows the model to get deep insights from the data, since the discriminator is trained at the token level, making it t more context-sensitive. The main advantage of ELECTRA is the rational use of computing resources. The generative approach and the discriminator's ability to learn from large amounts of data allow the method to achieve results using lower computational costs compared to other models. That makes it more accessible to researchers and developers who may have hardware limitations. The method effectively uses contextual dependencies, which allows one to take into account the semantic connections between words and phrases. Unlike other models for

training on limited datasets, ELECTRA, helps to maintain a balance between training and verification due to its unique approach to discrimination, The article studies the prospects for further development of the ELECTRA method, considers the possibilities for its integration with other learning approaches such as transfer learning and meta-learning, and highlights issues related to its adaptation to work with multilingual texts and domain-specific tasks. The article aims to demonstrate the ELECTRA method and unlock the potential for future research and practical use in the field of natural language processing.

Keywords: ELECTRA method, generative approach, discriminator, natural language processing

For citation: Titov, A.P. (2025), "Generative discrimination method for effective retraining of language models", *RSUH/RGGU Bulletin. "Information science. Information security. Mathematics" Series,* no. 2, pp. 54–68, DOI: 10.28995/2686-679X-2025-2-54-68

Введение

Одним из популярных методов искусственного интеллекта является обучение с учителем, при котором модель обучается на размеченных данных для выполнения конкретных задач, таких как классификация и регрессия. Однако самое широкое распространение получило обучение без учителя, где модель пытается выявить скрытые паттерны в неразмеченных данных, и происходит обучение с подкреплением, где агент обучается через взаимодействие с окружающей средой, получая награды за правильные действия. Он особенно полезен в задачах, связанных с робототехникой и играми.

В последние годы заметно возросло использование многослойных нейронных сетей для обработки больших объемов данных, используемых для глубокого обучения. Глубокие нейронные сети позволяют достигать высокой точности в таких областях, как обработка естественного языка, компьютерное зрение и генерация контента. Модели GPT и BERT, основанные на архитектуре трансформеров, стали особенно популярными в задачах анализа текста из-за своей способности эффективно обрабатывать контекст и искать зависимость между словами [Malov 2019].

Современный искусственный интеллект опирается на широкий спектр методов и технологий, и их комбинирование обеспечивает возможность создания сложных и эффективных решений для самых различных задач [Kim 2021].

BERT (Bidirectional Encoder Representations from Transformers) – один из наиболее значимых методов обработки естествен-

ного языка, разработанный Google в 2018 г. Он стал основой для задач, связанных с пониманием текста (классификация, извлечение информации, анализ чувств, переводы и многие другие).

Актуальность BERT обусловлена его способностью эффективно понимать контекст слов в предложении. В отличие от предыдущих моделей, таких как Word2Vec или GloVe, которые создавали векторные представления слов, не учитывая их окружение, BERT использует двунаправленный подход. Модель анализирует как левую, так и правую контекстуальную информацию при генерации представления слова. Благодаря этому BERT может более точно учитывать многозначность и разнообразие значений слов в зависимости от контекста [Lee 2023].

BERT модель обучается на больших объемах текстовых данных с использованием задачи Masked Language Modeling (MLM) и Next Sentence Prediction (NSP). В задаче MLM случайным образом маскируются некоторые слова в предложениях, и модель учится предсказывать их на основе контекста. NSP, в свою очередь, обучает модель понимать связи между предложениями, что полезно, например, для задач, связанных с вопросами и ответами. После предварительного обучения ее можно адаптировать к конкретным задачам, добавляя несколько дополнительных слоев, специфичных для области применения, и проводя дообучение на размеченных данных. Это позволяет гибко использовать модель в различных контекстах, от анализа текстов до генерации ответов [Shen 2023]. Существует множество модификаций этого метода, направленных на улучшение его производительности, снижение вычислительных затрат или адаптацию к специфическим задачам.

RoBERTa (A Robustly Optimized BERT Pretraining Approach) фокусируется на усилении процесса предобучения, увеличивая объем данных для обучения и изменяя некоторые детали, такие как исключение задачи предсказания следующего предложения. Показывает улучшенные результаты в большинстве задач по сравнению с оригинальным BERT.

ALBERT (A Lite BERT) направлена на снижение объема модели без потери качества. Использует параметризацию, которая ведет к уменьшению числа параметров за счет разделения эмбеддингов между слоями, а также специфической техники факторизации. Метод эффективен в плане памяти и вычислений, при этом сохраняет высокие результаты на различных benchmarks.

DistilBERT разработан с акцентом на создание более легкой и быстрой версии BERT. Модель BERT превращается в более компактную форму за счет «дистилляция знаний». DistilBERT достигает почти 97% эффективности BERT при использовании ме-

нее чем 60% его размера, что делает его более пригодным для применения в реальных приложениях, где важна скорость и экономия вычислительных ресурсов.

ELECTRA предлагает новый подход к предобучению, основанный на предсказании того, какие токены были заменены в ходе генерации. Модель быстрее обучается и делает более эффективные выводы, что повышает ее производительность на различных задачах [Wang 2022].

Модификации BERT продолжают эволюционировать, расширяя его возможности и применимость в различных областях обработки естественного языка. Каждая из этих версий вносит свой вклад в разработку более эффективных, адаптивных и экономически оправданных решений для решения задач NLP. В статье исследована модификация метода ELECTRA, как наиболее перспективная.

Метод ELECTRA (Efficiently Learning an Encoder that Classifies Token Replacements Accurately) представляет собой усовершенствованную архитектуру трансформеров для обучения представлений, которая демонстрирует эффективность и высокую производительность. Суть этого метода заключается в предсказании замены токенов, а не простом заполнении пропусков [Khan 2021].

ELECTRA состоит из двух основных частей: генератора и дискриминатора. Генератор отвечает за создание подмены токенов в предложениях. Дискриминатор учится определять, какие токены были заменены. Это делается для повышения обобщающих способностей модели. Метод генеративной дискриминации включает в себя несколько ключевых шагов, которые представлены на рис. 1.

Сбор данных начинается со сбора обучающего набора данных, который состоит из примеров как из одной, так и из другой категории. Далее создается генеративная модель, которая может генерировать новые образцы, основываясь на имеющихся данных. Эта модель обучается на структуре данных. Следующим этапом обучается дискриминативная модель, целью которой является различение между реальными образцами из обучающего набора и образцами, созданными генеративной моделью. Обе модели (генеративная и дискриминативная) обучаются поочередно, при этом дискриминативная модель получает улучшенные данные от генеративной модели. Для оценки качества проводится сравнение моделей, чтобы определить, насколько хорошо дискриминативная модель может отличать реальные данные от поддельных. Генеративная и дискриминативная модели оптимизируются до тех пор, пока не будут достигнуты приемлемые показатели для обеих моделей.

Рис. 1. Шаги метода генеративной дискриминации

Рассмотрим подробнее алгоритм реализации данного метода на языке Python. Установим и импортируем необходимые библиотеки:

```
pip install torch transformers datasets
import torch
from torch import nn
from transformers import ElectraTokenizer, ElectraModel, Electra
ForPreTraining, ElectraForSequenceClassification
from datasets import load_dataset
```

Предварительный этап начинается со сбора и подготовки текстовых данных для обучения. Для обеспечения однородности данные должны быть очищены и обработаны. Обязательно производится токенизация текста в соответствии с используемой моделью трансформеров.

```
функция для токенизации входов и создания выборки с заменами
def preprocess_data(examples):
    inputs = tokenizer(examples['sentence'], truncation=True,
padding=True, max_length=128)
```

```
    # генерируем замененные токены, случайным образом заменяем
    часть токенов
      replaced_targets = []
      for i in range(len(inputs['input_ids'])):
        input_ids = inputs['input_ids'][i]
        labels = input_ids.copy()
        for j in range(len(input_ids)):
          if torch.rand(1).item() < 0.15: # вероятность замены 15%
            # заменяем токен на сгенерированный
            replaced_token = generator.generate(ids=torch.tensor([input_
ids]), max_length=1, do_sample=True)
            labels[j] = replaced_token.item()
        replaced_targets.append(labels)
    inputs['labels'] = replaced_targets
    return inputs
train_data = dataset['train'].map(preprocess_data, batched=True)
```

Настраиваем устройство, на котором будем обучать модель (GPU или CPU):

```
device = torch.device("cuda" if torch.cuda.is_available() else "cpu")
discriminator.to(device)
```

На этапе обучения требуется подготовить генератор на задаче Masked Language Modeling (MLM). Для этого выделяются случайные токены в предложении, которые будут замещены. Создаются маскированные версии предложений и генерируются заменяющие токены. Обучается модель на задаче предсказания замаскированных токенов на основе контекста.

Процесс обучения дискриминатора:

```
optimizer = torch.optim.Adam(discriminator.parameters(), lr=5e-5)
discriminator.train()
for epoch in range(3): # количество эпох
  for batch in train_data:
    optimizer.zero_grad()
    input_ids = torch.tensor(batch['input_ids']).to(device)
    labels = torch.tensor(batch['labels']).to(device)
    outputs = discriminator(input_ids=input_ids, labels=labels)
    loss = outputs.loss
    loss.backward()
    optimizer.step()
    print(f"Epoch: {epoch}, Loss: {loss.item()}")
```

После обучения генератора создается выборка, в которой генератор предсказывает замены токенов. Для каждого токена во входном тексте существует вероятность заменить его на предсказанный генератором токен, а с другой вероятностью остается токен без изменений.

Далее происходит обучение дискриминатора, который получает на вход оригинальные и измененные последовательности. Его задача – определить, соответствует ли токен оригинальному тексту или был заменен. Используется функция потерь (бинарная кросс-энтропия) для оценки вероятности правильности предсказаний дискриминатора.

```
    def binary_cross_entropy(predictions, targets, epsilon=1e-15):
    Вычисляет бинарную кросс-энтропию между предсказаниями и истинными метками.
    :param predictions: массив, содержащий предсказанные вероятности (значения от 0 до 1).
    :param targets: массив, содержащий истинные бинарные метки (0 или 1).
    :param epsilon: небольшое значение для ухода от ошибки деления на ноль.
    :return: значение функции потерь.
      # Ограничиваем предсказания, чтобы избежать логарифма нуля.
      predictions = np.clip(predictions, epsilon, 1 – epsilon)
        # Вычисляем бинарную кросс-энтропию.
      bce = -np.mean(targets * np.log(predictions) + (1 – targets) * np.log(1 – predictions))
      return bce
```

После обучения генератора и дискриминатора они могут быть объединены для проведения дополнительного обучения на специфических задачах: классификация или взаимодействие в формате вопрос-ответ. При этом используются заранее подготовленные представления. Дискриминатор обучается по тем же задачам, как классические модели трансформеров.

Завершается процесс оценкой модели по различным задачам: анализ метрик, точность и полнота для оценки производительности как генератора, так и дискриминатора.

Интеграция метода ELECTRA может значительно улучшить эффективность и адаптивность моделей в сфере обработки естественного языка.

В контексте трансферного обучения ELECTRA может служить основой для предобученных моделей, которые дообучаются на

целевых наборах данных с целью выполнения конкретных задач. Например, после предобучения на обширном текстовом корпусе, ELECTRA может быть адаптирована под задачи текстовой классификации, извлечения информации или ответов на вопросы. Этот процесс включает Fine-tuning, который позволяет отрегулировать параметры модели в соответствии с требованиями определенной задачи.

Проведенные исследования подтверждают, что модели, предобученные с использованием ELECTRA, показывают более высокие результаты по сравнению с другими моделями благодаря более эффективному использованию имеющейся информации.

Интеграция мета-обучения с ELECTRA позволяет сократить время адаптации моделей на ограниченных данных. Мета-обучение включает обучение на множестве задач, создавая модель, которая быстро подстраивается под новые, но связанные задачи. Использование ELECTRA может рассматриваться как основа для модели, которая может быстро быть дообучена на новых задачах. В этом процессе модель используется для генерации начальных весов, которые затем адаптируются для решения новых задач с помощью нескольких шагов градиентного спуска. Это позволяет модели достигать высоких результатов даже при минимальной настройке в ситуациях с ограниченными или несбалансированными данными.

Взаимосвязь метода ELECTRA с трансферным и мета-обучением повышает эффективность обработки текстов, делает модели более универсальными и снижает затраты на ресурсы и данные для обучения. Это открывает новые направления для исследований, так как использовать сочетание этих подходов можно не только для повышения производительности систем, но и для создания новых архитектур моделей, способных к быстрой адаптации и обучению.

Адаптация методологии ELECTRA для функционирования с многоязычными данными и специфическими задачами в различных областях представляет собой интересную исследовательскую проблему. Языковые модели, обученные исключительно на одном языке, порой оказываются неэффективными в решении задач, возникающих на других языках или в узкоспециализированных областях.

В рамках многоязычного подхода ELECTRA улучшается через предобучение на многоязычных наборах данных. Происходит обучение модели на разнообразных текстах, охватывающих несколько языков и диалектов. Это позволяет модели осваивать уникальные языковые структуры и элементы, что, в свою очередь, повышает ее способность к пониманию контекста и смысла текстов, написанных

на различных языках. Использование параллельных наборов, содержащих переводы одних и тех же текстов на разных языках, играет важную роль в этом процессе, так как позволяет модели воспринимать кросс-языковой контекст и изучать переводимое значение и синтаксические особенности. Многоязычные архитектуры, такие как multilingual BERT, могут послужить ценным дополнением для интеграции с ELECTRA, создавая прочную основу для многоязычного обучения [Zhu 2023].

Касаемо специфических задач в отдельных доменах, адаптация модели может включать дообучение на специализированных наборах данных, например, на медицинских, юридических или технических текстах. Эти наборы содержат уникальную терминологию и структуры, отличающиеся от общепринятых текстов. Обычно для решения задач в рамках конкретной области применяется техника Fine-tuning, в процессе которой ELECTRA дообучается на конкретных примерах из выбранного домена с использованием меньшего объема данных. Также можно создать кастомизированные токенизаторы, которые учитывают особенности терминологии и стилистики данного домена, либо воспользоваться техникой активного обучения, где модель динамически выбирает образцы для своего обучения и тем самым улучшает свое понимание контекста, целевых задач и особенностей конкретного домена [Titov 2023].

Использование многоязычной адаптации с решением специфических задач через метод ELECTRA позволяет создать более адаптивные и мощные системы обработки естественного языка. Эти системы способны эффективно работать с разнообразными текстами и задачами, полностью раскрывая потенциал языковых технологий на глобальном уровне [Nguyen 2023].

Рассмотрим организацию процесса предобучения модели ELECTRA. Допустим, у нас есть небольшой набор текстовых данных, содержащий предложения, а также сгенерированный набор подмененных токенов (табл.1).

Во время создания архитектуры ELECTRA включает в себя генератор, создающий замены токенов, и дискриминатор, предсказывающий, является ли токен оригинальным или подмененным. Обучается дискриминатор на парах (оригинальное предложение, подмененное предложение) с меткой 0, если токен был заменен, и 1, если токен был оригинальным. Используем подходящие функции потерь (например, бинарная кросс-энтропия) для оптимизации параметров дискриминатора, что повышает его способность различать оригинальные токены и подмены. Далее корректируется модель с использованием техник регуляризации и дообучения с использованием более крупных наборов данных.

Таблица 1

Данные с оригинальными предложениями
и их подмененными версиями

Оригинальное предложение	*Подмененное предложение*	*Токены замены*	*Метка*
Кошка сидит на окне.	Кошка сидит на столе.	столе	0 (подмена)
Погода сегодня прекрасная.	Погода сегодня дождливая.	дождливая	0 (подмена)
Я люблю читать книги.	Я люблю смотреть фильмы.	смотреть фильмы	0 (подмена)
Он пошел в магазин.	Он пошел в парк.	парк	0 (подмена)
Она готовит ужин.	Она готовит десерт.	десерт	0 (подмена)
Собака бегает по двору.	Собака спит в доме.	спит в доме	0 (подмена)
Я пишу статьи.	Я пишу письма.	письма	0 (подмена)
Вечером идет дождь.	Вечером светит солнце.	светит солнце	0 (подмена)
У него большая коллекция марок.	У нее большая коллекция монет.	монет	0 (подмена)
Мы пойдем в кино сегодня.	Мы пойдем в театр сегодня.	театр	0 (подмена)

После предобучения на таком наборе данных модель будет готова для выполнения различных задач, таких как анализ тональности, извлечение информации или генерация текста. После этого наступает обучение модели ELECTRA, которая будет использовать подготовленные данные для оптимизации своего представления. Процесс включает в себя несколько важных составляющих.

Дискриминатор, реализованный на архитектуре трансформеров, будет ориентирован на то, чтобы различать оригинальные токены и те, которые были сгенерированы генератором. Во время тренировки:

– генератор создает подмененные версии оригинальных текстов. Например, предложение «Кошка сидит на окне» может быть преобразовано в «Кошка сидит на столе»;
– дискриминатор получает как оригинальные, так и подмененные токены из генератора и учится определять, какие из них являются оригинальными.

На каждом этапе обучения оптимизируется целевая функция, которая минимизирует потери дискриминатора [Kumar 2023]. Это позволяет ему с каждым шагом становиться все более чувствительным к подменам. Потери могут быть выражены следующим образом:

$$L = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(p_i) + (1 - y_i)\log(1 - p_i)],$$

где L – потери, N – количество токенов, y_i – метка для токена (1 – оригинал, 0 – подмена), а p_i – предсказанная вероятность для токена быть оригинальным.

Обученный дискриминатор может быть использован в приложениях, таких как: модерация контента, где требуется различать оригинальные подписи и потенциально нежелательные сообщения, автоматический анализ отзывов, который помогает быстро оценить, являются ли отзывы подлинными, генерация текста с высокими показателями завершенности и правдоподобия, что может быть полезно в чат-ботах и других системах обработки естественного языка.

Таким образом, метод ELECTRA предлагает новый взгляд на предобучение языковых моделей, который сочетает в себе эффективность генерации и точность классификации, что делает его мощным инструментом в арсенале разработчиков и исследователей в области обработки естественного языка.

Заключение

В статье рассмотрен метод генеративной дискриминации, внедренный в модель ELECTRA, который продемонстрировал значительные улучшения в предобучении языковых моделей, превосходящие традиционные подходы. Применяя принципы генерации и дискриминации, ELECTRA эффективно обучает языковую модель, используя более сложные задачи предсказания маскированных токенов. Это обеспечивает лучшую способность модели улавливать семантические и контекстуальные взаимосвязи в тексте.

Многоязычное предобучение расширяет горизонты понимания и обработки текстов на различных языках, что становится важным в условиях глобализации информации. Адаптация к специфическим доменным задачам, благодаря дообучению на специализированных наборах данных, дает модели возможность эффективно справляться

с задачами в узкоспециализированных областях, учитывая уникальную терминологию и стилевые особенности.

Метод ELECTRA не только символизирует прогрессивный шаг в развитии языковых моделей, но и открывает новые перспективы для исследования и применения в многоязычных и специализированных контекстах. Перспективы будущих исследований в этой области выглядят многообещающе и динамично, предлагая возможность для совершенствования модели и её адаптации для решения актуальных задач, а также реагирования на новые вызовы и реализации разнообразных языковых и доменных применений.

Литература

Малов 2019 – *Малов Д.А., Летенков М.А.* Методика генерации искусственных наборов данных и архитектура системы распознавания лиц для взаимодействия с роботами внутри киберфизического пространства // Робототехника и техническая кибернетика. 2019. Т. 7. № 2. С. 100–108.

Титов 2023 – *Титов А.П.* Анализ моделей адаптивных нейро-нечетких систем // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 21–35.

Khan 2021 – *Khan A., Ma Y., Zhou H.* ELECTRA-based Approach for Abstractive Text Summarization // Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing (EMNLP). Stroudsburg, PA: ACL, 2021. P. 996–1006.

Kim 2021 – *Kim Y., Lee Y.* Generative Discriminative Models for Joint Learning of Text Generation and Discriminative Classification // Proceedings of the Association for Computational Linguistics (ACL). Stroudsburg, PA: ACL, 2021. P. 1050–1061.

Kumar 2023 – *Kumar A., Singhal D.* Efficient Training Strategies for Generative Discriminative Models in Low-Resource Settings // Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing (EMNLP). Stroudsburg, PA: ACL, 2023. P. 681–690.

Lee 2023 – *Lee H., Park J.* Adaptive Generative Discriminative Learning for Personalized Content Recommendations // Proceedings of the 2023 International Conference on Web Engineering (ICWE). New York: Springer, 2023. P. 435–446.

Nguyen 2023 – *Nguyen T., Yang Y.* Exploring the Interplay Between Generative and Discriminative Models in Language Understanding Tasks // Proceedings of the 2023 Conference on Computational Natural Language Learning (CoNLL). Stroudsburg, PA: ACL, 2023. P. 56–66.

Shen 2023 – *Shen T., Zhao R.* A Unified Framework for Generative and Discriminative Learning in Natural Language Processing // Proceedings of the 2023 International Joint Conference on Natural Language Processing (IJCNLP). Stroudsburg, PA: ACL, 2023. P. 222–231.

Wang 2022 – *Wang S., Jiang J., Lai J.* Fine-tuning ELECTRA for Low-Resource Language Processing // Proceedings of the 2022 Annual Meeting of the Association for Computational Linguistics (ACL), Stroudsburg, PA: ACL, 2022. P. 1789–1797.

Zhu 2023 – *Zhu Y., Wang S.* Modeling User Preferences in Text Generation through Generative Discriminative Approaches // Proceedings of the 2023 Conference on Artificial Intelligence (AAAI). Menlo Park, CA: The AAAI Press, 2023. P. 1446–1455.

References

Khan, A., Ma, Y. and Zhou, H. (20021), "ELECTRA-based Approach for Abstractive Text Summarization", *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing (EMNLP),* ACL, Stroudsburg, PA, USA, pp. 996–1006.

Kim, Y.and Lee, Y. (2021), "Generative Discriminative Models for Joint Learning of Text Generation and Discriminative Classification", *Proceedings of the Association for Computational Linguistics (ACL),* ACL, Stroudsburg, PA, USA, pp. 1050–1061.

Kumar, A. and Singha, l D. (2023),"Efficient Training Strategies for Generative Discriminative Models in Low-Resource Settings", *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing (EMNLP),* ACL, Stroudsburg, PA, USA, pp. 681–690.

Lee, H. and Park J. (2023), "Adaptive Generative Discriminative Learning for Personalized Content Recommendations", *Proceedings of the 2023 International Conference on Web Engineering (ICWE)*, ACL, Stroudsburg, PA, USA, pp. 435–446.

Malov, D.A. and Letenkov, M.A. (2019), "A technique for generating artificial data sets and the architecture of a facial recognition system for interacting with robots inside a cyberphysical space", *Robotics and technical cybernetics*, vol. 7, no. 2. pp. 100–108.

Nguyen, T. and Yang, Y. (2023), "Exploring the Interplay Between Generative and Discriminative Models in Language Understanding Tasks", *Proceedings of the 2023 Conference on Computational Natural Language Learning (CoNLL)*, ACL, Stroudsburg, PA, USA, p. 56–66.

Shen, T. and Zhao, R. A (2023), "Unified Framework for Generative and Discriminative Learning in Natural Language Processing", *Proceedings of the 2023 International Joint Conference on Natural Language Processing (IJCNLP),* ACL, Stroudsburg, PA, USA, pp. 222–231.

Titov, A.P. (2023), "Analysis of models of adaptive neuro-fuzzy systems", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, vol. 1, pp. 21–35.

Wang, S., Jiang, J. and Lai, J. (2022), "Fine-tuning ELECTRA for Low-Resource Language Processing", *Proceedings of the 2022 Annual Meeting of the Association for Computational Linguistics (ACL),* ACL, Stroudsburg, PA, USA, pp. 1789–1797.

Zhu, Y. and Wang, S. (2023), "Modeling User Preferences in Text Generation through Generative Discriminative Approaches", *Proceedings of the 2023 Conference on Artificial Intelligence (AAAI)*, The AAAI Press, Menlo Park, CA, USA, pp. 1446–1455.

Информация об авторе

Андрей П. Титов, кандидат технических наук, доцент, МИРЭА – Российский технологический университет, Москва, Россия; 107076, Россия, Москва, ул. Стромынка, д. 20; titov_and@mail.ru

Information about the author

Andrei P. Titov, Cand. of Sci. (Mechanical Engineering), associate professor, MIREA – Russian Technological University, Moscow, Russia; bld. 20, Stromynka Str., Moscow, 107076, Russia; titov_and@mail.ru

УДК 004.491.22
DOI: 10.28995/2686-679X-2025-2-69-79

Модернизированная система генерации и управления криптостойкими ключами

Марьяна А. Георгиева
Кабардино-Балкарский государственный университет, Нальчик, Россия, maryana.g@list.ru

Константин С. Бархатов
Кабардино-Балкарский государственный университет, Нальчик, Россия, barhatov364@gmail.com

Аннотация. В условиях стремительного роста киберугроз и экспоненциального увеличения числа утечек конфиденциальных данных, разработка и внедрение эффективных методов защиты информации становятся абсолютным приоритетом для любой современной организации. В этом контексте надежная криптографическая система играет ключевую роль в обеспечении конфиденциальности и целостности данных, гарантируя их защиту от несанкционированного доступа и неправомерного использования. Однако, несмотря на важность криптографической защиты, создание простых, но одновременно устойчивых решений для генерации криптостойких ключей остается актуальной и сложной задачей, требующей постоянного совершенствования. Целью данного исследования является проектирование и практическая реализация инновационной системы генерации криптографических ключей, обладающей высокой степенью стойкости, на основе надежного алгоритма AES-CTR и современных методов оценки криптографической энтропии. Для достижения этой амбициозной цели были выполнены следующие задачи: разработана программная архитектура, обеспечивающая безопасную генерацию, защищенное сохранение и корректное использование ключей, реализована эффективная оценка криптостойкости с применением передовых методов анализа энтропии, и, наконец, предоставлен интуитивно понятный графический интерфейс, который сделает систему доступной для широкого круга конечных пользователей.

Ключевые слова: система генерации, симметричное шифрование, криптостойкие ключи, криптостойкость

Для цитирования: Георгиева М.А., Бархатов К.С. Модернизированная система генерации и управления криптостойкими ключами // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 2. С. 69–79. DOI: 10.28995/2686-679X-2025-2-69-79

Modernized system for generation and management of crypto-resistant keys

Mar'yana A. Georgieva
Kabardino-Balkarian State University, Nalchik, Russia, maryana.g@list.ru

Konstantin S. Barkhatov
Kabardino-Balkarian State University, Nalchik, Russia, barhatov364@gmail.com

Abstract. With the rapid growth of cyber threats and exponential increase in the number of confidential data leaks, the development and implementation of effective information security methods become an absolute priority for any modern organization. In that context, a robust cryptographic system plays a key role in ensuring the confidentiality and integrity of data, guaranteeing its protection from unauthorized access and misuse. However, despite the importance of cryptographic protection, creating simple yet robust solutions for crypto-resistant key generation remains a relevant and challenging task that requires continuous improvement. The goal of the research is to design and practically implement an innovative cryptographic key generation system with a high degree of resilience based on the robust AES-CTR algorithm and modern cryptographic entropy estimation techniques. To realize such an ambitious goal, the following tasks have been accomplished: a software architecture has been developed to ensure secure key generation, secure storage and correct use of keys, an efficient cryptostability evaluation using advanced entropy analysis methods has been implemented, and finally, an intuitively understandable graphical interface has been provided to make the system accessible to a wide range of end-users.

Keywords: generation system, symmetric encryption, crypto-resistant keys, cryptostability

For citation: Georgieva, M.A. and Barkhatov, K.S. (2025), "Modernized system of generation and management of crypto-resistant keys", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 69–79, DOI: 10.28995/2686-679X-2025-2-69-79

Введение

Работа основана на алгоритмах симметричного шифрования, включая стандарт AES в режиме CTR, с применением математического анализа для расчета энтропии, что позволяет оценить криптостойкость сгенерированных ключей. Для разработки программной системы использовались язык Python, встроенные библиотеки (такие как hashlib и os для генерации случайных чисел и хеширования), а также модуль Tkinter для создания графического интерфейса. Теоретическая основа включает изучение научных публикаций, посвященных стандартам шифрования и методам оценки стойкости данных[1].

Разработанная система представляет собой программное обеспечение, предназначенное для генерации криптографических ключей с высокой степенью случайности, анализа их стойкости и использования в рамках процесса шифрования. Основные функции системы включают создание случайных ключей и начальных векторов (nonce), шифрование данных на основе алгоритма AES-CTR, расчет энтропии для оценки уровня криптографической стойкости, а также безопасное хранение и управление ключами. Пользовательский интерфейс позволяет проводить операции через интуитивно понятное меню, обеспечивая гибкость и удобство при работе с системой.

Криптографическая стойкость системы определяется ее способностью противостоять различным атакам, направленным на получение ключа или исходных данных [Арванова 2024]. Для количественной оценки стойкости широко используется показатель энтропии. Энтропия H(X) описывает степень случайности распределения символов в данных и вычисляется по формуле Шеннона:

$$H(X) = -\sum_{i=1}^{n} p(xi) * log_2 (p(xi)),$$

где $H(X)$ – энтропия случайной величины X; $p(xi)$ – вероятность появления i-го символа xi в данных; n – общее количество уникальных символов[2].

---

[1] Pure Python implementation of AES, with optional cipher modes / H. Boppre. URL: https://github.com/boppreh/aes (дата обращения 10.02.2025).

[2] Implementation of AES CBC and CTR modes / D. Vieira. URL: https://github.com/diegodvv/AES-CBC-CTR-implementation (дата обращения 10.02.2025).

В программе реализован алгоритм, вычисляющий частоту появления каждого байта данных, нормирующий ее и подставляющий в формулу. Максимальная энтропия достигается при равномерном распределении вероятностей, что соответствует наиболее случайным данным.

Для нормализованной оценки криптографической стойкости используется отношение вычисленной энтропии $H(X)$ к ее максимальному значению *Hmax*, определяемому как[3]:

$$Hmax = log_2(n),$$

где $n = 256$ для байтовых данных.

Таким образом, относительная стойкость может быть выражена как:

$$S = \frac{H(X)}{Hmax} * 100\%,$$

где S интерпретируется как процент максимальной стойкости.

Значение $S > 95\%$ свидетельствует о высокой криптографической стойкости.

На практике программа генерирует случайные данные (например, с использованием os.urandom) и рассчитывает энтропию с учетом частот символов. После этого производится сравнение с теоретическим максимумом, а результат логируется для анализа.

Высокая энтропия гарантирует, что данные сложно предсказать или воспроизвести [Хаширова, Мамучиев, Мамучиева, Эдгулова 2019]. Если энтропия ниже порогового значения, это может указывать на слабости генератора случайных чисел или избыточность в данных, что повышает вероятность успешного криптоанализа, например, атаки по совпадению блоков (birthday attack) или атак на повторные ключи.

Алгоритм AES в режиме CTR используется в разработанной системе для шифрования данных, а также уникальное значение nonce, комбинируемое со счетчиком, чтобы исключить повторение одного и того же ключевого потока. Каждый блок данных шифруется следующим образом:

$$Ci = Pi \oplus E\ (K, Nonce\ \mathrm{V}\ Counteri),$$

[3] Python implementation of AES encryption algorithm in counter mode / R. Domanski. URL: https://github.com/rdomanski/AES-CTR (дата обращения 10.02.2025).

где *Ci* – шифротекст для *i*-го блока; *Pi* – исходный текст *i*-го блока; *K* – секретный ключ; *E* – функция шифрования AES; Nonce‖Counter – объединение уникального значения и счетчика[4].

Nonce (Number used once) используется как часть ввода для шифрования каждого блока данных, обеспечивая уникальность ключевого потока. Ключи и значения Nonce генерируются с использованием встроенной библиотеки os и функции os.urandom, которая обеспечивает криптографически стойкую случайность.

Секретный ключ имеет длину 128 бит, а Nonce – 64 бита. Выбор таких параметров обусловлен требованиями алгоритма AES и необходимостью обеспечения уникальности ключевого потока. Генерируемые значения сохраняются в файл формата JSON с использованием следующей функции:

```
def save_key_nonce(key, nonce):
    with open(KEY_FILE, 'w') as file:
        json.dump({"key": key.hex(), "nonce": nonce.hex()}, file)
```

Шифрование данных реализовано на основе алгоритма AES в режиме CTR. Режим CTR обеспечивает уникальность ключевого потока для каждого блока данных, используя комбинацию Nonce и счетчика. В коде это достигается с помощью функции:

```
def aes_ctr_encrypt(data, key, nonce):
    expanded_key = key_expansion(key)
    result = b''
    counter = 0
    block_size = 16
    for i in range(0, len(data), block_size):
        block = data[i:i + block_size]
        counter_block = nonce + struct.pack('<Q', counter)
        encrypted_counter = encrypt_block(counter_block, expanded_key)
        result_block = xor_bytes(block, encrypted_counter[:len(block)])
        result += result_block
        counter += 1
    return result
```

Рассмотрим более детально шаги этого алгоритма. Перед шифрованием выполняется расширение ключа с помощью функции

[4] Implementation of AES CBC and CTR modes / D. Vieira. Диего. URL: https://github.com/diegodvv/AES-CBC-CTR-implementation (дата обращения 10.02.2025).

key_expansion. Этот процесс создает набор раундовых ключей, используемых на каждом этапе AES. Для каждого блока данных создается уникальный счетчик. Nonce объединяется с текущим значением счетчика, упакованного в 64-битное число, что гарантирует уникальность.

Затем блок счетчика шифруется с помощью функции AES. Результат шифрования представляет собой ключевой поток, используемый для шифрования данных. Далее каждый блок данных Pi XOR-ится с результатом шифрования счетчика, объединенного с Nonce. Использование структуры struct.pack позволяет надежно упаковывать счетчик в 64-битное значение. После обработки каждого блока счетчик увеличивается на единицу, что гарантирует уникальность для следующего блока. Далее результирующий шифротекст собирается из всех обработанных блоков и возвращается.

Для анализа качества сгенерированных ключей используется расчет энтропии данных. Этот процесс основан на формуле Шеннона, где частотное распределение символов анализируется через:

```
def calculate_entropy(data):
    frequency = {byte: data.count(byte) / len(data) for byte in set(data)}
    entropy = -sum(p * math.log2(p) for p in frequency.values())
    return entropy
```

Программа считывает каждый уникальный байт в массиве данных, вычисляет его частоту, а затем подставляет полученные значения в формулу. Итоговая энтропия сравнивается с максимальной теоретической, что позволяет определить степень случайности ключей.

Архитектура программы построена таким образом, чтобы каждый компонент был модульным и переиспользуемым. Генерация ключей и Nonce связана с их последующим применением в AES-CTR. Оценка энтропии, в свою очередь, интегрирована в интерфейс для наглядной демонстрации качества ключей.

Для упрощения взаимодействия с пользователем был реализован графический интерфейс на базе библиотеки Tkinter. Главный экран программы предоставляет доступ к основным функциям: генерации ключей, шифрованию и расшифровке данных. Кнопки и элементы управления оформлены в современном стиле:

```
class ModernButton(ttk.Button):
    def¬_init_(self, *args, **kwargs):
        super()._init_(*args, **kwargs)
        self.configure(style='Modern.TButton')
```

Интерфейс состоит из двух основных частей: боковой панели навигации и рабочей области. Боковая панель содержит кнопки для переключения между модулями программы:

– генерация ключей;
– шифрование текста;
– расшифровка текста.

В центральной части расположена рабочая область, где пользователь может взаимодействовать с выбранной функцией. Дизайн интерфейса выдержан в минималистичном стиле, с темным фоном для снижения нагрузки на зрение.

Модуль генерации ключей предоставляет пользователю возможность выбрать алгоритм хеширования из выпадающего списка (SHA-256, SHA-512 или SHA3-256) и запустить процесс генерации. После выполнения команды программа отображает:

– сгенерированный ключ;
– значение Nonce;
– хеш данных для верификации;
– оценку криптографической стойкости в процентах.

Результаты отображаются в текстовых полях с возможностью копирования, пример показан на рис. 1.

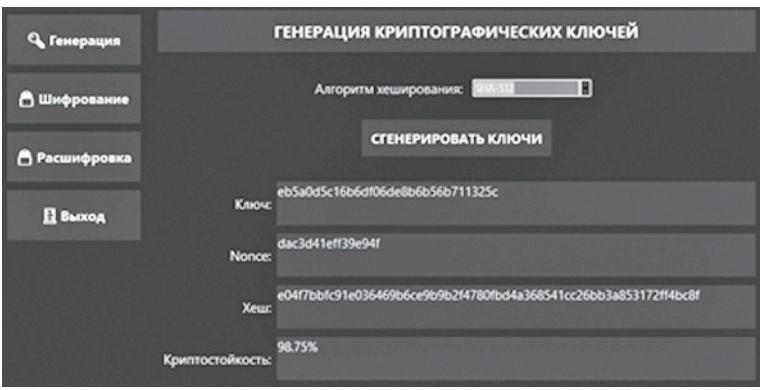

Рис. 1. Панель генерации ключей

В модуле шифрования пользователь вводит текст, выбирает алгоритм хеширования и нажимает кнопку «Зашифровать». Программа шифрует текст с использованием ранее сгенерированного ключа и отображает результат в формате hex-строки. Интерфейс предоставляет поле для ввода текста и кнопку управления, что упрощает процесс. Пример приведен на рис. 2, в нем мы зашифруем наш криптостойкий ключ из первого раздела.

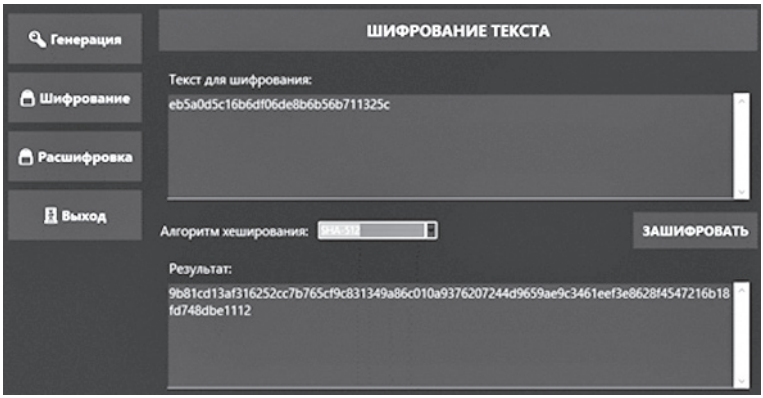

Рис. 2. Панель шифрования текста

В модуле расшифровки пользователь вставляет зашифрованный текст (hex-строку) и нажимает кнопку «Расшифровать». Программа автоматически расшифровывает данные с использованием ключа и Nonce из файла формата JSON. Результат отображается в текстовом поле ниже, поддерживая все стандартные символы. В качестве примера рассмотрим текст, который мы расшифровали, на рис. 3.

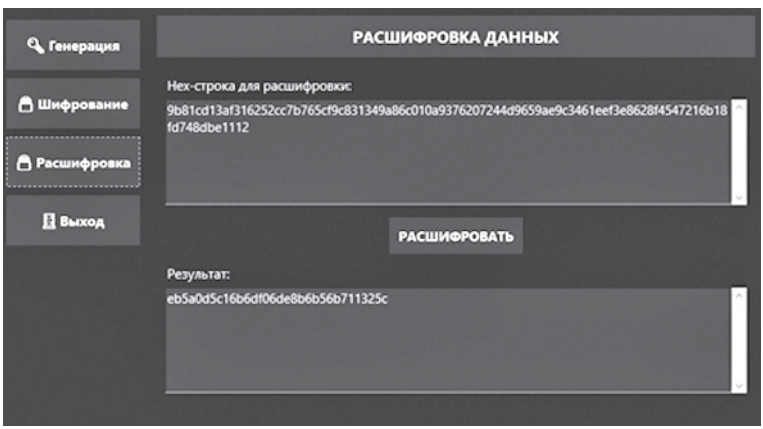

Рис. 3. Панель расшифровки текста

Разработанное приложение сочетает удобство использования и мощные криптографические механизмы. Помимо базовой функциональности, программа позволяет:

– анализировать качество генерации ключей с помощью встроенного расчета энтропии, что обеспечивает прозрачность процесса и возможность контроля качества случайности;
– безопасно сохранять ключи и Nonce в файл, что облегчает их повторное использование [Свейгарт 2020]. Формат JSON выбран для совместимости и удобства;
– демонстрировать результаты в наглядной форме через графический интерфейс. Пользователь видит ключи, Nonce, результаты шифрования и оценки стойкости, что делает процесс прозрачным даже для начинающих.

Программа может быть доработана для добавления дополнительных алгоритмов шифрования, таких как ChaCha20, или интеграции с системами управления ключами для промышленного использования.

Для оценки эффективности и удобства системы стоит рассмотреть ее в контексте других методов шифрования и программных решений.

1. AES в режиме CBC (Cipher Block Chaining). В режиме CBC каждый блок данных зависит от предыдущего, что делает его более сложным для параллельной обработки. В отличие от CTR, CBC требует выравнивания, что может стать уязвимостью при неправильной реализации. Программа, использующая CTR, избегает этой проблемы благодаря поблочному XOR.

2. Stream Ciphers (потоковые шифры). Потоковые шифры, такие как RC4, имеют схожую функциональность с режимом CTR, однако они более уязвимы к анализу при неправильной настройке. Использование AES в режиме CTR в разработанной программе обеспечивает криптографически стойкую основу за счет доказанной устойчивости самого AES.

3. Программные решения без графического интерфейса. Большинство решений для AES-CTR (например, библиотеки PyCryptodome) предоставляют инструменты для шифрования, но их использование требует навыков программирования. Разработанная программа с графическим интерфейсом снижает порог входа и делает функционал доступным для широкой аудитории.

4. Аппаратные реализации AES. Аппаратные реализации (например, Intel AES-NI) обеспечивают более высокую производительность, однако их интеграция требует соответствующего оборудования. Программная реализация в Python обеспечивает гибкость и доступность на любом устройстве.

Выводы

Разработанный программный продукт доказал свою эффективность как инструмент для генерации и анализа криптографически стойких ключей. Использование AES в режиме CTR обеспечивает высокий уровень безопасности за счет уникальности каждого ключевого потока, исключая возможность повторов.

Реализация расчета энтропии основана на применении формулы Шеннона для количественной оценки случайности ключевых данных. В программе вычисляется частотное распределение байтов, нормализуется вероятность появления каждого символа и рассчитывается энтропийная мера, позволяющая объективно оценить уровень случайности. Сопоставление полученных значений с теоретическим максимумом обеспечивает верификацию криптостойкости сгенерированных ключей и выявление потенциальных слабостей генератора случайных чисел.

Благодаря графическому интерфейсу работа с программой стала интуитивно понятной, что делает ее доступной для широкого круга пользователей, независимо от уровня их подготовки.

Программа сочетает надежные криптографические механизмы с простотой использования, что позволяет решать практические задачи информационной безопасности и демонстрировать ключевые аспекты шифрования в образовательных целях.

Литература

Арванова 2024 – *Арванова С.М.* Перспективы применения высокоскоростных генераторов случайных чисел для аутентификации доступа и распределения ключей // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2024. № 8. С. 67–70.

Свейгарт 2020 – *Свейгарт Э.* Криптография и взлом шифров на Python / Пер. с англ. А.Г. Гузикевич; ред. В.Р. Гинзбург. М.; СПб.: Диалектика, 2020. 512 с.

Хаширова, Мамучиев, Мамучиева, Эдгулова 2019 – *Хаширова Т.Ю., Мамучиев И.И., Мамучиева М.И., Эдгулова Е.К.* Модель обобщенной оценки защищенности информации в интегрированных системах безопасности // Университетский научный сборник № 3. Сборник научных трудов национальной университетской научно-практической конференции, приуроченной к 85-летию со дня основания Кабардино-Балкарского государственного университета. Т. 1. Нальчик, 2019.

References

Arvanova, S.M. (2024), "Prospects for application of high-speed random number generators for access authentication and key distribution", *Modern Science. Current issues of theory and practice. Series: Natural and technical sciences*, no. 8, pp. 67–70.

Khashirova, T.Yu., Mamuchiev, I.I, Mamuchieva, M.I. and Edgulova, E.K. (2019), "Model of generalized assessment of information security in integrated security systems", *University Scientific Collection No. 3: Collection of scientific articles of the National University Scientific-Practical Conference, timed to the 85th anniversary of Kabardino-Balkarian State University*, Nalchik, September 20–25, 2019, vol. 1, Kabardino-Balkarian State University, Nalchik, Kabardino-Balkaria, Russia, pp. 155–161.

Sweigart, E. (2020), *Kriptografiya i vzlom shifrov na Python* [Cryptography and cipher cracking in Python], Guzikevich, A.G. (transl. from Engl.) and Ginzburg, V.R. (ed.), Dialektika, Moscow, Saint Petersburg, Russia, 592 p.

Информация об авторах

Марьяна А. Георгиева, Кабардино-Балкарский государственный университет, Нальчик, Россия; 360004, Россия, Нальчик, ул. Чернышевского, д. 173; maryana.g@list.ru

Константин С. Бархатов, студент, Кабардино-Балкарский государственный университет, Нальчик, Россия; 360004, Россия, Нальчик, ул. Чернышевского, д. 173; barhatov364@gmail.com

Information about the author

Mar'yana A. Georgieva, Kabardino-Balkarian State University, Nalchik, Russia; bld. 173, Chernyshevskogo Str., Nalchik, 360004, Russia; maryana.g@list.ru.

Konstantin S. Barkhatov, student, Kabardino-Balkarian State University, Nalchik, Russia; bld. 173, Chernyshevskogo Str., Nalchik, 360004, Russia; barhatov364@gmail.com

УДК 004.056
DOI: 10.28995/2686-679X-2025-2-80-92

Разработка методики тестирования безопасности ИТ-проектов

Айрат Б. Шукенбаев
МИРЭА – Российский технологический университет,
Москва, Россия, shukenbaev@mirea.ru

Камилла Р. Зиатдинова
МИРЭА – Российский технологический университет,
Москва, Россия, kziatdinova@gmail.com

Наиля Ш. Шукенбаева
Российский государственный гуманитарный университет,
Москва, Россия, nelshuk@mail.ru

Аннотация. Тестирование безопасности – необходимый первый шаг для организаций, целью которых является определение уровня информационной безопасности и ее повышения для укрепления защиты.

Существуют различные методики и стандарты. Каждая отдельная методология описывает процесс, который организация может выполнить для обнаружения уязвимостей. Компании могут как создать свою внутреннюю методологию, так и использовать уже существующую методику, но чаще всего специалисты проводят тестирование безопасности согласно известным методикам.

Статья посвящена сравнительному анализу методик и стандартов тестирования безопасности систем, сетей и веб-приложений. Были рассмотрены: методологии тестирования безопасности веб-приложений OWASP WSTG, техническое руководство по тестированию и оценке информационной безопасности NIST SP 800-115, стандарт выполнения тестирования на проникновение PTES, методика оценки безопасности информационных систем ISSAF, методологии тестирования безопасности с открытым исходным кодом OSSTMM, методология изучения модели тестирования на проникновение BSI, методика Positive Technologies. Выявлены их сильные и слабые стороны. На основе анализа предложена методика, ориентированная на эффективность, простоту внедрения и адаптацию под различные проекты. Практическая значимость работы заключается в возможности ее применения для повышения уровня защищенности информационных систем. Результаты исследования могут быть полезны

специалистам в области информационной безопасности и организациям, стремящимся минимизировать риски кибератак.

Ключевые слова: тестирование безопасности, анализ уязвимостей, оценка рисков, методика тестирования, информационная безопасность

Для цитирования: Шукенбаев А.Б. Зиатдинова К.Р., Шукенбаева Н.Ш. Разработка методики тестирования безопасности ИТ-проектов // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 2. С. 80–92. DOI: 10.28995/2686-679X-2025-2-80-92

Development of a methodology for testing the security of IT projects

Airat B. Shukenbaev
MIREA – Russian Technological University, Moscow, Россия, shukenbaev@mirea.ru

Kamilla R. Ziatdinova
MIREA – Russian Technological University, Moscow, Россия, kziatdinova@gmail.com

Nailya Sh. Shukenbaeva
Russian State University for the Humanities, Moscow, Russia, nelshuk@mail.ru

Abstract. Security testing is a necessary first step for organizations whose goal is to determine the level of information security and enhance it for strengthening the protection. There are various methodologies and standards. Each individual methodology describes a process that an organization can perform to detect vulnerabilities. Companies can either create their own internal methodology or use an existing methodology, but most often specialists conduct security testing according to well-known methods.

The article deals with a comparative analysis of methods and standards for testing the security of systems, networks, and web applications. The following were considered: OWASP WSTG web application security testing methodologies, NIST SP 800-115 Technical Information Security Testing and Evaluation Manual, PTES Penetration testing standard, ISSAF information system security assessment methodology, OSSTMM open source security testing methodology, BSI penetration testing model study methodology, Positive Technologies methodology. Their strengths and weaknesses have been identified. Based on the analysis, a methodology is proposed that focuses on efficiency, ease of implementation and adaptation to various projects. The prac-

tical significance of the work lies in the possibility of its application to increase the level of security in information systems. The results of the study may be useful to information security specialists and organizations seeking to minimize the risks of cyber attacks.

Keywords: security testing, vulnerability analysis, risk assessment, testing methodology, information security

For citation: Shukenbaev, A.B., Ziatdinova, K.R. and Shukenbaeva, N.Sh. (2025), "Development of a methodology for testing the security of IT projects", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 2, pp. 80–92, DOI: 10.28995/2686-679X-2025-2-80-92

Введение

Стремительное развитие информационных технологий и увеличение числа киберугроз приводят к росту случаев несанкционированного доступа к конфиденциальной информации и анализу ее уязвимостей. Снизить их уровень можно как с помощью совершенствования систем информационной безопасности, так и с помощью проведения процесса проверки текущего состояния защищенности информационных систем, то есть их тестирования на безопасность. Тестирование безопасности проектов является необходимым первым шагом для организаций любых размеров, целью которых является определение уровня информационной безопасности и ее повышения для укрепления защиты с течением времени. В связи с этим становится актуальным проведение анализа известных методик и стандартов тестирования безопасности проектов и на их основе разработка собственной.

Основная часть

Тестирование безопасности является одним из основных процессов, обеспечивающих устойчивость современных информационных систем к различным современным угрозам.

Для всестороннего анализа процессов обеспечения безопасности проектов рассмотрены методики, которые широко применяются в индустрии: OWASP Web Security Testing Guide, стандарт NIST SP 800-115, стандарт PTES, методика Positive Technologies, методика ISSAF, методика OSSTMM и методика BSI Study a Penetration Testing Model. Каждая из них представляет собой комплексный подход к оценке защищенности, охватывающий различные аспек-

ты информационных систем и их инфраструктуры [Захаров 2023; Шукенбаев, Мирзоева 2022; Бакин, Ниязова, Шведова 2023].

OWASP Web Security Testing Guide – это методическое руководство, разработанное для проведения всестороннего тестирования безопасности веб-приложений[1].

Стандарт NIST SP 800-115 представляет собой руководство по проведению технического анализа безопасности и тестирования информационных систем[2].

Стандарт PTES – это методическое руководство для проведения тестирования на проникновение, охватывающее весь цикл выполнения проверки безопасности информационных систем[3].

Российская компания Positive Technologies предлагает методику тестирования безопасности, основное внимание в которой уделяется анализу уязвимостей, моделированию атак и предоставлению рекомендаций по устранению выявленных проблем[4].

Методика ISSAF представляет собой универсальное руководство для специалистов по информационной безопасности, позволяя проводить комплексный анализ инфраструктуры организации[5].

Методика OSSTMM направлена на выявление уязвимостей, анализ рисков и выработку рекомендаций для улучшения уровня защищенности[6].

Методика BSI Study a Penetration Testing Model разработана с целью обеспечения систематического подхода к проверке защищенности информационных систем, их компонентов и процессов[7].

---

[1] OWASP Web Security Testing Guide // OWASP Foundation. URL: https://owasp.org/www-project-web-security-testing-guide/ (дата обращения 08.01.2025).

[2] NIST SP 800-115. Technical Guide to Information Security Testing and Assessment // National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/ (дата обращения 08.01.2025).

[3] Penetration Testing Execution Standard (PTES). URL: http://www.pentest-standard.org/ (дата обращения 08.01.2025).

[4] Методология тестирования безопасности // Positive Technologies. URL: https://www.ptsecurity.com/ (дата обращения 09.01.2025)

[5] Information Systems Security Assessment Framework // ISSAF. URL: https://www.oissg.org/issaf/ (дата обращения 09.01.2025).

[6] OSSTMM: The Open Source Security Testing Methodology Manual // ISECOM. URL: https://www.isecom.org/ (дата обращения 09.01.2025).

[7] Study A Penetration Testing Model // Federal Office for Information Security (BSI). URL: https://www.bsi.bund.de/ (дата обращения 10.01.2025).

Анализ существующих подходов к тестированию безопасности продемонстрировал разнообразие методик, каждая из которых обладает уникальными характеристиками и областью применения:

1) гибкость и применимость: OWASP WSTG и PTES обеспечивают высокую гибкость для тестирования веб-приложений и инфраструктуры, тогда как NIST SP 800-115 и OSSTMM имеют более универсальный характер, позволяя тестировать как сети, так и приложения в различных сценариях;
2) регуляторные требования: NIST SP 800-115 и BSI Study Penetration Testing Model ориентированы на государственные стандарты, такие как стандарты США и Германии соответственно;
3) структурированность: OSSTMM и Positive Technologies предлагают высоко структурированные подходы с четким разделением по этапам и блокам тестирования, что упрощает их использование в крупных проектах;
4) инструменты: Positive Technologies выделяется использованием собственных инструментов для автоматизации тестирования и анализа уязвимостей, в то время как другие методики, такие как OWASP WSTG и PTES, полагаются на общеизвестные открытые решения и ручное тестирование.

Все проанализированные методики предоставляют эффективные средства для тестирования безопасности, но различаются по своему фокусу и области применения. Для веб-приложений лучше всего подходит OWASP WSTG, в то время как для инфраструктурного тестирования и аудита безопасности лучше выбирать NIST SP 800-115 или OSSTMM. Методики PTES и Positive Technologies могут быть полезны при проведении масштабных тестирований на проникновение с акцентом на глубокий анализ инфраструктуры и приложения.

Разработка современных методик тестирования безопасности базируется на интеграции проверенных практик и современных подходов, что позволяет учесть как известные угрозы, так и новые векторы атак. Усовершенствованная методика объединяет сильные стороны популярных подходов OWASP Web Security Testing Guide, ISSAF, OSSTMM, NIST SP 800-115, PTES и методологии Positive Technologies.

ЭТАП 1: Подготовительный. Подготовительный этап тестирования безопасности является ключевым, так как от его качества зависит точность и эффективность всех последующих действий. В рамках данного этапа были выполнены следующие шаги.

1. *Определение целей тестирования*. Четкое формулирование целей, которые необходимо достичь в процессе тестирования, обес-

печивает согласованность действий и позволяет сфокусироваться на приоритетных задачах. Цели были определены следующим образом:

– проверить устойчивость системы к наиболее распространенным типам атак, таким как SQL-инъекции, межсайтовый скриптинг (XSS) и атаки с использованием уязвимостей конфигурации;
– оценить конфигурацию серверов, чтобы выявить ошибки, которые могут привести к компрометации системы;
– определить уровень защиты пользовательских данных, включая методы шифрования и политики авторизации;
– для каждой цели были разработаны критерии успеха, которые позволят однозначно оценить результаты тестирования.

2. *Идентификация целевой системы*. На этом шаге была собрана информация о тестируемом приложении и его окружении. Исходные данные включали:

– IP-адрес целевой системы: 192.168.1.10, что позволило установить базовый доступ к серверу;
– используемые технологии: веб-сервер Apache версии 2.4, язык программирования PHP 5.4.16 и база данных MySQL.

Эта информация была использована для планирования тестов и выбора соответствующих инструментов анализа.

3. *Определение границ тестирования*.

Для минимизации рисков и соблюдения этических стандартов были установлены следующие границы тестирования. Тестирование проводилось в изолированной среде, созданной на базе локального сервера. Это исключило влияние на внешние системы и сети. DoS-атаки и любые действия, которые могли бы нарушить работоспособность системы, были исключены из сценария тестирования. Анализ ограничивался только веб-компонентами и конфигурацией серверного окружения, без затрагивания файловой системы. Данные ограничения обеспечили безопасное и этичное выполнение тестов, соответствующее согласованным параметрам.

4. *Согласование параметров тестирования*. Были рассмотрены технические и организационные аспекты выполнения работ.

Выбор инструментов тестирования. Для достижения поставленных целей были отобраны инструменты, соответствующие задачам этапа:

– Nmap: для сбора информации о сетевых сервисах и открытых портах;
– Nikto: для анализа настроек веб-сервера и выявления потенциальных проблем;
– OWASP ZAP: для автоматизированного поиска уязвимостей в веб-приложении, включая SQL-инъекции и XSS.

Инструменты выбирались, исходя из их надежности, совместимости с целевой системой и способностью эффективно выявлять уязвимости.

5. *Подготовка инфраструктуры*. Включала в себя:
- установку и настройку тестового приложение на локальном сервере;
- проведению проверки доступности сервера с использованием команд ping и базовых HTTP-запросов через браузер.

6. *Проверка корректности настроек и функциональности всех компонентов*. Результаты этого этапа были задокументированы в отчете, который включал описание целевой системы, перечень используемых инструментов и критерии оценки результатов тестирования. Каждый шаг был направлен на создание четкой и понятной структуры для дальнейших действий, что позволило минимизировать ошибки и обеспечить максимальную эффективность тестирования.

ЭТАП 2: Анализ угроз и рисков. Это один из ключевых этапов тестирования безопасности, который позволяет выявить уязвимости системы и оценить возможные последствия их эксплуатации.

1. *Идентификация активов* необходима для определения критически важных элементов системы, которые требуют повышенного внимания в процессе тестирования. Выделены следующие активы:
- веб-приложение: включает исходный код, настройки и базовые функции;
- сервер: операционная система, веб-сервер Apache, база данных MySQL;
- данные пользователей: информация об учетных записях, включая пароли, сохраненные данные форм.

Для каждого из этих активов определена значимость и оценены возможные угрозы.

2. *Выявление угроз*, которые могут затронуть обнаруженные активы. Анализ выполнен на основе известных векторов атак для веб-приложений:
- SQL-инъекции: возможность получения несанкционированного доступа к данным через некорректно обработанные пользовательские запросы;
- межсайтовый скриптинг (XSS): риск выполнения вредоносного JavaScript-кода на стороне клиента;
- ошибки конфигурации: использование небезопасных настроек серверов и баз данных, включая открытые порты или слабые пароли.

Каждая угроза была описана с точки зрения возможного механизма эксплуатации и ожидаемого воздействия на активы системы.

3. *Оценка рисков.* Для приоритизации угроз выполнена их оценка с использованием матрицы рисков, основанной на двух параметрах. Составлена таблица рисков, которая позволяет фокусироваться на наиболее критичных угрозах. Угрозы и риски представлены в табл. 1.

Таблица 1

Риски для наиболее критичных угроз

Угроза	Вероятность	Последствия	Уровень риска
SQL-инъекции	4	5	Высокий
Межсайтовый скриптинг	3	4	Средний
Ошибки конфигурации	2	3	Низкий

4. *План управления рисками.* На заключительном этапе был создан план действий по управлению выявленными рисками. Он включает:

Превентивные меры:
- реализация защиты от SQL-инъекций с использованием параметризованных запросов и фильтрации ввода;
- защита от XSS путем внедрения политик Content Security Policy (CSP) и экранирования пользовательских данных [Скабцов 2018];
- настройка безопасной конфигурации серверов, включая ограничение доступов и использование сложных паролей.

Меры обнаружения:
- настройка логирования попыток несанкционированного доступа и подозрительных действий;
- мониторинг серверов и приложений с использованием инструментов.

Реактивные меры:
- составление процедур реагирования на инциденты, включая уведомление ответственных лиц и восстановление данных.

Разработанный план был задокументирован и утвержден для дальнейшего использования в тестировании. Этот этап обеспечил понимание текущего уровня защищенности системы и задал направление для устранения обнаруженных рисков.

ЭТАП 3: Тестирование системы на уязвимости. Является практическим этапом, направленным на выявление уязвимостей

в приложении. Выполнены следующие действия, соответствующие разработанной методике.

1. Подготовка инструментов тестирования. Каждый из инструментов был установлен на тестовой машине, а их настройки приведены в соответствие с требованиями методики.

2. Проведение анализа уязвимостей. Анализ выполнялся поэтапно, с использованием выбранных инструментов.

3. Анализ с помощью Burp Suite:

– настроен прокси-сервер для перехвата запросов;
– проведено ручное тестирование, включающее модификацию параметров запросов;
– использованы автоматизированные модули для проверки на SQL-инъекции и XSS.

4. Сканирование OWASP ZAP. Проведено активное сканирование целевого сайта. Зафиксированы обнаруженные уязвимости, включая небезопасные параметры.

5. Сканирование Nmap. Выполнен анализ открытых портов с использованием команды: nmap -sV -p 1-65535. Проверены версии программного обеспечения на уязвимости (рис. 1).

```
Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-02 14:25 UTC
Nmap scan report for 192.168.0.101
Host is up (0.0010s latency).
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

Nmap scan report for 192.168.0.102
Host is up (0.0020s latency).
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https

Nmap scan report for 192.168.0.103
Host is up (0.0030s latency).
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http

Nmap scan report for 192.168.0.104
Host is up (0.0040s latency).
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap scan report for 192.168.0.105
Host is up (0.0050s latency).
PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 5 IP addresses (5 hosts up) scanned in 3.25 seconds
```

Рис. 1. Сканирование Nmap

6. Тестирование веб-сервера с помощью Nikto:

Выполнена проверка конфигураций веб-сервера командой: nikto-h. Обнаружены устаревшие версии программного обеспечения и потенциальные угрозы.

На основании проведенного анализа были получены результаты, представленные в табл. 2.

Таблица 2

Результаты анализа

Уязвимость	Инструмент	Описание
SQL-инъекция в форме логина	Burp Suite	Возможность выполнения произвольных SQL запросов.
Межсайтовый скриптинг (XSS)	OWASP ZAP	Уязвимость, позволяющая внедрить вредоносный скрипт.
Открытые порты 22 и 3306	Nmap	Возможные цели для эксплуатации.
Небезопасная конфигурация сервера	Nikto	Устаревшие версии ПО и ошибки конфигурации.

7. Создание отчета по тестированию. Для каждой обнаруженной уязвимости были разработаны рекомендации по ее устранению, представленные в итоговом отчете.

Пример рекомендаций.

1) SQL-инъекции – использование параметризованных запросов;
2) XSS – экранирование пользовательских данных и настройка Content Security Policy (CSP);
3) открытые порты – закрытие неиспользуемых портов и настройка правил брандмауэра;
4) ошибки конфигурации – обновление серверного ПО до актуальных версий.

Ключевые преимущества методики:

– интеграция лучших практик – объединяя сильные стороны всех упомянутых методологий, новая методика позволяет охватывать не только стандартные угрозы, но и учитывать особенности тестируемой системы, обеспечивая высокий уровень гибкости и адаптации;
– системный подход – в отличие от некоторых методов, сосредоточенных на отдельных аспектах тестирования, разрабо-

танная методика охватывает весь жизненный цикл проверки безопасности: от сбора информации до формулирования рекомендаций. Это позволяет исключить слепые зоны и минимизировать риски;
– улучшенная аналитика – методы анализа угроз и рисков были дополнены автоматизированными инструментами, что дало возможность эффективно выявлять как поверхностные, так и глубокие уязвимости, которые могут быть упущены при применении только одной из методик;
– упрощение процесса отчетности – разработанный формат отчета структурирован таким образом, чтобы результаты были легко воспринимаемы как техническими специалистами, так и управленческим персоналом, способствуя эффективному принятию решений;
– практическая ценность – внедрение инструментов, таких как Burp Suite, OWASP ZAP, Nmap и Nikto, позволяет проводить как детализированный анализ вручную, так и массовое автоматическое сканирование. Это улучшает масштабируемость тестирования и точность результатов.

Заключение

Проведенный анализ подтвердил важность тестирования безопасности как ключевого элемента обеспечения устойчивости информационных систем к современным угрозам. В рамках работы были рассмотрены семь методик, такие как OWASP WSTG, NIST SP 800-115, PTES, ISSAF, OSSTMM, BSI и Positive Technologies. На их основе разработана улучшенная методика, которая объединяет сильные стороны этих подходов, включая детализированный анализ уязвимостей, сочетание ручных и автоматизированных методов тестирования, а также адаптацию к различным типам проектов.

Практическое применение методики на тестовом веб-приложении подтвердило ее эффективность в выявлении критических уязвимостей и предложении мер для их устранения. Разработанная методика может быть применена как для внутренних проверок безопасности, так и для внешних аудитов, что делает ее универсальной и актуальной для организаций в различных отраслях.

Литература

Бакин, Ниязова, Шведова 2023 – *Бакин И.Б., Ниязова К.Ш., Шведова С.М.* Проблемы управления рисками в сфере информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 3. С. 49–60.

Захаров 2023 – *Захаров Д.И.* Управление рисками информационной безопасности. М.: Финансы и статистика, 2023. 300 с.

Скабцов 2018 – *Скабцов Н.* Аудит безопасности информационных систем. СПб.: Питер, 2018. 272 с.

Шукенбаев, Мирзоева 2022 – *Шукенбаев А.Б., Мирзоева Л.В.* Сравнительный анализ методик тестирования безопасности проектов // Теория и практика обеспечения информационной безопасности: Сб. трудов II Всероссийской научно-практической конференции (2 ноября 2022 г. Москва, МТУСИ). М., 2022. С. 176–184.

References

Bakin, I.B., Niyazova, K.Sh. and Shvedova, S.M. (2023), "Issues of risk management in the field of information security", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 49–60.

Skabtsov, N. (2018), *Audit bezopasnosti informatsionnykh sistem* [Audit of information systems security], Peter, St. Petersburg, Russia, 272 p.

Shukenbaev, A.B. and Mirzoeva, L.V. (2022), "Comparative analysis of project safety testing methods", *Theory and practice of information security. Coll. of articles of the 2nd All-Russian Scientific and Practical Conference (November 2, 2022. Moscow. MTUSHI)*, Moscow, Russia, pp. 176–184.

Zakharov, D.I. (2023), *Upravlenie riskami informatsionnoi bezopasnosti* [Information Security risk management], Finance and Statistics, Moscow, Russia, 300 p.

Информация об авторах

Айрат Б. Шукенбаев, кандидат технических наук, доцент, МИРЭА – Российский технологический университет, Москва, Россия; 119454, Россия, Москва, Проспект Вернадского, д. 78, shukenbaev@mirea.ru

Камилла Р. Зиатдинова, МИРЭА – Российский технологический университет, Москва, Россия; 119454, Россия, Москва, Проспект Вернадского, д. 78, kziatdinova@gmail.com

Наиля Ш. Шукенбаева, кандидат сельскохозяйственных наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; nelshuk@mail.ru

Information about the author

Airat B. Shukenbaev, Cand. of Sci. (Mechanical Engineering), associate professor, MIREA – Russian Technological University, Moscow, Russia; bld. 78, Vernadskogo Av., Moscow, 119454, Russia; shukenbaev@mirea.ru

Kamilla R. Ziatdinova, MIREA – Russian Technological University, Moscow, Russia; bld. 78, Vernadskogo Av., Moscow, 119454, Russia; kziatdinova@gmail.com

Nailya Sh. Shukenbaeva, Cand. of Sci. (Agriculture), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, 125047, Russia; nelshuk@mail.ru

Научный журнал
Вестник РГГУ
Серия «Информатика.
Информационная безопасность. Математика»
№ 2
2025

Дизайн обложки
Е.В. Амосова

Корректор
П.М. Смоктунова

Компьютерная верстка
Н.В. Москвина

Учредитель и издатель
Российский государственный гуманитарный университет
125047, Москва, Миусская пл., 6

Свидетельство о регистрации СМИ
ПИ № ФС77-72977 от 25.05.2018 г.
Периодичность 4 раза в год

Подписано в печать 28.05.2025
Выход в свет 05.06.2025
Формат 60×90 1/16
Уч.-изд. л. 5,7. Усл. печ. л. 5,9
Тираж 1050 экз. Свободная цена
Заказ № 2173

Отпечатано в типографии Издательского центра
Российского государственного гуманитарного университета
125047, Москва, Миусская пл., 6
www.rsuh.ru