

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет геосистем и технологий»
(СГУГиТ)

ИНТЕРЭКСПО ГЕО-СИБИРЬ

XXII Международный научный конгресс

Сборник материалов в 9 т.

Т. 6

Магистерская научная сессия

«ПЕРВЫЕ ШАГИ В НАУКЕ»

Новосибирск
СГУГиТ
2026

Ответственные за выпуск:

Сырнева А. С. – модератор магистерской научной сессии, канд. техн. наук, доцент кафедры физики

Рыжкова Е. В. – секретарь магистерской научной сессии, старший преподаватель кафедры информационной безопасности

Рецензенты:

Хацевич Т. Н. – канд. техн. наук, профессор кафедры фотоники

Никулин Д. М. – канд. техн. наук, доцент, заведующий кафедрой фотоники и приборостроения

Михайлов И. О. – канд. техн. наук, доцент кафедры фотоники и приборостроения

Карманов И. Н. – канд. техн. наук, доцент, заведующий кафедрой физики

Сырнева А. С. – канд. техн. наук, доцент кафедры физики

Михайлова Д. С. – канд. техн. наук, доцент кафедры физики

Усанькова Е. А. – канд. техн. наук, доцент кафедры специальных устройств, инноватики и метрологии

Троеглазова А. В. – доктор философии, доцент кафедры информационной безопасности

Титов Д. Н. – канд. техн. наук, доцент кафедры информационной безопасности

Белов В. М. – д-р техн. наук, профессор кафедры информационной безопасности

Чермошенцев А. Ю. – канд. техн. наук, доцент кафедры фотограмметрии и дистанционного зондирования

С26 Интерэкспо ГЕО-Сибирь. XXII Международный научный конгресс, 18–22 мая 2026 г., Новосибирск : сборник материалов в 9 т. Т. 6: Магистерская научная сессия «Первые шаги в науке». – Новосибирск : СГУГиТ, 2026. – 248 с. – ISSN 2618-981X. – Текст : непосредственный.

DOI 10.33764/2618-981X-2026-6

В сборнике опубликованы материалы XXII Международного научного конгресса «Интерэкспо ГЕО-Сибирь», представленные на Магистерской научной сессии «Первые шаги в науке».

Печатается по решению редакционно-издательского совета СГУГиТ

Материалы публикуются в авторской редакции

Издание может содержать сведения об иностранных агентах

УДК 528

© СГУГиТ, 2026

Д. М. Агеев^{1✉}, Д. М. Никулин¹

Стенд для контроля центрировки линз

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: 13aaaa.dima09@gmail.com

Аннотация. В данной статье предложена оптическая схема стенда для контроля центрировки линз, который является важным этапом при производстве оптических и оптико-электронных приборов и систем. В ней подробно описаны основные принципы работы стенда, его конструктивные элементы, а также методы измерения точности центрировки линз, что позволяет понять весь процесс. Статья подчеркивает значимость точной центрировки для достижения высококачественного изображения и повышения общей эффективности оптических устройств, так как небольшие отклонения могут привести к искажению изображения или снижению эффективности прибора. Поэтому разработка и усовершенствование таких стендов для контроля центрировки являются важными направлениями исследований в области оптики. Такой подход поможет в дальнейшем усовершенствовании производственных процессов и технологий в оптике.

Ключевые слова: оптическая схема стенда, контроль центрировки линз, оптические системы

D. M. Ageev^{1✉}, D. M. Nikulin¹

Lens Centering Verification Stand

¹ Siberian State University of Geosystems and Technology, Novosibirsk, Russian Federation
e-mail: 13aaaa.dima09@gmail.com

Abstract. This article proposes an optical scheme for a bench to control lens alignment, which is an important stage in the production of optical and optoelectronic devices and systems. It describes in detail the basic principles of the bench operation, its structural elements, as well as methods for measuring lens alignment accuracy, allowing for a comprehensive understanding of the entire process. The article emphasizes the importance of precise alignment for achieving high-quality images and improving the overall efficiency of optical devices, as small deviations can lead to image distortion or reduced device performance. Therefore, the development and improvement of such alignment control benches are important research areas in optics. This approach will help in further improving production processes and technologies in optics.

Keywords: optical scheme of the stand, lens centering control, optical systems

Введение

Научно-технический прогресс в сфере оптического приборостроения связан с непрерывным совершенствованием технологических процессов, направленных на изготовление оптических деталей.

Внедрение новых видов инструментов и приемов работы, а также применение автоматизированных систем и новых форм организации труда оказывают су-

щественное влияние на эволюцию технологических процессов, используемых при производстве оптических компонентов.

Центрирование линз представляет собой важный аспект, напрямую влияющий на качество формируемого изображения и общую функциональность оптических приборов [1-4]. Стенд для контроля центрировки линз представляет собой специальное оборудование, предназначенное для точной настройки и проверки положения оптических элементов, в данном случае линз, что обеспечивает достижение требуемых характеристик и параметров в конечном изделии.

Оптический метод контроля центрировки линз

Оптическая схема включает в себя светодиод или лазерный источник, светоделительный куб, защитные плоскопараллельные стекла, в плоскости наблюдения расположено фотоприемное устройство. Схема позволяет работать как на отражение (от обеих поверхностей) (рис. 1), так и на просвет [5].

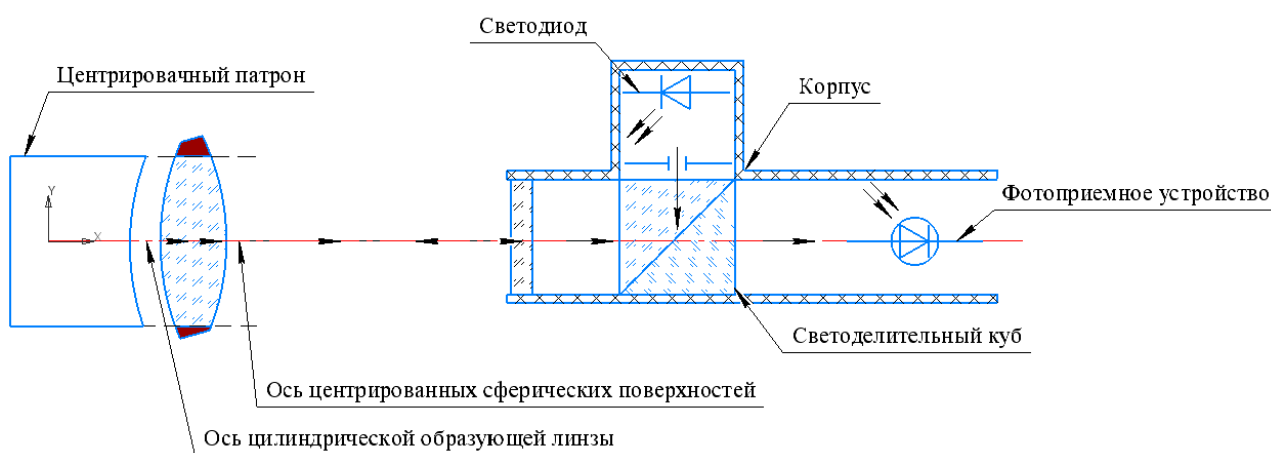


Рис. 1. Оптическая схема системы центрирования

Луч лазера, исходящий из источника, направляется на светоделительный кубик – оптический элемент, выполненный из двух склеенных под углом стеклянных призм с многослойным диэлектрическим покрытием на внутренней грани. При прохождении через кубик часть луча отражается от покрытия в сторону контролируемой линзы, а часть проходит сквозь него, что обеспечивает разделение входного луча на два с определенным соотношением интенсивностей.

Отраженная от светоделительного кубика часть лазерного луча далее падает на первую поверхность линзы, часть излучения отражается, а другая преломляется в линзу. Часть преломленного луча отражается от второй грани линзы и возвращается обратно. Отраженные от двух поверхностей линзы лучи формируют в плоскости наблюдения два пятна в точках В и D разнесенных от гипотетической точки А – места, где должны совпасть два отраженных луча при идеальной центрировке линз. Не совпадение свидетельствует о децентрировании контролируемой линзы (рис. 2).

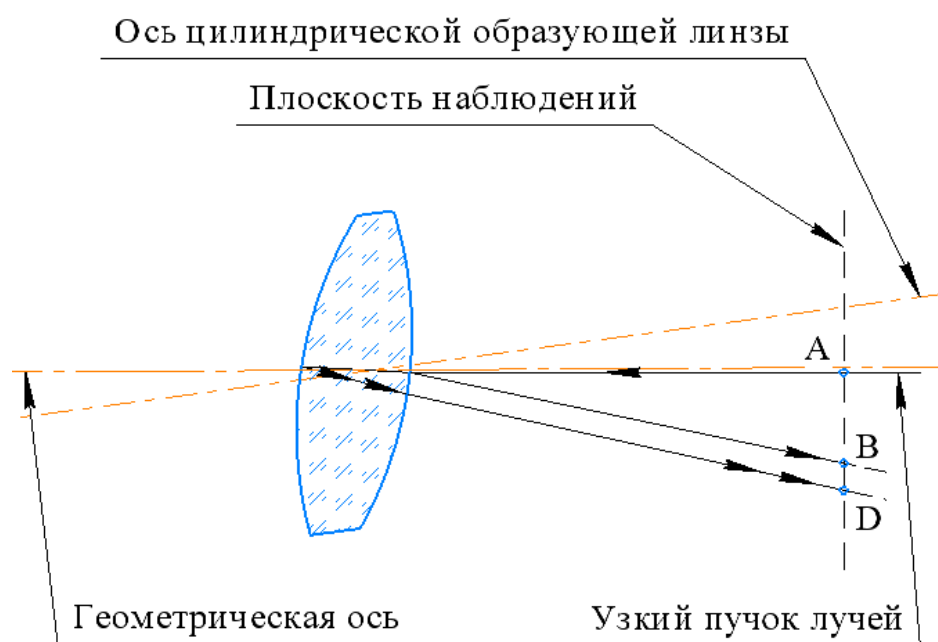


Рис. 2. Автоколлимация от двух сферических нецентрированных поверхностей

Основная идея состоит в том, чтобы определить, насколько сильно точки В и D отклоняются от точки А.

Затем выполняется совмещение двух точек в одну, путем настройки центрировочного патрона микродвижками для обеспечения необходимой точности оптической детали (рис. 3).

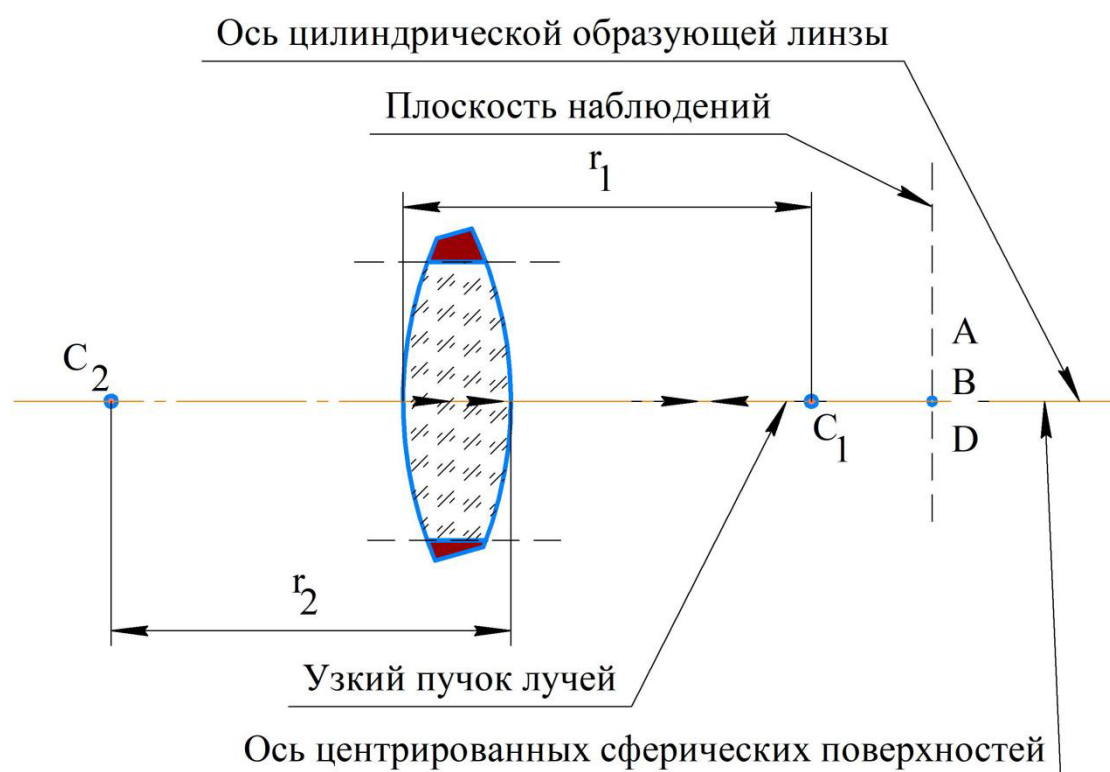


Рис. 3. Центрированная линза

Анализ смещений и искажений световых пятен, будут нести информацию о следующих параметрах центрируемой линзы:

- угловое отклонение центрируемой линзы;
- радиус кривизны линзы.

Результаты

В ходе исследования была предложена оптическая схема стенда для контроля центрирования линз. Данный стенд позволяет с помощью микроподвижек центрировачного патрона совместить геометрический центр с оптической осью линзы для дальнейшей ее центрировки.

Заключение

Оптический стенд для проверки центрирования линз является ключевым устройством для достижения высокой точности и качества оптических систем. Анализ данной проблемы подтверждает необходимость применения подобных стендов на оптических предприятиях, где изготавливаются оптически и оптико-электронные приборы. Дальнейшие исследования могут быть направлены на оптимизацию конструкции стенда.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бобылева Е. Г. Оптические технологии и материалы. Центрирование линз: методические указания / Бобылева Е. Г., Парко И. В. – Новосибирск : СГУГиТ, 2024. – 6 с. – Текст : непосредственный.
2. Справочник технолога-оптика / М.А. Окатов, Э.А. Антонов, А. Байгожин и др.; Под ред. М.А. Окатова. – 2-е изд., перераб. и доп. – Санкт-Петербург : Политехника, 2004. – 679 с. – Текст : непосредственный.
3. Сулим А. В., Производство оптических деталей: А. В. Сулим. Учебник «Производство оптических деталей». – 2-е изд. перераб. и доп. "Высшая школа" Москва, 1969 – 304 с. – Текст : непосредственный.
4. Грачева И. Н. Геометрическая оптика. Центрированные оптические системы: методические указания / Грачева И. Н., Филиппова Е. А., Фишман А. И. – Казань: Казан. ун-т, 2017. – 31 с. – Текст : непосредственный.
5. Михайлов, И. О. CAD-технологии. Проектирование технической системы методом «сверху вниз» : учебно-методическое пособие / И. О. Михайлов. – Новосибирск : СГУГиТ, 2020. – 204 с. – [Электронный ресурс]. – URL: <https://e.lanbook.com/book/222320>.

© Д. М. Агеев, Д. М. Никулин, 2026

А. А. Ануфриева¹✉, А. Ю. Чермошенцев¹

Методика выполнения обмерных работ методом наземной фотограмметрической съемки с применением панорамных камер

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: anufrievaanastasia167@mail.ru

Аннотация. В статье рассматривается методика выполнения высокоточных обмерных работ с использованием наземной фотограмметрической съемки и панорамных камер. Актуальность исследования обусловлена возрастающей потребностью в быстрой и детальной трехмерной документации объектов культурного наследия, промышленных сооружений и сложных архитектурных пространств. Выполнена обработка материалов съемки в специализированном программном обеспечении, предложена оптимальная технологическая схема полевых и камеральных работ. Описаны основные этапы выполнения съемки и обработки ее результатов на примере тестового объекта. Применение панорамных камер позволяет сократить время полевого этапа при достижении требуемой точности.

Ключевые слова: наземная фотограмметрия, панорамные камеры, обмерные работы, Agisoft Metashape, точность съемки.

A. A. Anufrieva¹✉, A. Y. Chermoshentsev¹

Methodology of Surveying Works Using Terrestrial Photogrammetry with Panoramic Cameras

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: anufrievaanastasia167@mail.ru

Abstract. The article examines a modern methodology for performing high-precision surveying work using terrestrial photogrammetry based on panoramic cameras. The relevance of the study is driven by the growing need for rapid and detailed three-dimensional documentation of cultural heritage sites, industrial facilities, and complex architectural spaces. Work was carried out using specialized software, and an optimal technological workflow for field and office work is proposed. The main stages of surveying and data processing are described using a test object as an example. The use of panoramic cameras allows for a reduction in the time required for the field stage and to achieve required accuracy.

Keywords: terrestrial photogrammetry, panoramic cameras, surveying works, Agisoft Metashape, survey accuracy

Введение

Современные отрасли, такие как геодезия, архитектура, реставрация и промышленный инжиниринг, сталкиваются с растущим спросом на высокоточные и детализированные трехмерные модели сложных объектов. Существующие ме-

тоды измерений зачастую трудозатратны и не отвечают требованиям к полноте и оперативности данных.

Наземная фотограмметрия представляет собой бесконтактный, эффективный и точный подход к документированию, однако стандартные фотограмметрические системы, использующие одиночные камеры, могут быть неоптимальны для сложных пространств, требуя большого количества снимков и времени на их получение [1, 2].

Внедрение панорамных камер является перспективным шагом для оптимизации наземной фотограмметрической съемки, предлагая ряд ключевых преимуществ. Их способность мгновенно фиксировать полную сферу пространства означает, что требуется меньше станций съемки, полевые работы выполняются быстрее, а риск образования «слепых зон» на объекте сводится к минимуму [3, 4].

Целью данного исследования является разработка и анализ методики выполнения обмерных работ с использованием панорамных камер, включая оценку точности и производительности.

Задачи работы: систематизировать требования к планированию съемки, оценить влияние искажений панорамных изображений на точность построения модели и предложить оптимальную технологическую схему обработки данных.

Методы и материалы

В качестве тестового объекта для отработки методики был выбран коридор третьего этажа лабораторного корпуса СГУГиТ. Съемка выполнялась с помощью камеры Insta360 X3, путем прохождения двух маршрутов для обеспечения наилучшего перекрытия.

Обработка данных выполняется в специализированном фотограмметрическом программном обеспечении Agisoft Metashape Professional, поддерживающем работу с эквидистантными и сферическими проекциями и учитывающем модель дисторсии камеры «рыбий глаз». В ходе исследования использовалось программное обеспечение VD Video Capture Tool для разделения материалов съемки двух объективов панорамной камеры на отдельные кадры с заданным интервалом результатов съемки. Общая методика выполнения полевого и камерального этапов представлена на рис. 1.

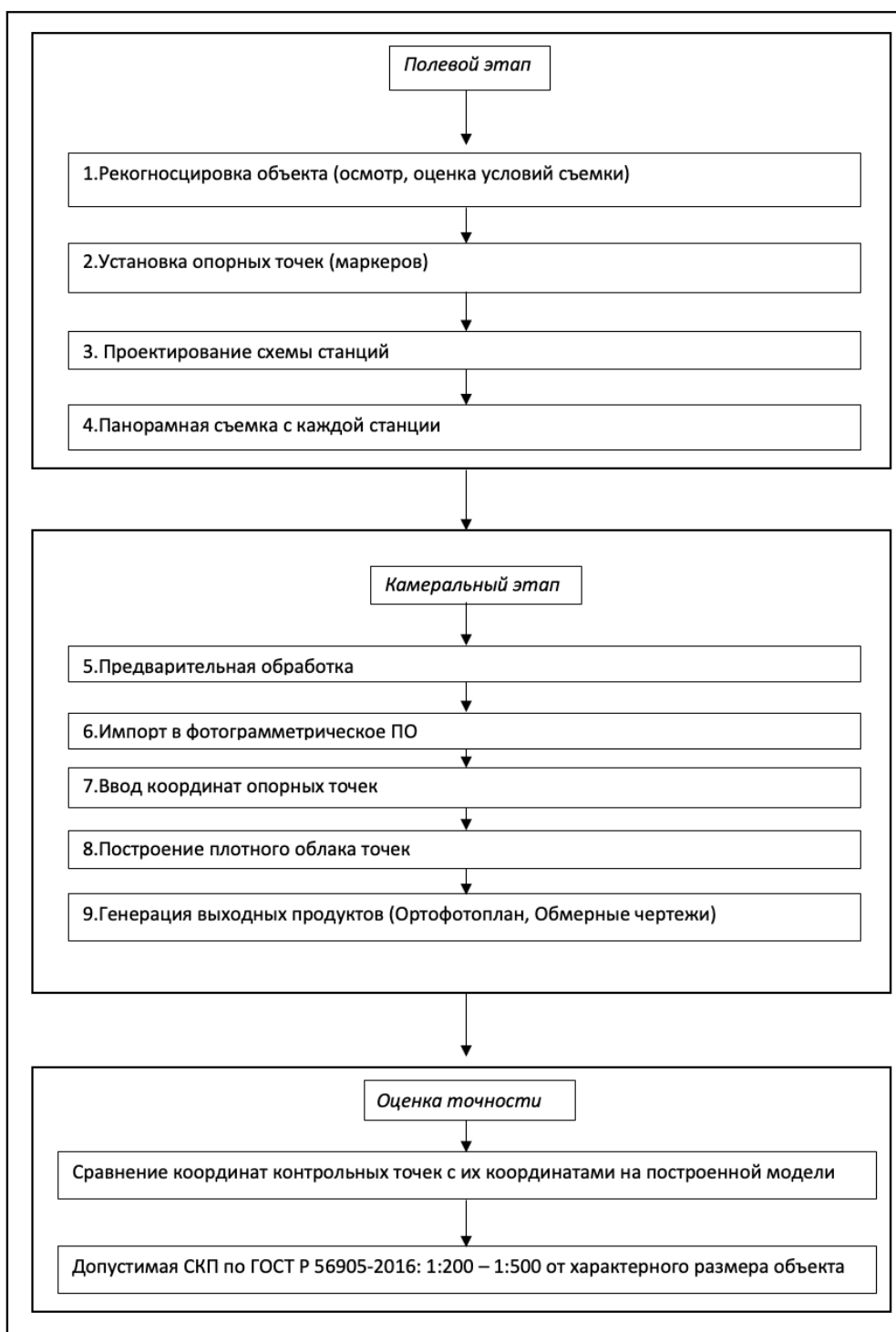


Рис. 1. Технологическая схема панорамной фотограмметрии съемки

Результаты

В результате сформированы два видеофайла, полученных левым и правым объективами, общим объемом 1,8 Гб. Далее выполнялось разделение на отдельные кадры с помощью программного обеспечения VD Video Capture Tool в котором устанавливается временной промежуток между отдельными кадрами не чаще чем 2 секунды (рис.2).

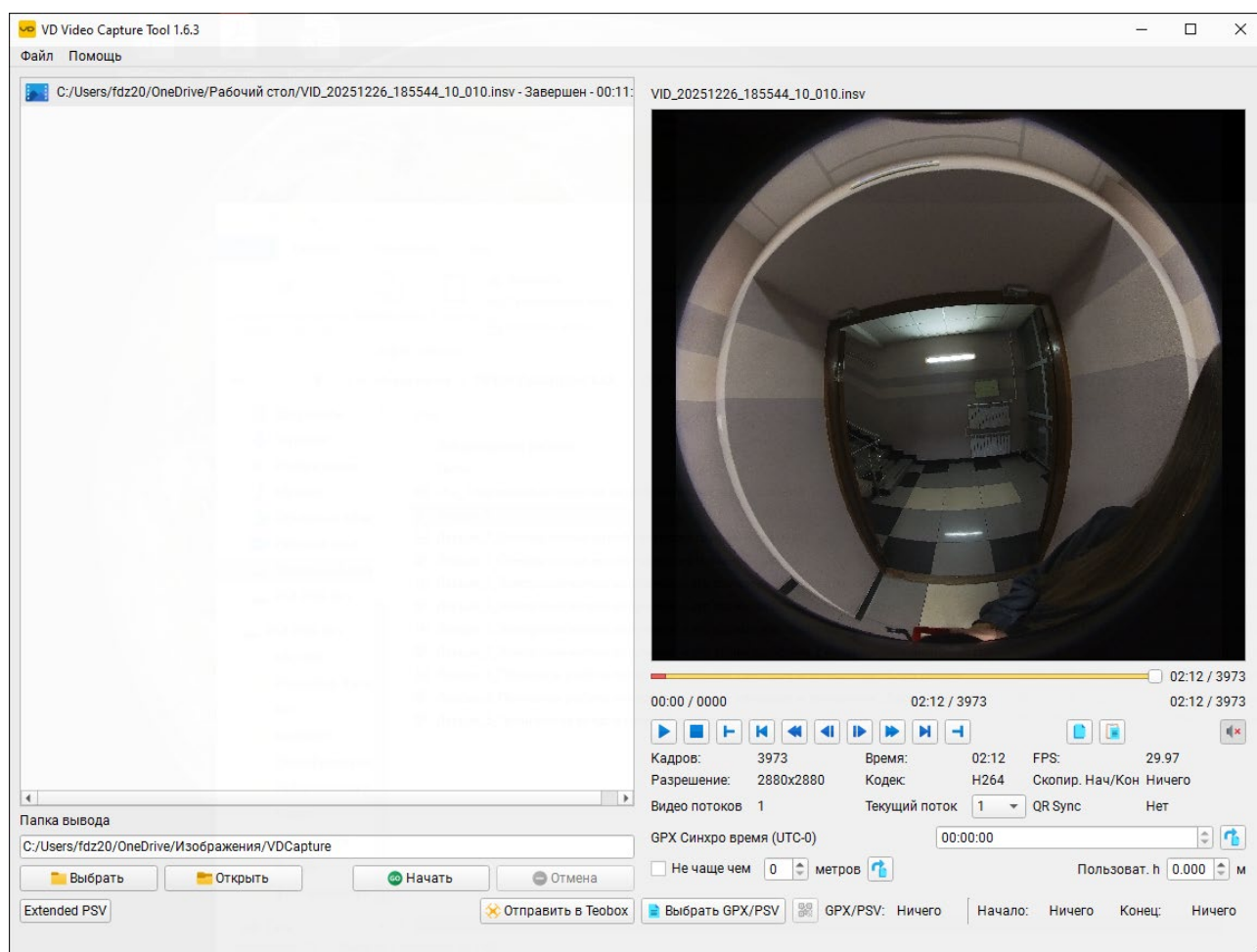


Рис. 2. Процедура разделения на кадры

Обработка выполнялась в Agisoft Metashape. Каждая группа снимков обрабатывалась в отдельном блоке, поскольку калибровка объективов имеет различия. Процедура обработки включала основные операции по ориентированию снимков, определению положения точек фотографирования, фильтрации, построению плотного облака точек и модели, а также их масштабированию. На рис. 3 – 4 представлены результаты основных этапов

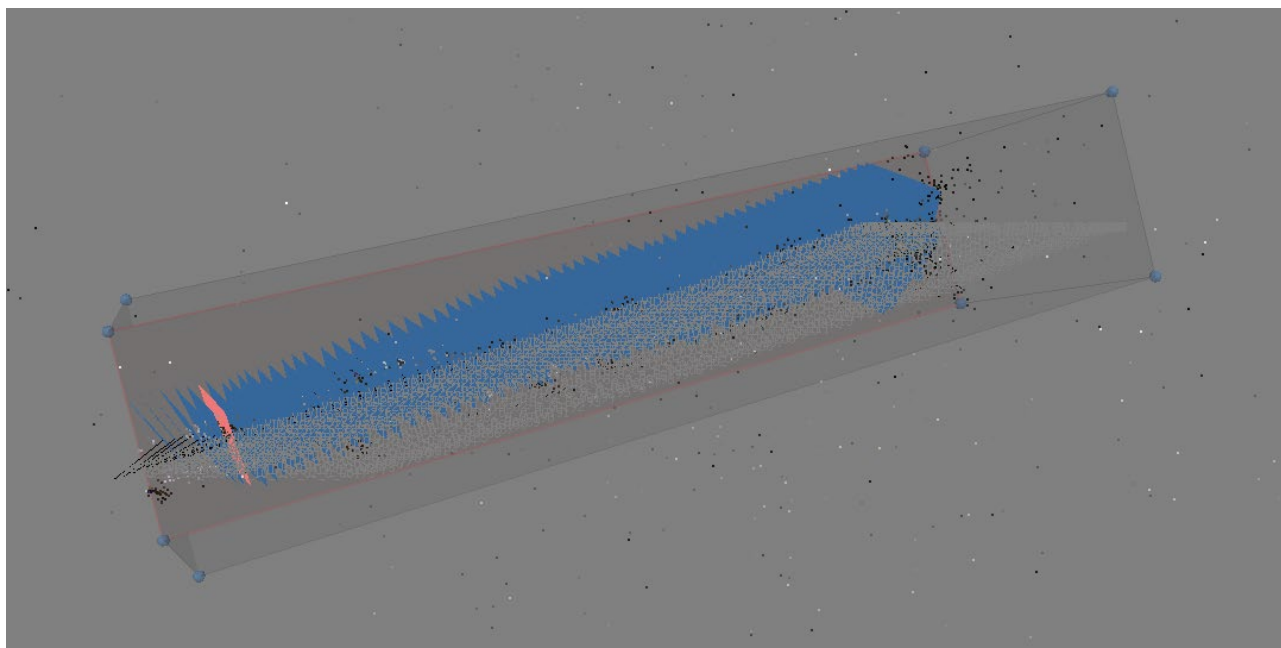


Рис. 3. Расположение снимков после ориентирования



Рис. 4. Плотное облако точек

Недостаточное количество света, попадающее в объектив, приводит к неполному извлечению информации. Из-за недостаточного распознавания точек при построении плотного облака, создаваемая трехмерная модель имеет неровности и артефакты, в связи с чем необходимо проводить ее сглаживание.

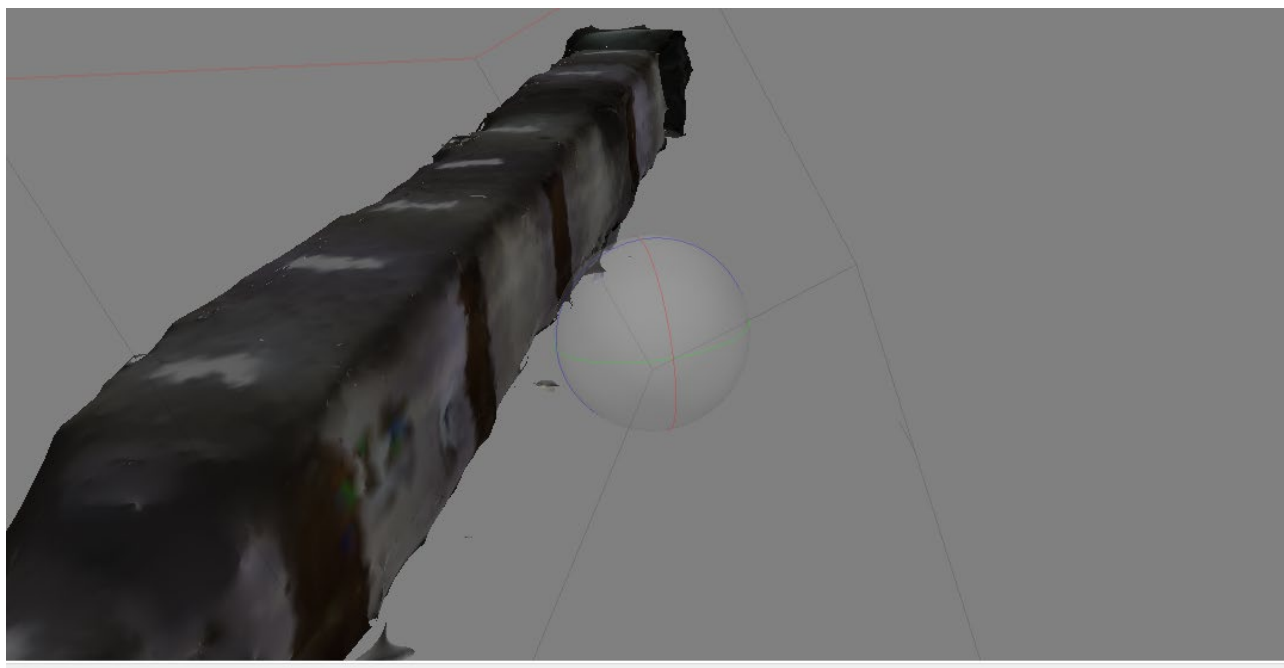


Рис. 5. Трехмерная модель до сглаживания

Точность построения модели оценивалась по расхождениям контрольных измерений, выполненных с помощью рулетки и масштабных линеек, созданных в программе (табл. 1.).

Таблица 1 – Оценка точности построения модели по масштабным линейкам

Масштабные линейки	Расстояние (м)	Ошибка (м)
point 1 point 2	0,54	0,000165
point 3 point 4	1,56	-0,000883
point5 point 6	1,24	-0,002572
point 9 point 10	1,56	-0,000799

По результатам обработки получена максимальная ошибка по масштабной линейке 2,5 мм. Это соответствует масштабу чертежа 1:50 и удовлетворяет требованиям для большинства обмерных задач.

Обсуждение

Полученные результаты согласуются с выводами работ [3, 4, 7]. Однако следует учитывать ряд ограничений:

Панорамные камеры потребительского уровня имеют фиксированное фокусное расстояние и не позволяют менять оптику, что может ограничивать съемку удаленных или очень мелких деталей. Требуется хорошая освещенность. Необходимо применять камеры с большим размером светочувствительной матрицы.

Обработка сферических изображений требует больше оперативной памяти и времени вычислений из-за большого количества исходных файлов.

Искажения на краях панорамы могут приводить к систематическим ошибкам, если не выполнена точная калибровка камеры.

Рекомендуется обязательное геодезическое обеспечение (не менее 4–6 опор-

ных точек на объект) для ориентирования модели в абсолютной системе координат и контроля качества.

Заключение

В ходе исследования разработана и апробирована методика выполнения обмерных работ с применением панорамных камер. Экспериментально подтверждено, что максимальная ошибка по масштабным линейкам составляет 2,5 мм, что соответствует масштабу чертежа 1:50 и удовлетворяет требованиям ГОСТ для большинства обмерных задач.

Методика обеспечивает высокую полноту данных и минимизирует «теневые» зоны за счет регистрации полной сферы вокруг станции съемки. Применение панорамных камер позволяет сократить время полевого этапа за счет уменьшения количества необходимых станций.

Вместе с тем выявлены ограничения: зависимость от освещенности, необходимость точной калибровки камеры и повышенные требования к вычислительным ресурсам при обработке сферических изображений. Рекомендуются обязательное использование не менее 4–6 опорных точек для контроля качества и ориентирования модели.

Дальнейшие исследования будут направлены на автоматизацию процесса распознавания опорных марок на панорамных изображениях и разработку специализированных алгоритмов калибровки многокамерных панорамных систем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Комиссаров А. В., Чермошенцев А. Ю. Наземная фотограмметрия: учеб. -метод. пособие. – Новосибирск: СГУГиТ, 2023. – 84 с.
2. Измestьев, А.Г. Фотограмметрия и дистанционное зондирование территории: учеб. пособие / А.Г. Измestьев. – Кемерово: КузГТУ им. Т.Ф. Горбачева, 2013. – 107 с.
3. Быков, Л.В. Исследование точности элементарных фотограмметрических построений при наземной стереофотограмметрической съемке с одновременным определением координат центров фотографирования / Л.В. Быков, А.А. Федоровский, В.Л. Быков // Изв. вузов. Геодезия и аэрофотосъемка. – 2021. – Т. 65. – N 2. – С. 194-199.
4. Щенявская Л.А., Шевченко Г.Г. Порядок проведения наземной фотограмметрической съемки для получения обмерных чертежей здания // Научные труды КубГТУ. – 2023. – № 3. – С. 52–65.
5. Обиралов, А.И. Фотограмметрия и дистанционное зондирование: учебник / А.И. Обиралов, А.Н. Лимонов, Л.А. Гаврилова. – М.: КолосС, 2008. – 334 с.
6. ГОСТ Р 56905-2016. Проведение обмерных и инженерно-геодезических работ. – М.: Стандартинформ, 2016. – 44 с.
7. Руководство пользователя Agisoft Metashape. Версия 2.0. – 2023. – 210 с. URL: https://www.agisoft.com/pdf/metashape-pro_2_0_ru.pdf
8. Федоровский А.А., Быков Л.В. Влияние параметров конфигурации съемочной сети на точность наземной стереофотограмметрической съемки // Изв. вузов. Геодезия и аэрофотосъемка. – 2024. – Т. 68. – № 2. – С. 17–29.
9. Федоровский, А.А. Особенности применения методики наземной стереофотограмметрической съемки с прямой пространственной привязкой для трехмерного моделирования объектов местности / А.А. Федоровский // Изв. вузов. Геодезия и аэрофотосъемка. – 2022. – Т. 66. – N 5. – С. 73-86.

© А. А. Ануфриева, А. Ю. Чермошенцев, 2026

М. Е. Арапова^{1✉}, В. С. Ефремов¹

Автоматизация процесса поверки изделий с использованием искусственного интеллекта

¹ Сибирский государственный университет геосистем и технологий, г. Новосибирск,
Российская Федерация
e-mail: 89635115285@mail.ru

Аннотация. Статья посвящена проблеме автоматизации поверки средств измерений с использованием искусственного интеллекта, в дальнейшем ИИ. Основной темой же является анализ эффективности применения искусственного интеллекта для замены трудоемкого ручного труда в метрологических лабораториях. Проблема заключается в том, что традиционные методы поверки отнимают до 70 % рабочего времени на рутинные операции и подвержены ошибкам из-за человеческого фактора, а существующие автоматизированные системы недостаточно гибки. Цель исследования – обоснование применимости методов ИИ для автоматизации поверочного процесса. В качестве основных методов рассмотрены нейросети с автоассоциативной памятью, алгоритмы кластеризации и обнаружения дефектов. Результаты показывают, что внедрение ИИ позволяет сократить время поверки на 35-45 % и снизить число ошибок в 3-4 раза по сравнению с ручным методом. Применение ИИ существенно повышает эффективность поверки, однако требует изменения нормативной базы для юридического признания автоматических протоколов, а также решения проблем объяснимости решений и интеграции в существующие процессы.

Ключевые слова: автоматизация поверки, искусственный интеллект, метрология, машинное обучение, нейросети, обнаружение аномалий, контроль качества средств измерений

М. Е. Arapova^{1✉}, V. S. Efremov¹

Automation of the product verification process using artificial intelligence

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation,
Novosibirsk, Russian Federation
e-mail: 89635115285@mail.ru

Abstract. The article is devoted to the problem of automation of verification of measuring instruments using artificial intelligence, hereinafter AI. The main topic is the analysis of the effectiveness of the use of artificial intelligence to replace labor-intensive manual labor in metrological laboratories. The problem is that traditional verification methods take up to 70% of the working time for routine operations and are prone to errors due to the human factor, and existing automated systems are not flexible enough. The purpose of the study is to substantiate the applicability of AI methods for automating the verification process. Neural networks with auto-associative memory, clustering and defect detection algorithms are considered as the main methods. The results show that the introduction of AI makes it possible to reduce the verification time by 35-45% and reduce the number of errors by 3-4 times compared with the manual method. The use of AI significantly increases the efficiency of verification, but requires a change in the regulatory framework for the legal recognition of automatic protocols, as well as solving problems of explainability of solutions and integration into existing processes.

Keywords: automation of verification, artificial intelligence, metrology, machine learning, neural networks, anomaly detection, quality control of measuring instruments

Введение

Поверка средствами измерений различных изделий до сих пор остается во многом ручным трудом. Работник отдела технического контроля, в дальнейшем работник ОТК, подключает прибор или подготавливает инструменты поверки, переключает режимы, фиксирует показания, заполняет протоколы. Из источников [1, 5], большая часть рабочего времени, а это 60 %, уходит именно на расчетные операции. При этом неизбежны ошибки – как при измерениях (из-за усталости или невнимательности), так и при оформлении документов. Например, указан не верный номер детали, изделия, или в результате неразборчивого почерка, затруднено определение записанных данных. И вот тут-то, казалось бы, давно существующие автоматизированные системы и должны решать эту проблему. Однако на практике, процесс настройки аппаратного комплекса, разработки и программного обеспечения под каждый измерительный процесс, по началу будет довольно трудозатратен [9].

В отличие от обычных программ, ИИ способен определить отклонение или сменить способ проверки без вмешательства со стороны, оставляя за человеком лишь окончательную проверку проведенных измерений [2, 4]. В условиях цифровизации промышленности и ужесточения стандартов качества такие возможности становятся не просто полезным дополнением, а необходимым инструментом. Тем более что, по данным [20], почти 40 % метрологических работ на предприятиях до сих пор выполняются без серьезной автоматизации – потенциал для повышения эффективности здесь огромен.

Целью данной статьи является обоснование возможности и эффективности применения методов искусственного интеллекта для автоматизации процесса поверки изделий. Для достижения поставленной цели необходимо решить следующие задачи: проанализировать существующие подходы к автоматизации поверки на основе литературных источников; описать конкретные методы ИИ (нейросети, кластеризация, обнаружение аномалий), которые можно применить в метрологии; представить результаты сравнения ручной и ИИ-автоматизированной поверки; выявить недостатки внедрения интеллектуальных систем и предложить пути их решения.

Методы и материалы

В рамках теоретического анализа рассмотрены три класса задач автоматизированной поверки, решение которых можно осуществить с помощью методов искусственного интеллекта: выбор оптимальных режимов измерений, обнаружение дефектов и классификация состояния прибора или изделия (годен / не годен / доработать / перепроверить).

В обычных автоматизированных системах режимы поверки задается определенное количество измеряемых параметров и количество поверок, что приводит к избыточности или, наоборот, недостаточности измерений. Альтернативой

является использование нейросетей с автоассоциативной памятью, заранее обученную на большом количестве заведомо исправных приборов и деталей, параметры которых она запоминает, что позволяет ей адаптировать программу проверки под текущий экземпляр прибора или детали [13], тем самым сократит количество измерений неточных измерений.

Так же в процессе проверки могут возникать нештатные ситуации. Например, кратковременные сбои связи. Человек иногда не замечает такие события, особенно при наличии большого объема данных. Алгоритмы машинного обучения – в частности, метод изолирующего леса (Isolation Forest) и методы кластеризации – позволяют автоматически маркировать подозрительные измерения и либо повторить их, либо исключить из расчета [3, 4], что в результате повышает надежность итогового заключения.

Окончательной задачей является, определение нахождения погрешности прибора в допустимых значениях. Например, ИИ-методы могут учитывать не только текущее отклонение, но и динамику его изменения, а также совокупность косвенных признаков, что особенно полезно для многопараметрических приборов [8, 12].

Все перечисленные ранее методы не требуют создания новой физической инфраструктуры. Они могут быть реализованы путем внедрения поверх существующего поверочного оборудования, компьютерной программы, что соответствует экономичному подходу к автоматизации [15]. Интеграция таких решений в действующие лаборатории возможна по стандартным методикам внедрения информационных систем [18] с использованием шаблонов процессов [11]. Таким образом, методологическая основа для применения ИИ в проверке уже существует и может быть адаптирована к нуждам конкретной лаборатории без кардинального переоснащения. Алгоритм процессов контроля представлен на рисунке 1 и 2.

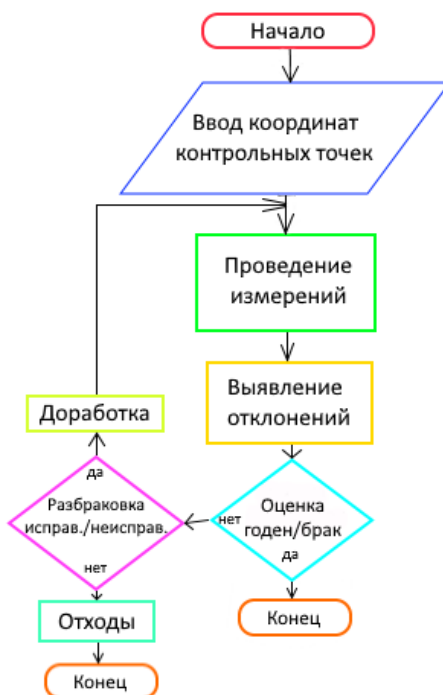


Рис. 1. Блок-схема процесс контроля без использования ИИ

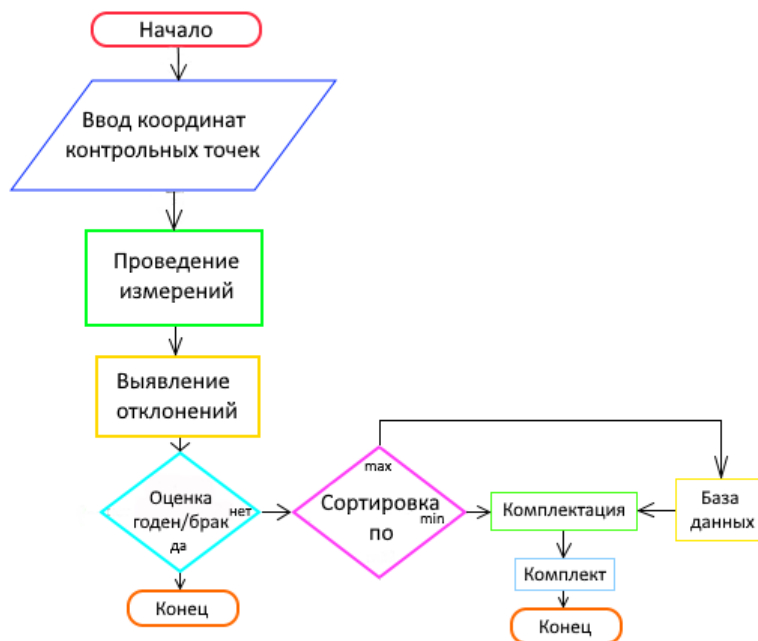


Рис. 2. Блок-схема процесс контроля с использованием ИИ

Результаты

На основе обобщения данных из литературных источников [1, 5-7, 20] можно сделать следующие выводы о потенциальной эффективности внедрения ИИ в процессы поверки.

Например, ожидаемое сокращение времени по оценкам, приведенным в [7] и [15], автоматизация рутинных операций (переключение диапазонов, запись показаний) дает выигрыш в 20-25 %. Добавление интеллектуальных алгоритмов, адаптирующих программу поверки под конкретный прибор, позволяет дополнительно сократить время еще на 15-20 % за счет исключения избыточных измерений. В результате, суммарное снижение времени поверки может достигать 35-45 % по сравнению с ручным методом.

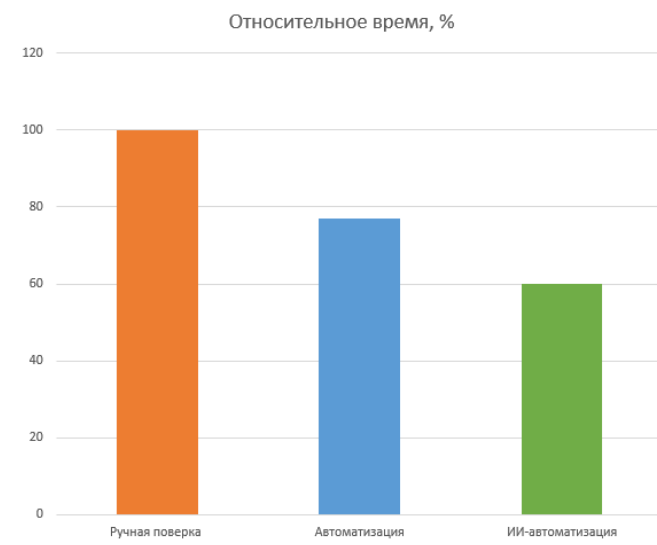


Рис. 3. Затраты времени

Человеческий фактор – основная причина ошибок при поверке: пропуск бракованного прибора, неверная запись в протокол, неправильный выбор диапазона. По данным [6] и [8], автоматизация снижает количество таких ошибок в 2-3 раза. Использование ИИ-алгоритмов обнаружения аномалий и автоматической классификации позволяет сократить ошибки еще сильнее – в 3-4 раза по сравнению с ручной проверкой, поскольку система не устает и одинаково строго оценивает каждое измерение.

В отличие от человека, ИИ-система дает идентичный результат при повторении поверки одного и того же прибора в одинаковых условиях. Это критически важно для спорных ситуаций и повторных проверок.

Общую теоретическую оценку эффективности представлена в таблице 1, представленной ниже.

Таблица 1 – Оценка эффективности различных подходов к поверке

Параметры	Ручная проверка	Автоматизация	Автоматизация с помощью ИИ
Относительное время	100 %	65-75 %	55-65 %
Относительное число ошибок	100 %	40-50 %	25-35 %
Воспроизводимость результатов	90-95 %	100 %	100 %
Адаптация к новому типу изделия	Переобучение персонала для поверки нового изделия (несколько минут или дней)	Перепрограммирование программы для проверки нового изделия (от нескольких часов или дней)	Переадаптация ИИ для нового изделия (несколько минут)

Обсуждение

Полученные теоретические оценки согласуются с выводами практических работ [6-8] и показывают, что ИИ действительно может стать следующим шагом после простой автоматизации. Однако для реализации этого потенциала необходимо преодолеть ряд ограничений.

Главный барьер – это юридический статус. Действующее законодательство в области обеспечения единства измерений (Федеральный закон № 102-ФЗ «Об обеспечении единства измерений» [21], ГОСТ Р 8.000-2015 [22], ГОСТ Р 8.894-2015 [23]) требует, чтобы поверку проводило аттестованное лицо. Протокол, сформированный ИИ-системой без участия человека, не имеет юридической силы [9, 12]. Необходимы изменения в нормативной базе или разработка отраслевых стандартов, признающих автоматическую поверку при условии полного логирования всех действий системы [2, 10]. На сегодняшний день утвержденных методик поверки с использованием искусственного интеллекта не существует, а имеющиеся ГОСТы предполагают только традиционные методы поверки [23].

Вторым барьером является – чувствительность к изменению эталонов. ИИ-алгоритмы обучаются на имеющихся уже проверенных данных. Если эталонное оборудование имеет незамеченный дрейф, нейросеть может «привыкнуть» к систематической ошибке и начать проводить измерение с этой же ошибкой. Решением может служить регулярная валидация ИИ-моделей на контрольных образцах и обязательное периодическое тестирование на пограничных значениях [5, 8].

Отдельного внимания заслуживает проблема объяснимости решений, принимаемых нейросетью. Специалист должен не просто получить вердикт «годен» или «не годен», но и понять, какие именно измерения привели к такому выводу. В противном случае невозможно ни проверить корректность поверки, ни аргументированно отстаивать ее результаты. Выход предлагают методы объяснимого ИИ – SHAP и LIME, которые для каждого решения показывают, какие измерения сильнее всего повлияли на вердикт [4].

Барьером является – интеграция в существующие процессы. Внедрение ИИ требует не только технических, но и организационных изменений: переобучения персонала, пересмотра должностных инструкций, создания новых регламентов [18, 19]. Наиболее реалистичный путь – поэтапное внедрение по гибридной схеме: ИИ выдает предварительное заключение, а метролог его утверждает, сначала на всех приборах, а затем – выборочно, только в пограничных случаях.

Заключение

Подводя итог по проведенному теоретическому анализу, можно утверждать, что искусственный интеллект действительно способен стать следующим логическим шагом в развитии автоматизации поверочных процессов. Проблема высокой трудоемкости и подверженности ошибкам, характерная для ручного труда [1, 5], а также недостаточная гибкость традиционных автоматизированных систем [9] могут быть в значительной степени преодолены за счет внедрения методов машинного обучения. Как указано в работе, нейросети с автоассоциативной памятью позволяют адаптировать программу поверки под конкретный экземпляр прибора или детали [13], а методы обнаружения дефектов и интеллектуальной классификации повышают достоверность результатов [3, 4, 8]. По оценкам, основанным на обобщении литературных данных, потенциальное сокращение времени поверки может составить 35-45 %, а снижение числа ошибок – в 3-4 раза по сравнению с ручными методами [6, 7, 15]. Это подтверждает актуальность цифровой трансформации метрологии и необходимость более широкого внедрения ИИ-решений на предприятиях [14, 20].

Вместе с тем, в проведенном анализе были выявлены серьезные ограничения, которые носят не столько технический, сколько организационный и юридический характер. Главным барьером остается неготовность нормативной базы: действующий Федеральный закон «Об обеспечении единства измерений» [21] и сопутствующие ГОСТы [22, 23] не признают автоматически сформированный ИИ-протокол поверки как юридически значимый документ [9, 12]. Кроме того, требуют решения проблемы объяснимости решений нейросетей [4], чувствительности к изменениям эталонов [5, 8] и интеграции интеллектуальных систем

в сложившиеся метрологические процессы [18, 19]. Тем не менее, эти препятствия не выглядят непреодолимыми. Наиболее реалистичным путем представляется поэтапное внедрение. Как пример, когда ИИ выступает в роли интеллектуального помощника, а окончательное решение остается за аттестованным метрологом [2, 10]. Параллельно необходимо развивать методы объяснимого ИИ и разрабатывать отраслевые стандарты для автоматизированной поверки [4, 8].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Автоматизация процессов поверки и калибровки средств измерений в современных лабораториях. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/avtomatizatsiya-protseessov-poverki-i-kalibrovki-sredstv-izmereniy-v-sovremennyh-laboratoriayah/viewer> (дата обращения 06.04.26). - Режим доступа: свободный.

2. Цифровизация и искусственный интеллект в метрологии. – Текст : электронный // Качество.ру : [сайт]. – URL: <https://kachestvo.pro/metrology/articles/luchshie-praktiki/tsifrovizatsiya-i-iskusstvennyu-intellekt-v-metrologii/> (дата обращения 06.04.26). - Режим доступа: свободный.

3. Контроль качества, искусственный интеллект, интеграция и автоматизация. – Текст : электронный // Polymer Branch : [сайт]. – URL: <https://polymerbranch.com/articles/kontrol-kachestva-iskusstvennyj-intellekt-integratsiya-i-avtomatizatsiya/> (дата обращения 06.04.26). - Режим доступа: свободный.

4. Как искусственный интеллект и машинное обучение переосмысливают контроль качества продукции. – Текст : электронный // Synaptik : [сайт]. – URL: <https://synaptik.ru/blog/kak-it-resheniya-uluchshayut-kachestvo-produkcii/kak-iskusstvennyj-intellekt-i-mashinnoe-obuchenie-pereosmyslivayut-podhod-k-kachestvu-produkcii> (дата обращения 10.04.26). - Режим доступа: свободный.

5. Автоматизация в сфере метрологии. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/avtomatizatsiya-v-sfere-metrologii/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

6. Повышение качества поверочных работ с помощью применения автоматизированных систем. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/povyshenie-kachestva-poverochnyh-rabot-s-pomoschyu-primeneniya-avtomatizirovannyh-sistem/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

7. Автоматизация операций поверки и калибровки электроизмерительных приборов. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/avtomatizatsiya-operatsiy-poverki-i-kalibrovki-elektroizmeritelnyh-priborov/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

8. Оценка качества автоматизированной поверки средств измерений. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/otsenka-kachestva-avtomatizirovannoy-poverki-sredstv-izmereniy/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

9. Недостатки применения автоматизированных систем поверки. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/nedostatki-primeneniya-avtomatizirovannyh-sistem-poverki/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

10. Автоматизация метрологического обеспечения на стадии производства продукции. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/avtomatizatsiya-metrologicheskogo-obespecheniya-na-stadii-proizvodstva-produkcii/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

11. Создание шаблона процесса (оказание услуг в области метрологии) с помощью программы PDM step suite (PSS) URL: <https://cyberleninka.ru/article/n/sozdanie-shablona-protseessa>

okazanie-uslug-v-oblasti-metrologii-s-pomoschyu-programmy-pdm-step-suite-pss/viewer (дата обращения 10.04.26). - Режим доступа: свободный.

12. Автоматизация процедуры поверки средств измерений. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/avtomatizatsiya-protsedury-poverki-sredstv-izmereniy/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

13. Актуальность разработки автоматизированной системы учета средств измерений на предприятии. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/avtomaticheskii-vybor-rezhimov-raboty-iis-s-ispolzovaniem-avtoassotsiativnoy-pamyati/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

14. Актуальность разработки автоматизированной системы учета средств измерений на предприятии URL: <https://cyberleninka.ru/article/n/aktualnost-razrabotki-avtomatizirovannoy-sistemy-ucheta-sredstv-izmereniy-na-predpriyatii/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

15. Экономичный подход к автоматизации поверки средств измерений. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/ekonomichnyy-podhod-k-avtomatizatsii-poverki-sredstv-izmereniy/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

16. Особенности создания автоматизированных систем управления в современных условиях. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/osobennosti-sozdaniya-avtomatizirovannyh-sistem-upravleniya-v-sovremennyh-usloviyah/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

17. Разработка автоматизированной системы для определения погрешности измерительных каналов. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/razrabotka-avtomatizirovannoy-sistemy-dlya-opredleniya-pogreshnosti-izmeritelnyh-kanalov/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

18. Методика внедрения информационных систем на промышленных предприятиях. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/metodika-vnedreniya-informatsionnyh-sistem-na-promyshlennyh-predpriyatiyah/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

19. Система оборота технологической оснастки на предприятии. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/sistema-oborota-tehnologicheskoy-osnastki-na-predpriyatii/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

20. Направления повышения эффективности метрологических работ. – Текст : электронный // CyberLeninka : научная электронная библиотека : [сайт]. – URL: <https://cyberleninka.ru/article/n/napravleniya-povysheniya-effektivnosti-metrologicheskikh-rabot/viewer> (дата обращения 10.04.26). - Режим доступа: свободный.

21. Федеральный закон от 26.06.2008 № 102-ФЗ (ред. от 02.07.2021) «Об обеспечении единства измерений». – Текст : электронный // КонсультантПлюс : [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_77904/ (дата обращения 21.04.26). – Режим доступа: свободный.

22. ГОСТ Р 8.000-2015. Государственная система обеспечения единства измерений. Основные положения. – Введ. 2016-01-01. – Москва : Стандартинформ, 2015. – 15 с.

23. ГОСТ Р 8.894-2015. Государственная система обеспечения единства измерений. Поверка средств измерений. Организация и порядок проведения. – Введ. 2016-03-01. – Москва : Стандартинформ, 2015. – 20 с.

© М. Е. Арапова, В. С. Ефремов, 2026

Д. А. Бантос^{1✉}, И. О. Михайлов¹

Особенности использования и изготовления оптоволоконных катушек для беспилотных авиационных систем

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: bantos.d.17@gmail.com

Аннотация. В статье рассмотрены особенности применения оптоволоконных катушек (ОВК) в беспилотных авиационных системах в качестве элемента волоконно-оптической линии связи. Представлена классификация ОВК по двум основаниям: по способу размотки и по форме намотки. Проведен сравнительный анализ каждого типа катушек, по результатам которого сделан вывод о предпочтительности бескаркасных катушек с ракетной или конической формой намотки. Рассмотрены основные дефекты, возникающие при намотке ОВК: постоянные и переменные. Описаны технологические аспекты производства ОВК: применение сервопривода для синхронизации механизмов намотки и раскладки, использование машинного зрения для контроля качества намотки, а также способы нанесения клеящего вещества при изготовлении бескаркасных катушек. Предложена схема намоточного станка с блоком нанесения клеящего вещества, обеспечивающего контроль процесса намотки. Результаты работы могут быть использованы при проектировании систем связи беспилотных авиационных систем на основе волоконно-оптических линий.

Ключевые слова: оптоволоконная катушка, беспилотные авиационные системы, намотка оптического волокна

D. A. Bantos^{1✉}, I. O. Mikhailov¹

Features of Using and Manufacturing of Fiber Optic Coils for Unmanned Aerial Vehicles

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: bantos.d.17@gmail.com

Abstract. This article examines the application of fiber optic coils (FOC) in unmanned aerial vehicles as a fiber optic communication link element. FOC is classified based on two criteria: unwinding method and winding shape. A comparative analysis of each reel type is conducted, leading to the conclusion that frameless reels with a rocket-shaped or conical winding shape are preferable. The main defects that arise during FOC winding are considered: constant and variable. The article describes technological aspects of FOC production, including the use of a servo drive to synchronize the winding and unwinding mechanisms, the use of machine vision for winding quality control, and adhesive application methods in the manufacture of frameless reels. A diagram of a winding machine with an adhesive application unit, which ensures winding process control, is proposed. The results of this work can be used in the design of unmanned aerial vehicles communication systems based on fiber optic lines.

Keywords: optical fiber coil, unmanned aerial systems, optical fiber winding

Введение

Беспилотные авиационные системы (БАС) находят все более широкое применение в военной, гражданской и научной сферах. Одной из ключевых задач при их эксплуатации является обеспечение надежного канала передачи данных между БАС и оператором. Традиционные радиоканалы имеют ряд существенных ограничений: подверженность радиопомехам и средствам радиоэлектронной борьбы, ограниченная пропускная способность, возможность перехвата сигнала. В качестве альтернативы все активнее рассматривается применение волоконно-оптических линий связи [1].

Оптоволокно обеспечивает защищенный высокоскоростной канал передачи данных, невосприимчивый к электромагнитным помехам. Однако его применение на БАС требует решения ряда инженерных задач: волокно должно разматываться с катушки в процессе полета без чрезмерного натяжения, без образования перегибов и петель, при этом масса катушки должна быть минимальной, чтобы не снижать летные характеристики. Таким образом, оптоволоконная катушка (ОВК) является ключевым элементом системы связи БАС на основе волоконно-оптических линий связи, а ее конструкция и качество намотки во многом определяют надежность всей системы.

В данной работе рассмотрены существующие типы ОВК, проанализированы дефекты, возникающие в процессе их изготовления, а также предложена схема намоточного станка для производства бескаркасных ОВК.

Существующие типы оптоволоконных катушек

ОВК для БАС можно классифицировать по двум основаниям: по способу размотки и по форме намотки.

По способу размотки выделяют внешнюю и внутреннюю размотку.

Катушки с внешней размоткой наматываются на шпулю, и размотка происходит от внешнего диаметра к внутреннему. Основным преимуществом данного вида катушек является простота процесса намотки. Однако недостатки более существенны, а именно:

наличие шпули увеличивает массу ОВК, что уменьшает дальность полета БАС и массу поднимаемого груза;

в процессе разматывания волокно перегибается через фланцы шпули, что сильно уменьшает радиус изгиба вследствие чего повышаются риски обрыва волокна, ухудшается качество передаваемого сигнала [2, 3].

Альтернативой катушек с внешней размоткой служат катушки с внутренней размоткой (бескаркасные катушки). Процесс намотки данного типа катушек происходит на разборную шпулю, которая удаляется по завершению процесса намотки. Для того чтобы волокно не слетало используется клеящее вещество, наносимое в процессе намотки. Размотка же происходит от внутреннего радиуса к внешнему. Преимуществами данного типа катушек являются:

меньшая масса ОВК, что позволяет увеличить дальность полета, путем наматывания большей длины оптоволоконной линии при сохранении массы;

отсутствие перегибов через фланец минимизирует риски обрыва оптоволокна и исключает место сильного перегиба;

при размотке в первую очередь выпускаются внутренние ряды с большим внутренним напряжением.

Недостатком данного типа намотки является сложность производства. Поскольку ввиду отсутствия шпули необходимо использовать клеящее вещество для сохранения формы ОВК.

Выделяют 3 формы намотки катушек: цилиндрическая, коническая, ракетная (рис 1).

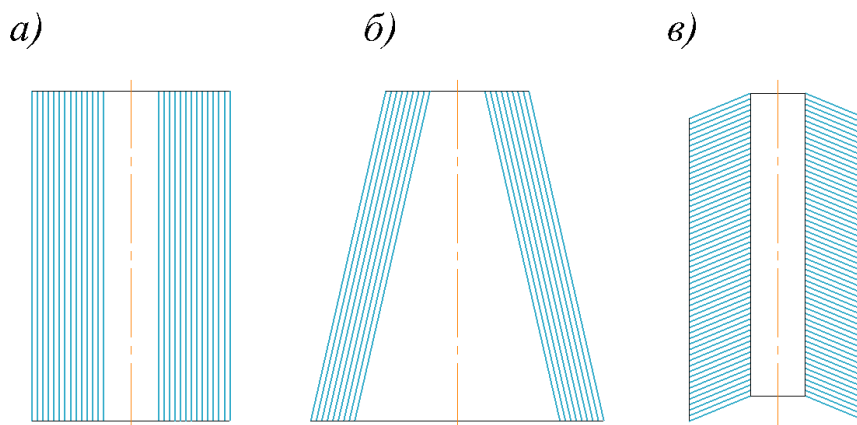


Рис. 1. Формы намотки: цилиндрическая (а); коническая (б); ракетная (в)

Цилиндрическая намотка является самой простой и производится на шпулю с фланцами на всю высоту намотки [4]. Скорость разматывания данной катушки не высока, так как в процессе схода волокно трется о нижележащие слои.

Коническая намотка распространена в текстильной промышленности. Данная форма намотки позволяет предотвратить слет витков, так как сходя от большего торца к меньшему волокно не задевает витки, находящиеся ближе к меньшему торцу [5].

Ракетная намотка также изначально разработана для текстильной промышленности. Намотка данной формы отличается от остальных тем, что слои наращиваются не горизонтально, а вертикально и под углом. Размотка происходит от меньшего диаметра к большему, а волокно отрывается от тела катушки по нормали к ее поверхности [6]. Однако данный способ намотки является самым сложным в реализации из-за жесткости самого волокна приводящего к сползанию волокна и как следствие полной потере работоспособности ОВК.

В эксперименте проведенным Паниным А. И. [7], направленным на замер натяжения нити при смотке с бобин различных форм (рис. 2).

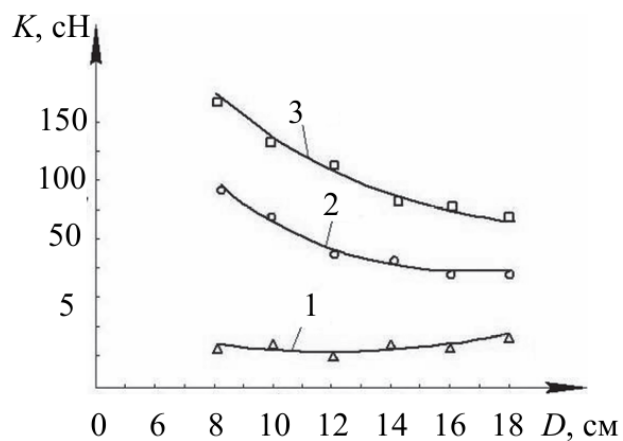


Рис. 2. Зависимость натяжения нити (K , сН) от диаметра (D , см) при различных формах намотки: при работе с бобиной ракетной формы (1); при работе с конической намоткой (2); при работе с цилиндрической намоткой (3)

На основании полученных данных можно сделать вывод, что оптимальной ОВК является бескаркасная катушка с ракетной или конической формой намотки, представляющая компромисс между относительной простотой намотки и натяжением нити.

Проблемы и дефекты при намотке

Выбор оптимальной конструкции катушки не гарантирует качество готового изделия. Ключевым фактором, определяющим работоспособность ОВК, является точность процесса намотки, поскольку возникающие при формировании катушки погрешности намотки приводят к увеличению сил отрыва волокна и потере сигнала [2, 3].

Основными сложностями при намотке ОВК всех типов являются постоянные и переменные дефекты. Постоянные дефекты появляются из-за чередования направления намотки, различного угла между наматываемым оптоволоконном и фланцем катушки. Можно выделить три основных вида постоянных дефектов: перескок, пристеночный (прифланцевый) и дефект «выходящего волокна». Перескок характеризуется регулярным смещением витка относительно нижнего слоя из-за разного направления намотки. Прифланцевый и дефект «выходящего волокна» образуются в крайних точках катушки. Прифланцевый характеризуется провалом витка к фланцу возникающий из-за разных углов укладки волокна и фланца. Дефект «выходящего волокна» возникает, когда виток переходит на новый слой, тем самым оказывая большее давление на нижележащий виток [8].

Переменные дефекты образуются вследствие неточности в работе намоточного станка. К ним относятся смещение витка через n -й ряд в пределах одного слоя (рис. 3, а) и наложение волокна поверх n -го предшествующего витка (рис. 3, б) [9]. Смещение витка через n -й ряд в пределах одного слоя возникает при неточности в работе механизма раскладки, выраженная в неправильном смещении при заданном натяжении и скорости намотки. Данный дефект приводит к

микроизгибам при наматывании следующего слоя (локальных повышениях сдвигания волокна и как следствие изменению его геометрических параметров). Дефект наложение волокна поверх n -го предшествующего витка вызван неточностью в работе датчиков натяжения волокна в процессе намотки ввиду чего волокно из-за своей жесткости не переходит на следующий ряд, а наслаивается на прошлые, что также приводит к микроизгибам и одновременному сходу нескольких витков в процессе разматывания катушки.

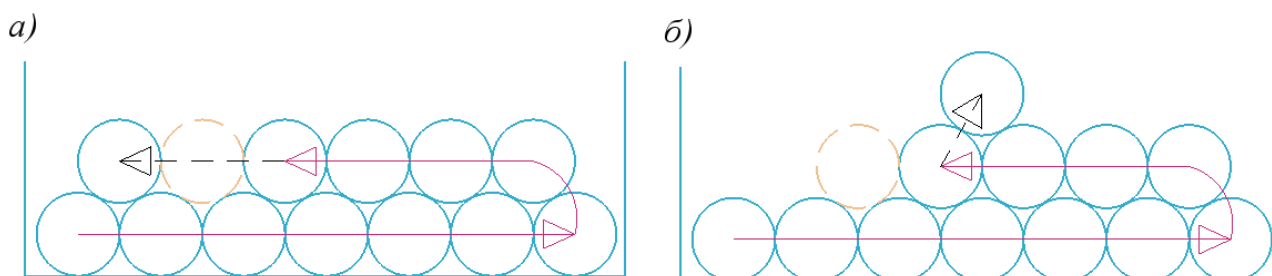


Рис. 3. Переменные дефекты

Технология производства оптоволоконных катушек

Для минимизации описанных выше дефектов и обеспечения стабильного качества ОВК намотка производится на специализированных станках с высокоточными системами управления. Конструкция станков должна обеспечивать три ключевых условия: точную синхронизацию механизмов намотки и раскладки, непрерывный контроль качества укладки волокна, а также нанесение клеящего вещества при изготовлении бескаркасных ОВК. Рассмотрим каждое из этих условий подробнее.

В соответствии с рис. 4 сигнал с датчиков натяжения поступает в блок управления механизма намотки, управляющий скоростью вращения катушки. Сигнал с блока управления намотки поступает в блок управления механизмом раскладки, управляющий смещением направляющей каретки. Эта связь необходима для синхронизации процессов намотки и раскладки, для минимизации переменных дефектов. Чтобы обеспечить большую точность и компенсировать люфт в приводе при синхронизации механизмов раскладки и намотки предлагается использовать сервопривод [10]. Механизм контроля укладки может производиться контактными (инструментальными) и бесконтактными методами. Применение контактных методов для оптоволоконна недопустимо ввиду возможности механических повреждений. Применение бесконтактных методов возможно с использованием машинного зрения, основанного на глубоком обучении. Скорость проверки данным методом выше фактической скорости намотки и позволяет определять дефекты с точностью выше 94,67 % [11]. Однако данный метод сталкивается с проблемой невозможности исправить обнаруженные дефекты.

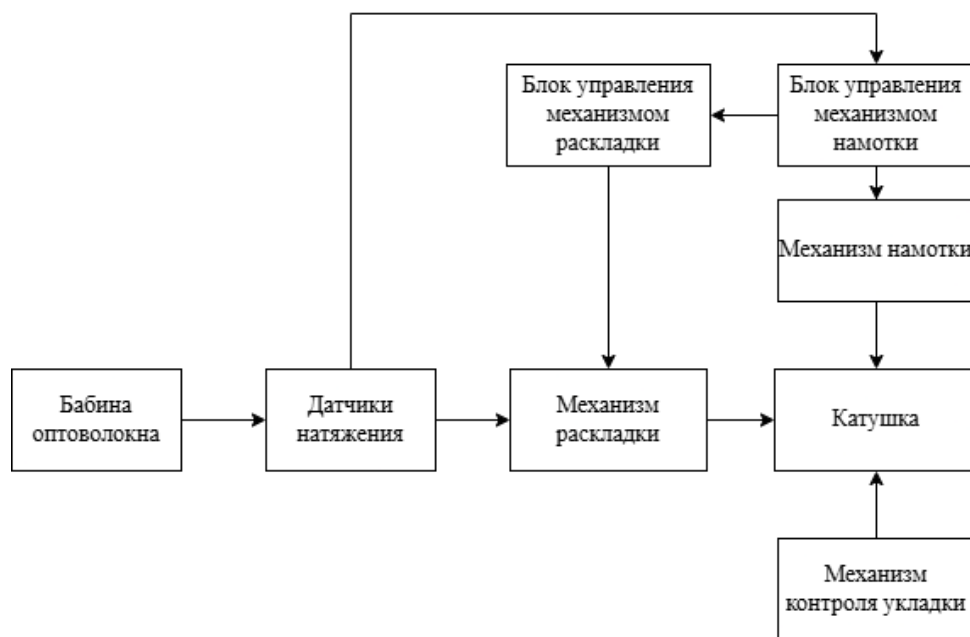


Рис. 4. Блок схема станка

При создании бескаркасных катушек необходимо использование клеящего вещества, нанесение которого может происходить двумя способами: в процессе намотки и после намотки. Нанесение клеящего вещества в процессе намотки производится под давлением путем пропускания оптоволокна через специальное устройство. Нанесение клея вторым способом происходит с использованием вакуумной пропитки. ОВК помещается в камеру, где под воздействием вакуума клеящее вещество полностью проникает в ОВК не оставляя пустот.

Заключение

В работе проведен сравнительный анализ типов ОВК и выявлены основные дефекты намотки. Предложена схема намоточного станка для производства бескаркасных катушек с контролем качества укладки волокна. Блок нанесения клеящего вещества на схеме не указан в связи с возможностью использования вакуумной камеры.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Полковников В. П. Оптоволоконные технологии в противовес средствам радиоэлектронной борьбы противника. – СПб. : ФЛАГМАН НАУКИ, 2024. Т.3. С. 405-411.
2. Шрамко О.А., Рупасов А.В., Новиков Р.Л., Аксарин С.М. Метод исследования зависимости h -параметра анизотропного световода от радиуса изгиба. – М. : Научно технический вестник информационных технологий, механики и оптики. 2014. С. 26–31.
3. Аксарин С.М., Архипов С.В., Варжель С.В., Куликов А.В., Стригалева В.Е. Исследование зависимости параметров анизотропных одномодовых волоконных световодов от диаметра намотки. – М. : Научно-технический вестник информационных технологий, механики и оптики. 2013. Т.4. С. 22–26.

4. Лопарев В. А., Киселев С. С., Шилин М. М. Выбор способа намотки для технической реализации волоконно оптической линии связи с высокоскоростным объектом. – М : Научно-технический вестник информационных технологий, механики и оптики. 2017. Т2. С. 612—619.
5. Лопарев В. А., Киселев С. С., Шилин М. М. Особенности станочного оборудования для намотки оптического волокна. – М : Известия вузов приборостроение. 2019. С. 78-85.
6. Патент RU191207U1 Россия, G02B 6/44. Катушка для волоконно-оптического кабеля линии связи с высокоскоростным объектом; № 2018140819; заявл. 19.11.2018; опубл. 29.07.2019/ Мешковский И.К., Киселев С.С. – 6 с.
7. Панин А. И. Построение модели зависимости удельной плотности намотки от угла сдвига витков и толщины наматываемого слоя пряжи : статья – Димитровград. : Вестник ДИТУД, 2001. Т.1. С. 12-17
8. Мешковский И. К, Унтилов А. А., Киселев С. С., Куликов А. В., Новиков Р. Л. Качество намотки чувствительного элемента волоконно-оптического гироскопа. – М : Известия вузов приборостроение. 2011. С. 76-80.
9. Мешковский И. К, Киселев С. С., Куликов А. В., Новиков Р. Л. Дефекты намотки оптического волокна при изготовлении чувствительного элемента волоконно-оптического интерферометра. – М : Приборостроение. 2010. С. 47-51.
10. Авдеюк Ю. А., Рыжкова Е. А., Тимохин А. Н. Применение сервопривода в процессе намотки-раскладки оптических волокон. – М : Сборник научных трудов кафедры автоматики и промышленной электроники. 2015. Т.4. С. 72-74.
11. Liu Yu, Wei Xi-lai, Wang Shuai, Dai Li. Machine vision automatic inspection technology of optical fiber winding based on deep learning. – Shenyang : Journal of Northeastern University. 2020. С 68-74.

© Д. А. Бантос, И. О. Михайлов, 2026

К. В. Бондаренко¹✉

Анализ патентных решений и зарубежных разработок в области гиперспектральных систем для дистанционного зондирования

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: banderars001@gmail.com

Аннотация. В статье представлен углубленный технический анализ пяти патентных документов (четырёх российских и одного международного) и двух зарубежных публикаций, посвящённых гиперспектральным приборам, их применение, возможные технические решения. Для каждого патента рассмотрены: решаемая проблема, конструктивные особенности, оптическая схема, режимы работы, приведенные формулы, а также указаны ограничения и возможные пути их преодоления. На основе выполненного анализа предложена концепция гибридной гиперспектральной камеры, объединяющей цифровое накопление (TDI), вогнутую решетку с переменным шагом и элементы сжатого зондирования для дистанционного зондирования и разведки, для исследования и обнаружения различных спектральных диапазонов. Отдельное внимание уделено адаптации рассмотренных технических решений к климатическим условиям Российской Федерации.

Ключевые слова: гиперспектральная камера, патент RU 2624622, патент RU 2653772, патент RU 230837, патент RU 2635841, сжатое зондирование, интерферометр Фабри–Перо, VLS-решетка, цифровой TDI, линейный переменный фильтр

К. В. Bondarenko¹✉

Analysis of Patent Solutions and Foreign Developments in the Field of Hyperspectral Systems for Remote Sensing

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: banderars001@gmail.com

Abstract. The article presents an in-depth technical analysis of five patent documents (four Russian and one international) and two foreign publications devoted to hyperspectral instruments, their applications, and possible technical solutions. For each patent, the problem to be solved, design features, optical scheme, operating modes, provided formulas, as well as limitations and possible ways to overcome them are considered. Schematic technology applications and device designs are also provided. Based on the performed analysis, a concept of a hybrid hyperspectral camera is proposed, combining digital time delay integration (TDI), a concave variable line-space (VLS) grating, and compressed sensing elements for remote sensing and reconnaissance, for the study and detection of various spectral ranges. Special attention is paid to the adaptation of the considered technical solutions to the climatic conditions of the Russian Federation.

Keywords: hyperspectral camera, patent RU 2624622, patent RU 2653772, patent RU 230837, patent RU 2635841, compressed sensing, Fabry–Perot interferometer, VLS grating, digital TDI, linear variable filter

Введение

Развитие гиперспектральной аппаратуры для дистанционного зондирования Земли в настоящее время характеризуется интенсивным поиском новых конструктивных подходов, позволяющих одновременно улучшить пространственное и спектральное разрешение, повысить отношение сигнал/шум и снизить массогабаритные характеристики приборов. Наиболее радикальные инженерные идеи часто находят отражение в патентной литературе, тогда как апробация серийных технологий описывается в профильных научных журналах, таких как *Sensors* и *Optics Express*. Комплексное сопоставление сведений из этих источников дает возможность выявить перспективные направления для дальнейших разработок.

В рамках данной работы выполнен детальный разбор пяти патентных решений и двух экспериментальных систем. Для каждого объекта анализа приведено описание устройства, принципа действия, заявленных преимуществ и скрытых недостатков. В заключительной части сформулирована концепция гибридной гиперспектральной камеры, ориентированной на эксплуатацию в широком диапазоне температур (от -40 до $+50$ °C), характерном для регионов Сибири и Арктики.

Патент RU 2624622: многощелевая камера с ВЗН и жидкокристаллической щелевой структурой

В традиционных гиперспектральных камерах типа pushbroom с одной входной щелью время накопления сигнала ограничено скоростью движения носителя. С увеличением требуемого пространственного разрешения экспозиция сокращается, что приводит к падению отношения сигнал/шум. Авторы патента [1] предлагают компенсировать этот эффект за счет двух решений: использования многощелевой структуры и перевода фотоприемника в режим временной задержки и накопления (ВЗН).

Оптическая схема (рис. 1а, 1б) включает входной объектив (поз. 1), строящий изображение местности на щелевой структуре. Щелевая структура выполнена не механически, а в виде жидкокристаллического (ЖК) дисплея либо матрицы микрозеркал (DMD). Управляющий контроллер формирует на дисплее несколько параллельных щелей, ширина и межщелевое расстояние которых задаются программно.

Далее свет последовательно проходит коллимационный объектив (поз. 3), диспергирующий элемент – призму прямого зрения Амичи (поз. 4) и выходной объектив (поз. 5). Фотоприемное устройство (поз. 6) представляет собой строчно-кадровую ПЗС-матрицу, функционирующую в режиме ВЗН: зарядовые пакеты переносятся синхронно со смещением изображения, обеспечивая накопление сигнала на нескольких строках одновременно.

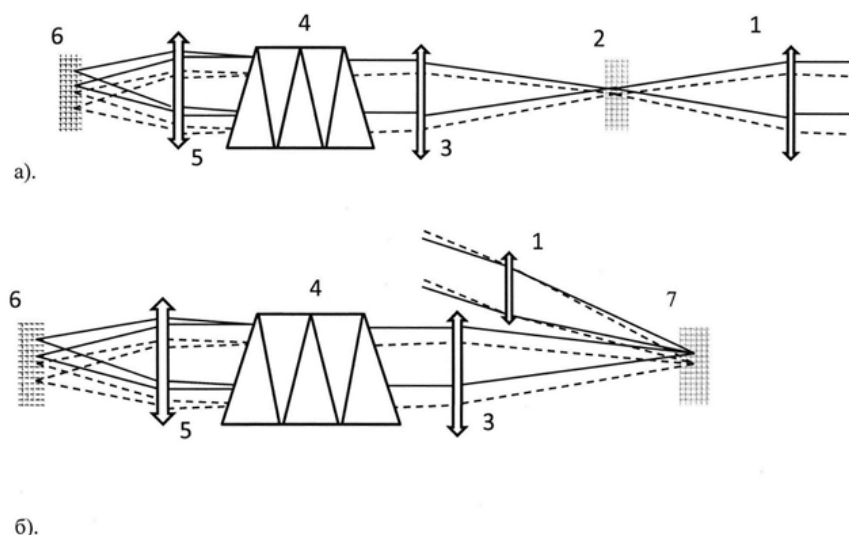


Рис. 1. Оптическая схема

Контроллер синхронизирует два процесса. Во-первых, тактовые сигналы ПЗС-матрицы согласуются со скоростью движения изображения: время переноса заряда на одну строку равно времени пролета изображения на один пиксель. Во-вторых, положение каждой щели на ЖК-дисплее динамически изменяется, следуя за движением изображения.

В патенте [1] описан трехуровневый алгоритм управления: внешний цикл по номеру сканирования, средний – по номеру линейного участка в пределах области одной щели, внутренний – по шагу сопровождения участка. Частота синхроимпульсов рассчитывается исходя из высоты и скорости носителя, а также требуемого пространственного разрешения вдоль направления полета.

Показано повышение чувствительности без потери пространственного разрешения. Эффективное время накопления возрастает пропорционально числу щелей. Например, при четырех щелях более удачное решение в отношении сигнал/шум (при доминировании фотонного шума) составляет около двух. Отказ от механического поворотного зеркала, использованного в прототипе [5], исключает вибрации и искажения изображения.

Несмотря на очевидные достоинства, предложенное решение сопряжено с энергетическими потерями. ЖК-дисплей даже в прозрачном состоянии характеризуется коэффициентом пропускания не более 30–40 % для поляризованного света. Если дисплей установлен перед объективом, указанные потери могут устранить преимущества от многощелевого режима. Вероятно, авторы подразумевали работу ЖК-ячейки на отражение (по аналогии с LCoS), однако в тексте патента этот момент детально не раскрыт. Применение DMD также не обеспечивает 100 % дифракционной эффективности. Тем не менее для задач, где приоритетом является равномерность покрытия, а не предельная светосила, подобная архитектура сохраняет практическую значимость.

Патент RU 2653772: сжатое зондирование с нерегулярной дифракционной решеткой

Патент [2], переданный в Российскую Федерацию по процедуре РСТ, базируется на теории сжатого зондирования (compressed sensing). В отличие от классической гиперспектральной съемки, порождающей трехмерный массив данных (x, y, λ) , здесь предполагается восстановление информации из существенно меньшего числа измерений благодаря разреженности сигнала в некотором базисе.

Система содержит принимающую оптику (телескоп, фотоаппарат или микроскоп в зависимости от решаемой задачи), светоделительный блок (дихроичные зеркала либо полосовые фильтры) и несколько параллельных каналов. В каждом канале последовательно размещены система переноса выходного зрачка, нерегулярная дифракционная решетка и фотоприемная система (линза увеличения с ПЗС-матрицей).

Ключевым элементом служит нерегулярная дифракционная решетка – структура с псевдослучайным фазовым профилем. Она одновременно выполняет две функции: рассеивает падающее излучение в спектр-картину (фазовая модуляция) и диспергирует свет по длинам волн. В результате каждый узкополосный точечный источник формирует на фотоприемнике уникальное спектр-поле, слабо коррелированное с полями от других источников.

Восстановление сигнала сводится к решению задачи нелинейной оптимизации. Матрица Φ определяется экспериментально в ходе калибровки: для каждого положения (x, y) и каждой длины волны λ регистрируется соответствующая спектр-картина.

Объем регистрируемых данных сокращается в 5–10 раз по сравнению с полным сканированием. Благодаря использованию фазовой модуляции (в отличие от амплитудной, характерной для однопиксельных камер с DMD) потери энергии сведены к минимуму. Система может работать в широком спектральном диапазоне – от ультрафиолетового до дальнего инфракрасного – путем выбора материала решетки (кварц, германий и т.д.).

Обработка сигнала требует решения сложной задачи, что на борту носителя (спутника или БПЛА) сопряжено с высокими вычислительными затратами. Предполагается, что основная обработка будет выполняться на наземных станциях. Однако передача сжатых данных по узкополосным каналам связи остается проблемой, особенно актуальной для удаленных территорий. Дополнительную сложность представляет технология изготовления нерегулярных решеток с высокой воспроизводимостью: в патенте не приведено конкретных сведений о производственном процессе.

Патент RU 230837 U1: телевизионное гиперспектральное устройство с компенсацией мод интерферометра Фабри–Перо

Интерферометр Фабри–Перо (ФПИ) состоит из двух полупрозрачных зеркал с регулируемым зазором. Изменение зазора смещает максимум пропускания, однако наряду с основной модой возникают побочные порядки интерференции.

При широкополосном освещении детектор регистрирует сумму сигналов от основной и дополнительных мод, что искажает спектр.

Структурная схема (рис. 2) включает объектив (1), ФПИ (2), монохромную телевизионную камеру на ПЗС-матрице (3), микроконтроллер (4) с цифро-аналоговым преобразователем для управления ФПИ и блок памяти (5). Новым элементом по сравнению с прототипом (патент US 10323985) является блок вычитания (6).

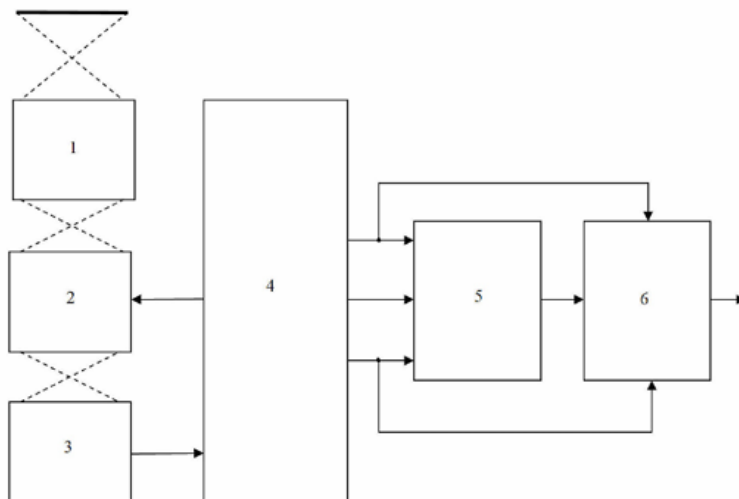


Рис. 2. Структурная схема

Блок памяти реализован в виде цепочки ОЗУ, в которой каждый кадр последовательно сдвигается. Число ячеек памяти соответствует числу узких спектральных зон регистрации.

Сначала микроконтроллер формирует n приращений напряжения, изменяя воздушный зазор. На этом этапе регистрируются изображения только от первой моды (паразитные порядки отсутствуют из-за малой величины зазора). Полученные кадры сохраняются в памяти.

Затем микроконтроллер переключает коммутатор и генерирует n приращений. При увеличенном зазоре возникает вторая мода, и детектор фиксирует суммарный сигнал (первая + вторая моды). Одновременно активируется блок вычитания: на его первый вход поступает текущий суммарный кадр, на второй – ранее сохраненный кадр первой моды. Результатом вычитания становится изображение, соответствующее исключительно второй моде. Процедура повторяется для всех шагов сканирования, обеспечивая разделение мод.

Авторы провели численное моделирование в среде MATLAB для диапазона 0,4–0,7 мкм с шагом по зазору 0,01 мкм, используя формулу Эйри. На рис. 3 исходного патента показаны спектральные характеристики, а также разностный сигнал. Видно, что после вычитания остается только узкий пик второй моды.

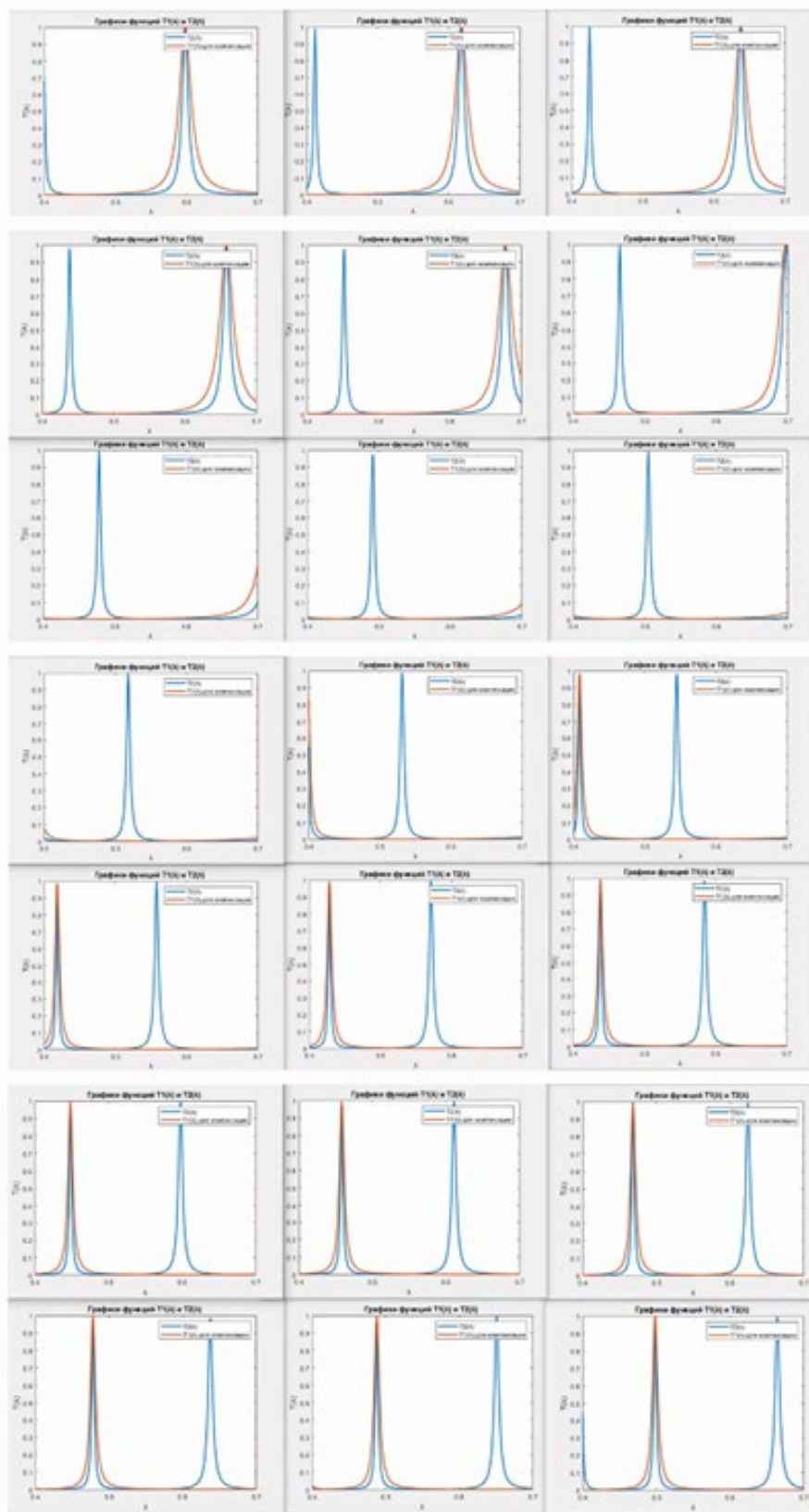


Рис. 3. Исследования в программе

К достоинствам следует отнести простоту элементной базы (стандартные микроконтроллеры, серийные ПЗС-камеры) и отсутствие сложной оптики. Недо-

статком является двукратное увеличение времени сканирования: сначала кадров для первой моды, затем n кадров для вычитания. При количестве спектральных каналов порядка ста общее число экспозиций достигает двухсот, что делает метод малоприменимым для съемки динамичных сцен с подвижных платформ.

Патент RU 2635841: гиперспектральный 2D-спектрофотометр на основе анастигмата

В данном устройстве [4] отсутствуют как щель, так и традиционная дифракционная решетка. Спектроделитель выполнен в виде двухзеркального матричного анастигмата – двух ортогонально скрещенных четверть-цилиндрических отражателей (рис. 4). Авторы (Мельников Г.С. и Самков В.М, ГОИ им. Вавилова) развивают подходы фрактальной оптики.

Параллельный световой поток от объекта падает на первый четверть-цилиндрический отражатель (поз. 8), который фокусирует излучение в линию. Второй отражатель (поз. 9), ортогональный первому, осуществляет фокусировку в перпендикулярном направлении. В результате на выходе формируется двумерный массив изображений, где одна координата соответствует пространственной информации, а другая – спектральной (за счет дисперсии, обусловленной цилиндрической геометрией).

Отражатели могут быть зеркальными либо диэлектрическими (кварц для УФ-видимого диапазона, германий для ИК). По утверждению авторов, при использовании фрактальных элементов с коэффициентом фрактальности достижимо относительное спектральное разрешение $\Delta\lambda/\lambda$ порядка 10^{-3} – 10^{-4} , что в видимой области соответствует 0,1–1 нм.

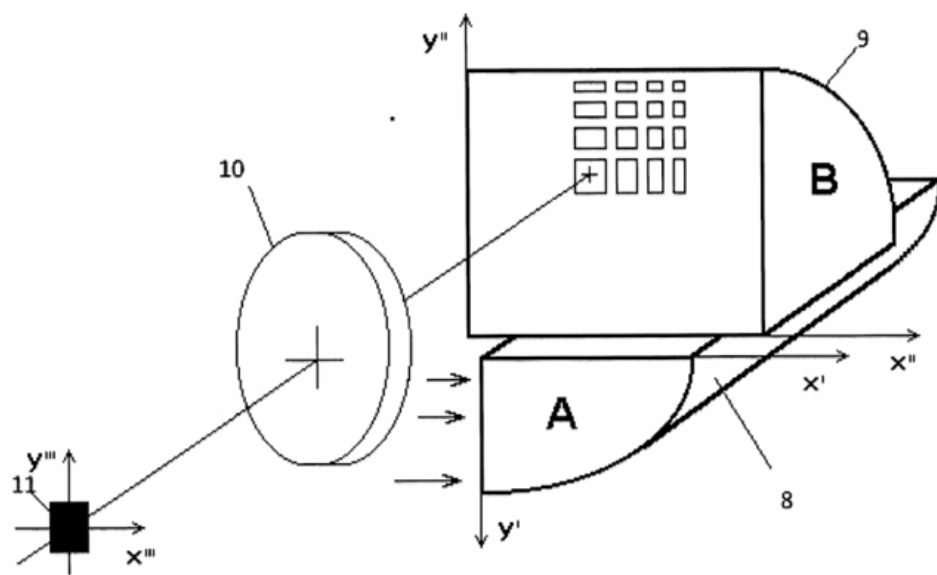


Рис. 4. Спектроделитель

Отсутствие движущихся частей и щелевого сканирования позволяет регистрировать гиперспектральный куб за одну экспозицию (режим snapshot). Зер-

кальная схема свободна от хроматических aberrаций, что особенно важно при работе в широком спектральном диапазоне.

Изготовление двух ортогональных цилиндрических отражателей с требуемой точностью представляет собой нетривиальную технологическую задачу. Конкретные методы изготовления в патенте не раскрыты. Кроме того, отсутствуют данные о величине поля зрения и требованиях к фотоприемнику, который должен обладать большим числом пикселей для регистрации матрицы спектральных каналов.

Зарубежные разработки: цифровой TDI и VLS-решетки

В работе [6] исследователи из Чанчуньского института оптики и точной механики применили линейный переменный фильтр (LVF), наклеенный непосредственно на КМОП-матрицу. Фильтр обеспечивает плавное изменение центральной длины волны вдоль строк матрицы. При движении спутника один и тот же участок местности последовательно экспонируется под разными строками, после чего сигналы с нескольких строк, соответствующих одному пикселю местности, суммируются (цифровой TDI). Использование детектора GSENSE5130 с частотой кадров до 1550 fps (при выборе 256 активных строк) позволило реализовать TDI уровня 8. Выигрыш в SNR составил около 2,8 раза, при этом влияние на спектральное разрешение не превысило 0,4 нм.

Авторы [7] изготовили вогнутую решетку с переменным расстоянием между штрихами (VLS).

Такая решетка корректирует астигматизм и обеспечивает фокусировку спектра на плоскую линию, что позволяет использовать стандартный линейный фотоприемник (Sony ILX511, 2048 пикселей).

Изготовление решетки осуществлялось методом вакуумного наноимпринтинга через эластичный штамп из ПДМС. Плоский мастер с 600 штр/мм размножался в ПДМС, затем штамп неравномерно растягивался и прижимался к вогнутой подложке с УФ-отверждаемым полимером. После металлизации алюминием получена решетка с измеренной эффективностью 43 % (выше, чем у типичных голографических решеток). Спектральное разрешение составило 1,46 нм при ширине щели 10 мкм. Габариты спектрометра – 11×11×3 см³, масса около 230 г.

Таблица 1 – Сравнительная таблица рассмотренных решений

Патент	RU 2624622	RU 2653772	RU 2635841	Fan 2021	Chen 2017
Тип прибора	Pushbroom + TDI	Сжатое зондирование		Pushbroom + LVF + TDI	Спектрометр с VLS-решеткой
Спектральный диапазон нм	400–1000	УФ-ИК	УФ-ИК	450–950	360–825
Спектральное разрешение	Не указано	Не указано	0.1–1 нм	10,2 нм	1,46 нм

Окончание табл. 1

Патент	RU 2624622	RU 2653772	RU 2635841	Fan 2021	Chen 2017
Пространственное разрешение	Высокое	Высокое	Высокое	10 м	10 мкм
Масса	3,2 кг	Не указана	Не указана	Легкая	230 г
Сложность изготовления	Средняя	Высокая	Высокая	Низкая	Средняя

Концепция гибридной камеры для условий России

Проведенный анализ показывает, что ни одно из рассмотренных решений не является универсально оптимальным для эксплуатации в климатических условиях Российской Федерации. Вместе с тем синтез нескольких подходов представляется перспективным.

В качестве базового диспергирующего элемента целесообразно использовать вогнутую VLS-решетку [7], обеспечивающую спектральное разрешение 1–2 нм при малых габаритах и массе. Для повышения отношения сигнал/шум при высоком пространственном разрешении предлагается внедрить цифровой TDI [6] в классической pushbroom-схеме, что потребует детектора с частотой кадров не менее 1000 fps.

Расширение спектрального диапазона в коротковолновую ИК-область (SWIR, до 1600–2500 нм) может быть реализовано путем добавления второго канала с дихроичным светоделителем и отдельной VLS-решеткой, аналогично патенту [2], но без применения сжатого зондирования. Альтернативный вариант – использование единого детектора на InGaAs, однако при этом придется пожертвовать видимым диапазоном.

Алгоритм компенсации мод интерферометра Фабри–Перо [3] для системы с решеткой представляется избыточным, однако при необходимости регистрации сверхузких спектральных линий он может быть реализован программно.

С учетом эксплуатации в широком интервале температур (–40...+50 °С) все оптические элементы должны размещаться в герметичном корпусе из материала с низким температурным коэффициентом линейного расширения (инвар, титан). Детектор следует термостабилизировать с помощью элемента Пельтье; при температурах ниже –40 °С может потребоваться подогрев корпуса, что несколько увеличит энергопотребление, но допустимо для кратковременных полетов БПЛА.

Заключение

Выполненный технический анализ пяти патентных документов и двух научных публикаций демонстрирует наличие нескольких конкурирующих подходов

к построению гиперспектральных систем. Наиболее перспективными для дальнейшего развития признаны:

- вогнутые решетки с переменным шагом (VLS) – благодаря высокому спектральному разрешению и компактности;
- цифровой TDI – как средство повышения SNR без увеличения апертуры;
- многощелевые структуры на ЖК-дисплеях – за счет гибкости и отсутствия механических узлов.

Российские патенты, в частности RU 2624622 и RU 2635841, содержат оригинальные идеи, заслуживающие практической реализации. Зарубежные публикации указывают на отработанные технологические цепочки (наноимпринтинг, линейные переменные фильтры), которые могут быть адаптированы к отечественной элементной базе.

В ближайшей перспективе планируется создание экспериментального образца гибридной камеры на основе VLS-решетки, изготовленной методом наноимпринтинга, с использованием российского ПЗС-детектора, поддерживающего режим цифрового TDI.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Щербина Г.А., Щербаков М.В. Многощелевая гиперспектральная камера с комбинированным отслеживанием изображения. Патент RU 2624622 С1. Оpubл. 04.07.2017.
2. Хан Шеншенг, Лиу Цхентао, Ву Джианронг и др. Система формирования широкополосного гиперспектрального изображения на основе сжатого зондирования с нерегулярной дифракционной решеткой. Патент RU 2653772 С1. Оpubл. 14.05.2018.
3. Корнышев Н.П., Гареев В.М., Гареев М.В. и др. Телевизионное гиперспектральное устройство. Патент RU 230837 U1. Оpubл. 20.12.2023 (дата публикации уточнена по реестру).
4. Мельников Г.С., Самков В.М. Гиперспектральный 2D (изображающий) спектрофотометр рассеянных или вынужденных излучений в широком (определенном) спектральном диапазоне. Патент RU 2635841 С2. Оpubл. 20.11.2017.
5. Ansley D.A., Cook L.G. Multi-slit spectrometer. Patent WO 1998010254 A1. Publ. 12.03.1998.
6. Fan X., Liu C., Liu S., Xie Y., Zheng L., Wang T., Feng Q. The Instrument Design of Lightweight and Large Field of View High-Resolution Hyperspectral Camera // Sensors. 2021. Vol. 21, No 7. P. 2276. DOI: 10.3390/s21072276.
7. Chen J., Chen W., Zhang G., Lin H., Chen S.C. High-resolution compact spectrometer based on a custom-printed varied-line-spacing concave blazed grating // Optics Express. 2017. Vol. 25, No 11. P. 12446–12454.

© К. В. Бондаренко, 2026

В. А. Васильева¹✉

Сравнение методов обработки для асферических зеркал и линз из разных материалов на станках алмазного микроточения

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: tupi4ok.nika@yandex.ru

Аннотация. В рамках данного исследования осуществлено сопоставление характеристик двух станков для алмазного микроточения: российского станка АМТ-150 и иностранного станка SATISLOH SPM/SPS-200. Основное внимание уделено их техническим характеристикам, возможностям обработки различных материалов, а также особенностям технологического процесса. Исследованы преимущества и недостатки каждого станка, выявлены их сильные и слабые стороны. Показано, что российский станок АМТ-150 обладает преимуществом по цене, доступности запчастей, универсальности и энергопотреблению, что делает его привлекательным вариантом для российских предприятий. В то же время, SATISLOH SPM/SPS-200 превосходит по точности обработки и автоматизации, что делает его лучшим выбором для задач, требующих ультравысокой точности и качества поверхности. Сделан вывод о том, что выбор станка для алмазного микроточения должен основываться на конкретных требованиях к точности, материалам и бюджету проекта.

Ключевые слова: алмазное микроточение, станок SPM/SPS-200, станок АМТ-150, оптические элементы

V. A. Vasileva¹✉

Comparison of processing methods on diamond micro-machining machines for aspherical mirrors and lenses made of different materials

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: tupi4ok.nika@yandex.ru

Abstract. This study compares the characteristics of two diamond micro-machining machines: the Russian AMT-150 machine and the foreign SATISLOH SPM/SPS 200 machine. The main focus is on their technical characteristics, processing capabilities for various materials, and the specific features of the manufacturing process. The advantages and disadvantages of each machine are explored, and their strengths and weaknesses are identified. It is shown that the Russian AMT-150 machine has an advantage in terms of price, availability of spare parts, versatility, and energy consumption, making it an attractive option for Russian enterprises. At the same time, the SATISLOH SPM/SPS 200 machine excels in terms of processing accuracy and automation, making it the best choice for tasks that require ultra-high precision and surface quality. Project-specific requirements for precision, materials, and budget should guide the selection of a diamond micro-machining machine.

Keywords: Diamond micro-abrasive finishing, SPM/SPS 200 machine tool system, AMT-150 production machine, optical elements

Введение

Сегодня в мире оптики очень важно уметь делать асферические линзы и зеркала. Они нужны везде: от самолетов и ракет до медицинского оборудования и автомобилей. Чтобы эти оптические детали получались максимально точными и качественными, часто используют алмазное микроточение. Этот способ позволяет сделать поверхность очень гладкой, почти без погрешностей, что напрямую влияет на то, насколько хорошо оптика будет работать.

Для определения преимуществ и недостатков, в статье будет проведен сравнительный анализ российского станка АМТ-150 и иностранного станка SPM/SPS-200, которые используются для алмазного микроточения. Основное внимание будет уделено их техническим характеристикам, возможностям обработки различных материалов.

Целью исследования является выявление сильных и слабых сторон обоих станков, а также определение наиболее подходящего оборудования для различных задач в оптической промышленности.

Характеристики и материалы

Алмазное микроточение – это метод высокоточной механической обработки, при котором используются сверхострые инструменты из природного алмаза для создания сложных поверхностей из различных материалов с высочайшей точностью. Это технология применяется в оптической промышленности для изготовления линз, зеркал и других оптических компонентов с минимальным отклонениями и идеальной гладкой поверхностью [1,2].

Станок SPM/SPS-200 представляет собой очень быстрый, очень эргономичный и твердый шлифовальный станок, разработанный с учетом новейших технологий, для производства сложных компонентов, прецизионной оптики. Он предназначен для работы с объектами до 200 мм в диаметре, которые выполнены из разрушаемых материалов, таких как стекло, хрусталь, инфракрасный материалов, алюминий, медные сплавы и керамики. Этот аппарат оснащен двумя шпинделями смонтирована на многофункциональной поворотной головкой, которая позволяет проводить одновременную обработку в нескольких различных режимах, таких как «включения и выключения инструмента Кубок ось» и «инструмент диск» режимы. Станок работает с высокой точностью и стабильностью благодаря прямому подключению двигателей шпинделей и осей, а также системе охлаждения водой [3, 9].

Для работы со станком SPM/SPS 200 можно использовать прямое программирование по стандарту DIN 66025 или подключить его к программе Satisloh CAMPos. Основание станка сделано из специального полимербетона, который помогает убирать вибрации, делает станок очень прочным и не дает ему нагреваться или остывать. Станок можно собрать из разных частей, чтобы поставить нужный шпиндель для разных задач. Встроенный 3D-измеритель позволяет проверять, насколько точно получилась деталь, и менять путь инструмента, чтобы

обработка была очень точной и всегда одинаковой. На рисунках 1 и 2 показано, модель станка и его рабочее место [4, 10].



Рис. 1. Изделие Satisloh, модель SPM/SPS 200

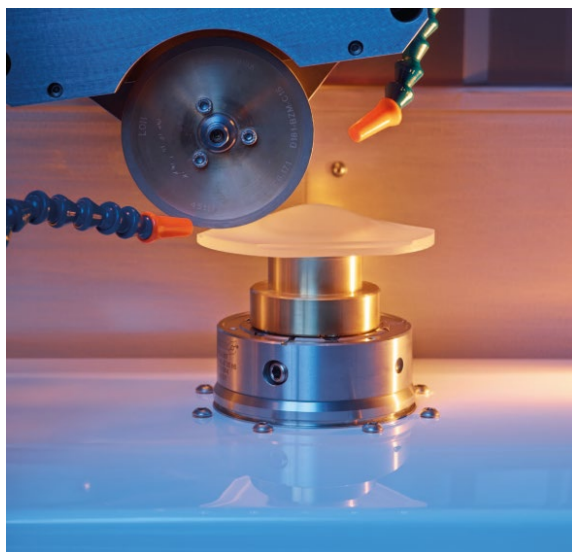


Рис. 2. Зона обработки станка SPM/SPS 200

Технология обработки [5]:

- алмазное микроточение: обработка с помощью алмазного инструмента с точностью до $\pm 0,1$ мкм и шероховатостью до 10 нм.
- полировка: завершающая стадия для достижения зеркального блеска.

Преимущества станка SPM/SPS-200 [5]:

- высочайшая точность: погрешность до $\pm 0,1$ мкм, идеальна для сложных асферических поверхностей.

- гладкость поверхности: Шероховатость до 10 нм, обеспечивает превосходное качество изображения.

- автоматизация: станок оснащен системами самокоррекции и мониторинга.

- универсальность: подходит для полимеров, металлов, керамик и стекол.

Область применения – высокоточные оптические системы (авиация, космонавтика, микроскопия), медицина (эндоскопы, хирургические системы), автомобильная и бытовая оптика (камеры, очки, VR/AR-устройства).

Идеален для: миниатюрных и средних оптических элементов с ультранизкой шероховатостью.

Не подходит для: крупногабаритных деталей.

Ультрапрецизионный станок алмазного микроточения АМТ-150 – это сверхточный станок с ЧПУ со стабильной производительностью и чрезвычайно высокой точностью обработки, который может адаптироваться к сложным условиям обработки [1, 6]. Общий вид станка и его рабочая зона показан на рисунках 3 и 4.

Данное оборудование разработано для высокоточного формирования оптических поверхностей, включая сферические, асферические и киноформные. Оно способно обрабатывать широкий спектр материалов, таких как оптический кристаллический германий, кремний, селенид и сульфид цинка, а также благородные металлы (золото, платина), свинец и полиметилметакрилат (известный также как авиационный пластик) [7, 8].



Рис. 3. Общий вид станка модели АМТ-150

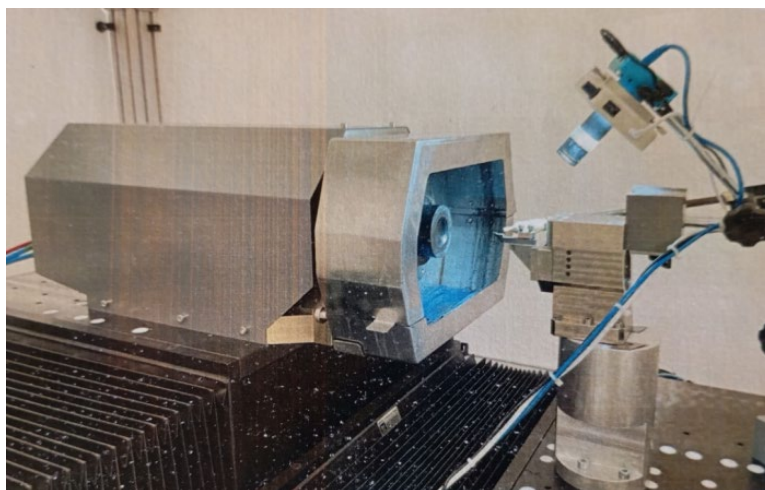


Рис. 4. Рабочая зона станка АМТ-150

Основные особенности применения станка:

- система контроля реального времени;
- станина из натурального гранита собственной частотой 2 Гц;
- гистологические направляющие для перемещения осей;
- ультрапрецизионный шпиндель на воздушной подушке 10.000 об/мин;
- встроенной системы измерения и коррекция профиля поверхности;
- система двойного контроля положения оси с разрешающей способностью

нм;

- большое количество вариантов обрабатывает поверхности: плоскости, сферических и асферических поверхностей, свободной формы и так далее [7].

Преимущества станка АМТ-150:

- широкий диапазон материалов: подходит для классических и экзотических оптических материалов.
- большая рабочая зона: позволяет обрабатывать крупные детали.
- доступность: традиционные методы шлифования и полировки дешевле.

Область применения – классическая оптика (астрономические телескопы, микроскопы), инфракрасная и ультрафиолетовая оптика (тепловизоры, лазерные системы), крупногабаритные оптические системы (зеркала для астрофизических обсерваторий) [8].

Идеален для: крупногабаритных деталей и широкого спектра материалов.

Не подходит для: сверхвысоких требований к точности ($\pm 0,1$ мкм).

Основные отличия и преимущества АМТ-150 по сравнению с SPM/SPS-200:

Цена и доступность запчастей: Российский станок АМТ-150 значительно выигрывает по цене и доступности сервисного обслуживания, что позволяет снизить затраты на эксплуатацию и ремонт;

Универсальность: АМТ-150 может использоваться не только для алмазного микроточения, но и для других видов обработки, что расширяет сферу применения станка;

Ремонтопригодность: конструкция станка АМТ-150 спроектирована с учетом удобства ремонта и замены деталей, что обеспечивает долговечность и надежность;

Энергопотребление: энергозатраты АМТ-150 ниже по сравнению с иностранным аналогом, что позволяет экономить на электричестве;

Климатическая адаптация: Российский станок лучше адаптирован к российским климатическим условиям, что обеспечивает стабильную работу в широком диапазоне температур;

Местная поддержка: наличие местных сервис-центров и поставщиков запчастей значительно упрощает обслуживание и ремонт.

Российский станок АМТ-150 показал себя как эффективный инструмент для работы с материалами различной степени твердости (от мягких до средней твердости). Его способность обрабатывать алюминий, керамику и полимеры делает его важным в таких отраслях как оптическая, медицинская и авиационная промышленность.

Помимо своих технических возможностей, АМТ-150 предлагает российским предприятиям ряд существенных преимуществ: выгодную цену, оперативную доступность запасных частей, широкую сферу применения и низкие эксплуатационные расходы по энергопотреблению.

Результаты

Результаты проведенного анализа свидетельствуют о наличии у российского станка АМТ-150 и иностранного станка SPM/SPS 200 как преимуществ, так и недостатков. Станок АМТ-150 характеризуется привлекательной ценой, широким спектром обрабатываемых материалов и удобством эксплуатации, что делает его привлекательным для российских производственных предприятий. В то же время, SPM/SPS 200 превосходит по показателям точности обработки и степени автоматизации, что определяет его применимость для задач, предъявляющих повышенные требования к точности и качеству поверхности.

В итоге, когда речь заходит о выборе станка для алмазного микроточения, главное – ориентироваться на то, какая точность нужна, с чем предстоит работать и сколько денег есть. Оба станка отлично справляются со своими задачами, и если правильно подобрать оборудование, то и оптические элементы получатся наилучшего качества.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Медунецкий В.М., Солк С.В. Опыт применения и перспективы технологии алмазного микроточения : Научно-технический вестник информационных технологий, механики и оптики: НИИ оптико-электронного приборостроения, 2014. – 165 с.
2. Бурыкин В. В. Шероховатость поверхностного слоя оптических изделий после алмазного микроточения: Вестник Брянского ГТУ, 2018.– 9 с.
- 3.Оборудование
https://promarchive.ru/catalog/machinetools/finishing_machines/surface_grinding_machines/precision_grinding_machine_optical_-_lt_200_mm_spm-140/?ysclid=mmvxsy9srm335421455

4. Ермолаев В. К. Шлифовальные станки для обработки оптики: журнал "РИТМ машиностроения" № 1-2019
5. Оборудование <https://www.satisloh.com/precision-optics/grinding/spm-150>
6. Медунецкий, В. М. Экспериментальные методы и средства защиты оптико-электронных систем космического базирования от механических воздействий: НИИ оптико-электронного приборостроения, 2023. – 910 с.
7. Гурин Н.А. Изготовление дифракционного оптического элемента методом презеционного алмазного микроточения: журнал «Интерэкспо ГЕО-Сибирь» , 2022.– 27 с.
8. Яковлев А. А., Солк С. В. Особенности технологического процесса изготовления охлаждаемых зеркал на основе меди и медных сплавов для мощных лазеров непрерывного и импульсно-периодического действия: оптический журнал, 2019. – 44 с.
9. Оборудование <https://www.sales-cncoptics.ru/products/pretsizionnaya-optika/shlifovalnie-stanki/spm-200/?ysclid=mo2e1j5kpl540886386>
10. Оборудование <https://pdf.directindustry.com/pdf/satisloh/precision-optics-spm-sps-200-grinding-polishing/36200-747213.html>

© В. А. Васильева, 2026

А. Д. Воропаев^{1✉}, В. М. Белов¹, Д. Л. Косов²

Требования к цифровым доказательствам, полученным с использованием систем искусственного интеллекта

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация

²Общество с ограниченной ответственностью «Надежда», г. Новосибирск
e-mail: wad0230@yandex.ru

Аннотация. В статье рассматриваются процессуальные требования, предъявляемые к цифровым доказательствам, сформированным с применением систем искусственного интеллекта. Анализируется проблема допустимости подобных доказательств в условиях отсутствия специализированного правового регулирования в Уголовно-процессуальном кодексе Российской Федерации (УПК РФ). Особое внимание уделено феномену «черного ящика», вопросам верификации алгоритмических выводов и распределения ответственности за ошибки искусственного интеллекта. На основе доктринального анализа и изучения зарубежного опыта сформулированы предложения по внедрению критериев воспроизводимости и транспарентности как обязательных условий признания доказательственной силы за результатами работы интеллектуальных систем.

Ключевые слова: цифровые доказательства, искусственный интеллект, допустимость доказательств, уголовный процесс, «черный ящик», верификация, алгоритмическая прозрачность, машинное обучение, электронные носители информации, процессуальная форма

A. D. Voropaev^{1✉}, V. M. Belov¹, D. L. Kosov¹

Requirements for Digital Evidence Obtained Using Artificial Intelligence Systems

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: wad0230@yandex.ru

Abstract. The article examines the procedural requirements for digital evidence generated using artificial intelligence (AI) systems. The article analyzes the problem of the admissibility of such evidence in the absence of specialized legal regulation in the Criminal Procedure Code of the Russian Federation. Special attention is paid to the phenomenon of the «black box», the verification of algorithmic conclusions and the allocation of responsibility for AI errors. Based on a doctrinal analysis and the study of foreign experience, proposals have been formulated to introduce criteria for reproducibility and transparency as mandatory conditions for recognizing the evidentiary value of the results of the work of intelligent systems.

Keywords: digital evidence, artificial intelligence, admissibility of evidence, criminal procedure, «black box», verification, algorithmic transparency, machine learning, electronic media, procedural form

Введение

Дискуссия о правовой природе и допустимости электронных данных в уголовном судопроизводстве России имеет многолетнюю историю. В научной ли-

тературе традиционно выделяются работы, посвященные проблемам собирания и фиксации доказательств на электронных носителях. Так, после принятия Федерального закона от 28 июля 2012 г. № 143-ФЗ в УПК РФ, впервые появилась категория «электронные носители информации», которую законодатель отнес к вещественным доказательствам [1], что положило начало формированию нормативной базы для работы с цифровыми следами. Дальнейшее развитие данная проблематика получила в исследованиях Д.В. Бахтева, О.В. Гладышевой, Я.В. Лошкобановой и В.А. Семенцова, в которых предпринята попытка осмысления места искусственного интеллекта (ИИ) в системе средств уголовно-процессуального доказывания. При этом вопросы допустимости результатов, генерируемых системами ИИ, остаются недостаточно изученными, а законодательные механизмы их оценивания фактически отсутствуют.

Актуальность темы обусловлена взрывным ростом объемов цифровой информации, подлежащей анализу в рамках расследования преступлений. Экстенсивное увеличение массива данных, содержащихся в социальных сетях, мессенджерах, облачных хранилищах и на иных интернет-ресурсах, делает невозможным их полноценный осмотр и оценивание исключительно силами человека [2]. Следователь и суд объективно нуждаются в автоматизированных инструментах, способных обрабатывать большие данные, выявлять скрытые закономерности и логические противоречия в показаниях [3]. ИИ уже применяется для распознавания лиц, анализа видео, построения поведенческих моделей и даже для создания текстовых моделей судебного следствия с целью последующего поиска в них несоответствий. Вместе с тем, стремительное развитие технологий генеративного ИИ порождает новые риски, связанные с появлением дипфейков и иных форм высокотехнологичной фальсификации доказательств [4].

Проблема исследования заключается в отсутствии четких правовых регламентов, определяющих условия и пределы использования данных, полученных с помощью систем ИИ, в процессе доказывания по уголовным делам [5]. Действующий УПК РФ не содержит ни легальной дефиниции «цифрового доказательства», ни специальных норм, регулирующих алгоритмическую обработку информации [6]. Такая правовая неопределенность создает риски признания недопустимыми доказательств, полученных с применением передовых технологий, либо, напротив, некритичного принятия судами машинных выводов без надлежащей проверки их достоверности.

Целью настоящего исследования является выявление пробелов в уголовно-процессуальном законодательстве и разработка предложений по обеспечению допустимости цифровых доказательств, сформированных с использованием ИИ. Для достижения поставленной цели необходимо решить следующие задачи:

- 1) проанализировать существующие требования к допустимости доказательств по УПК РФ и их применимость к цифровым данным;
- 2) исследовать проблему «черного ящика» и ее влияние на оценивание достоверности результатов работы ИИ;

3) определить условия, при которых результаты алгоритмического анализа могут приобретать доказательственную силу;

4) сформулировать практические рекомендации по совершенствованию правового регулирования.

Теоретическая значимость работы состоит в систематизации научных подходов к пониманию правовой природы цифровых доказательств, полученных с участием ИИ, и обосновании необходимости введения специальных критериев их допустимости. Практическая значимость заключается в возможности использования сформулированных предложений для совершенствования уголовно-процессуального законодательства и формирования единообразной судебной практики оценивания таких доказательств.

Допустимость доказательств как ключевой институт уголовного процесса

Допустимость доказательств является фундаментальной категорией уголовно-процессуального права, определяющей саму возможность использования тех или иных сведений для установления обстоятельств, подлежащих доказыванию. Согласно ч. 1 ст. 75 УПК РФ, доказательства, полученные с нарушением требований уголовно-процессуального закона, являются недопустимыми, не имеют юридической силы и не могут быть положены в основу обвинения, а также использоваться для доказывания любого из обстоятельств, предусмотренных ст. 73 УПК РФ [7]. Таким образом, допустимость выступает своего рода процессуальным фильтром, отсекающим информацию, добытую неправомерным путем.

Традиционная доктрина уголовного процесса выделяет несколько обязательных условий допустимости:

1) доказательство должно быть получено надлежащим субъектом, уполномоченным на производство процессуальных действий;

2) источник доказательства должен соответствовать перечню, установленному ч. 2 ст. 74 УПК РФ;

3) процедура собирания, фиксации и закрепления доказательства должна строго соответствовать предписанной законом процессуальной форме.

Нарушение любого из этих условий влечет за собой признание доказательства недопустимым [8].

Внедрение цифровых технологий в сферу уголовного судопроизводства поставило перед правоприменителем ряд принципиально новых вопросов. Прежде всего, до настоящего времени в УПК РФ отсутствует легальное определение понятия «электронное доказательство», что существенно осложняет их понимание и использование в уголовном судопроизводстве [6]. Законодатель ограничился лишь отнесением электронных носителей информации к категории вещественных доказательств [1], что явно недостаточно для охвата всего многообразия цифровых данных (облачные хранилища, потоковые данные, результаты работы алгоритмов). В доктрине неоднократно высказывались предложения о необходи-

мости пополнения уголовно-процессуального закона дефиницией электронных доказательств и закреплением порядка обращения с ними [6].

Цифровые доказательства обладают рядом специфических особенностей, предопределяющих повышенные правовые риски их использования. Во-первых, они характеризуются высокой степенью изменчивости и подверженности модификации, что требует применения специальных технических средств для обеспечения их аутентичности и целостности (хэширование, цифровая подпись, временные метки) [9]. Во-вторых, цифровая информация, как правило, неразрывно связана с материальным носителем, однако может существовать в виртуальной среде без четкой географической локализации. В-третьих, оценивание цифровых доказательств зачастую требует специальных познаний в области информационных технологий, что обуславливает необходимость привлечения специалистов или производства судебных экспертиз. Классические критерии допустимости доказательств, сформированные в эпоху «бумажного» делопроизводства, сталкиваются с новыми вызовами при оценивании цифровых данных [5].

Применительно к доказательствам, полученным с использованием ИИ, проблема допустимости приобретает особую остроту. Результаты работы алгоритмов машинного обучения не подпадают в чистом виде ни под одну из традиционных категорий, предусмотренных ст. 74 УПК РФ. Они не являются в полном смысле ни вещественными доказательствами, ни документами, ни заключением эксперта, поскольку генерируются не человеком, а автоматизированной системой. Как справедливо отмечается в литературе, ИИ не является субъектом уголовного процесса, не относится к техническим средствам по смыслу норм УПК, не несет ответственности за принятые решения и не обладает внутренним убеждением [10]. Следовательно, возникает настоятельная потребность в выработке специальных критериев, позволяющих оценивать допустимость и достоверность таких данных. При этом суды критически относятся к использованию нейросетей при подготовке доказательств по делу, подчеркивая, что такие материалы не отвечают критерию достоверности и не позволяют проверить источник сведений [11].

Искусственный интеллект как субъект процессуальной деятельности: проблемы атрибуции и верификации

Одной из центральных проблем, препятствующих полноценной интеграции ИИ в систему уголовно-процессуального доказывания, является так называемый «эффект черного ящика». Под ним понимается фундаментальная непрозрачность алгоритмических процессов, протекающих внутри сложных нейросетевых моделей. Даже разработчики таких систем зачастую не могут с достоверностью объяснить, почему на основе одних и тех же входных данных модель пришла к тому или иному выводу [12]. Данный принцип предполагает, что любая юридически значимая операция, совершенная «черным ящиком», должна подлежать верификации человеком, а правовые последствия такой операции должны быть вменены конкретному субъекту права. В контексте уголовного судопроизводства, где цена ошибки измеряется судьбой человека, непрозрачность алгоритмов создает

непреодолимое препятствие для их использования в качестве источника доказательств, поскольку суд и стороны лишены возможности полноценно проверить корректность машинных выводов [13].

В современных исследованиях предпринимаются попытки преодоления «эффекта черного ящика» с помощью технологий механистической интерпретируемости, которые позволяют визуализировать внутренние связи в нейросетях и выявлять, какие именно части модели отвечают за конкретное поведение. Однако широкое внедрение таких технологий в юридическую практику – дело отдаленного будущего. На сегодняшний день наиболее реалистичным подходом является внедрение стандартов объяснимости и обязательного человеческого контроля за результатами работы ИИ.

С проблемой «черного ящика» тесно связан вопрос ответственности за ошибки, допущенные ИИ при обработке данных [14]. Кто должен нести юридическую ответственность в случае, если алгоритмический вывод повлек за собой неверную квалификацию деяния, незаконное привлечение к уголовной ответственности или, напротив, укрытие преступления: разработчик программного обеспечения, следователь, применивший систему, эксперт, интерпретировавший результаты, или само государство? Очевидно, что ИИ лишен социоцентрической мотивации при принятии решения, а применяемый им алгоритм не может охватить множественность мотивационных установок, обусловленных как назначением правосудия, так и субъективно-личностными особенностями судьи, рассматривающего дело [10]. Ответственность в любом случае должна возлагаться на человека – либо на должностное лицо, принявшее процессуальное решение на основе данных ИИ, либо на эксперта, использовавшего ИИ в качестве инструмента исследования. Однако для этого необходимо четко разграничить функции человека и машины в процессе доказывания. Как отмечается в литературе, системы ИИ не обладают правосубъектностью и не могут нести уголовную ответственность [15].

С точки зрения уголовно-процессуальной формы, результаты работы ИИ могут быть введены в процесс двумя основными способами: либо как приложение к протоколу следственного действия (например, осмотра интернет-ресурсов), либо как составная часть заключения эксперта или специалиста. При этом в доктрине обосновано, что результаты работы систем ИИ в процессе доказывания по уголовному делу являются вспомогательными средствами доказывания [16]. В любом случае, обязательным условием их допустимости должна выступать проверяемость и воспроизводимость полученных результатов. Воспроизводимость является фундаментальным требованием для признания судебных доказательств допустимыми: независимый эксперт должен иметь возможность применить ту же методологию и прийти к тем же результатам. Применительно к ИИ это означает, что алгоритм должен быть документирован, его исходный код или, по крайней мере, архитектура и параметры должны быть доступны для независимого экспертного оценивания, а процесс обучения модели должен быть верифицируемым [17].

В международной практике прослеживается ужесточение подходов к оцениванию доказательств, полученных с применением алгоритмических систем. Показательным примером здесь служат правовые тенденции в Соединенных Штатах, где в настоящее время идет работа над Предлагаемым правилом доказывания 707. Согласно проекту этого документа, любая информация, сгенерированная машиной, должна отвечать тем же критериям надежности, которые предъявляются к заключению и показаниям эксперта-человека [18]. В странах Европейского союза аналогичным образом инициированы процессы формирования нормативной базы, касающейся применения ИИ в сфере уголовной юстиции. Особый акцент в этих инициативах сделан на обязательной прозрачности вычислительных процессов и возможности независимой перепроверки итоговых данных [19]. Практическим следствием таких требований становится обязанность инициатора использования ИИ-доказательства раскрыть не только конечный результат, но и исходные массивы информации, методологию их обработки, а также подтвердить, что конкретная вычислительная модель применялась к этим данным корректно и не дала сбой.

Результаты

Итоги анализа позволяют сгруппировать основные препятствия для признания цифровых ИИ-доказательств допустимыми по нескольким ключевым направлениям, которые образуют единую структурно-логическую модель.

Первая группа рисков связана с непрозрачностью алгоритмического механизма (так называемый «черный ящик»). Если архитектура нейронной сети и логика принятия ею решений остаются недоступными для изучения участниками процесса, суд лишается возможности убедиться в отсутствии случайной или системной ошибки, что делает результат работы ИИ непригодным для доказывания. Сопутствующим требованием здесь становится документирование процесса обучения модели, включая фиксацию версий программного обеспечения и характеристик тренировочных выборок, поскольку без этих сведений невозможно воспроизвести полученные выводы на другом оборудовании.

Второй блок касается обеспечения целостности и аутентичности исходных цифровых объектов. Любое неконтролируемое изменение файла или потока данных, произошедшее до момента процессуальной фиксации, влечет недопустимость сведений согласно ст. 75 УПК РФ. Минимизировать подобные риски можно лишь внедрением криптографических методов защиты (расчет хэш-сумм, использование электронной подписи) и ведением непрерывного журнала событий.

Третья группа проблем охватывает процессуальную форму. В настоящее время в УПК РФ не закреплены ни отдельный вид доказательств, ни специальная процедура осмотра информационных ресурсов с применением ИИ. Соответственно, даже технически корректный результат анализа может утратить силу из-за пробелов в протоколировании. Выходом видится внесение в закон норм, обязывающих указывать в протоколе не только факт применения автоматизированной системы, но и ее идентификационные параметры.

Наконец, нельзя игнорировать человеческий фактор и вопрос смещения данных. Поскольку ИИ не обладает процессуальной правосубъектностью, бремя доказывания надежности алгоритма и корректности его обучения ложится на ту сторону, которая ходатайствует о приобщении таких материалов. Кроме того, требуется обязательная предварительная валидация модели на предмет наличия дискриминационных искажений и оценивание частоты ошибочных срабатываний.

Обсуждение

Изложенные данные подтверждают тезис о том, что действующая система уголовно-процессуального оценивания доказательств оказалась не готова к экспансии технологий машинного обучения. Сложившаяся нормативная база, ориентированная на традиционные источники информации, не содержит инструментов для адекватной проверки данных, генерируемых самообучающимися алгоритмами. Это подтверждается и выводами других исследователей. В частности, А.П. Папикян указывает на отсутствие в УПК РФ не только легального определения «электронных доказательств», но и универсальных критериев их допустимости [5]. Аналогичной позиции придерживаются авторы, подчеркивающие назревшую необходимость дополнения УПК РФ статьей 74.1, содержащей определение электронных доказательств [6]. Неуказание хэш-суммы цифрового файла в постановлении о назначении экспертизы и в самом экспертном заключении признается в литературе серьезной процессуальной ошибкой, влекущей невозможность идентификации цифрового объекта [9]. Высказываются предложения о необходимости закрепления в УПК РФ принципов использования технологий ИИ в экспертной деятельности [20].

Интересным представляется сопоставление полученных результатов с подходами, выработанными в зарубежной доктрине. В исследовании Singh S. подчеркивается, что, несмотря на очевидный потенциал ИИ для повышения эффективности анализа доказательств, суды демонстрируют вариативность в принятии таких доказательств из-за ограниченной технической грамотности и отсутствия стандартизированных протоколов валидации [21]. Это наблюдение в полной мере применимо и к российской правовой действительности. Более того, в зарубежной практике уже формируется понимание необходимости многоуровневой системы проверки ИИ-доказательств, включающей предварительную оценку на стадии расследования, контроль со стороны прокурора и углубленную судебную проверку с привлечением технических специалистов.

Представляется, что предложенная в настоящей статье модель обеспечения допустимости ИИ-доказательств, основанная на принципах транспарентности, воспроизводимости и обязательного человеческого контроля, в целом коррелирует с международными тенденциями [19]. Вместе с тем необходимо признать, что российская правовая система обладает определенной спецификой. В отличие от англосаксонской модели, где акцент делается на состязательности и экспертных показаниях, в российском уголовном процессе ключевое значение имеет соблюдение процессуальной формы собирания доказательств. Следовательно, про-

стое заимствование зарубежных подходов без их адаптации к отечественным реалиям невозможно. Кроме того, актуальной проблемой является необходимость совершенствования методического обеспечения применения ИИ в судебной деятельности [22].

Дискуссионным остается вопрос о допустимости использования генеративного ИИ для создания текстовых моделей судебного следствия. Как отмечается в литературе, нейросеть не способна выступать в роли субъекта оценивания доказательств, но она может быть эффективно задействована для анализа логических противоречий в показаниях [23]. Представляется, что такая практика допустима лишь при условии, что окончательные выводы делаются судом самостоятельно, на основе своего внутреннего убеждения, а результаты работы ИИ рассматриваются не как готовое доказательство, а как вспомогательный аналитический инструмент [24].

Заключение

Проведенное исследование позволяет сформулировать следующие основные выводы и рекомендации.

Действующее уголовно-процессуальное законодательство Российской Федерации не содержит норм, регламентирующих порядок получения, проверки и оценивания цифровых доказательств, сформированных с применением систем ИИ. Отсутствие легальной дефиниции «электронное доказательство» и специальных критериев допустимости создает правовую неопределенность и препятствует эффективному использованию передовых технологий в доказывании.

Ключевыми условиями признания допустимости результатов работы ИИ должны выступать:

- 1) прозрачность алгоритма, исключая «эффект черного ящика» и обеспечивающая возможность понимания логики машинных выводов;
- 2) воспроизводимость результатов, гарантирующая возможность их независимой проверки;
- 3) соблюдение процессуальной формы фиксации, включающей обязательное отражение в протоколе следственного действия факта и условий применения ИИ;
- 4) обязательный человеческий контроль и интерпретация результатов специалистом или экспертом.

В целях устранения выявленных пробелов правового регулирования представляется необходимым внесение изменений в УПК РФ, предусматривающих:

- 1) введение статьи 74.1 «Электронные доказательства», содержащей определение и критерии допустимости цифровых данных;
- 2) дополнение норм о производстве осмотра (ст. 176–177 УПК РФ) положениями об особенностях осмотра интернет-ресурсов с применением ИИ, включая обязанность фиксации в протоколе используемых алгоритмов и их версий;
- 3) установление требования обязательной сертификации программного обеспечения, используемого в целях получения доказательств.

Дальнейшие научные исследования в данной области должны быть направлены на разработку конкретных методик верификации алгоритмов машинного обучения в контексте уголовного судопроизводства, а также на изучение возможностей применения технологий объяснимого ИИ (ХАИ) для повышения прозрачности и проверяемости машинных выводов [25]. Особого внимания заслуживает проблема правового оценивания доказательств, потенциально сфальсифицированных с помощью генеративных нейросетей (дипфейков) [4].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Российская Федерация. Законы. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 28.07.2012 № 143-ФЗ // Собрание законодательства РФ. – 2012. – № 31. – Ст. 4332. – URL: <https://www.consultant.ru> (дата обращения: 19.04.2026).
2. Бирюков, С. Ю. Современные инструменты оптимизации расследования: искусственный интеллект, Big Data и интеллект-карты / С. Ю. Бирюков // Вестник Сургутского государственного университета. – 2025. – № 4. – URL: <https://www.surguvest.ru> (дата обращения: 19.04.2026).
3. К вопросу о перспективах использования технологий искусственного интеллекта в процессе доказывания по уголовным делам // Молодой ученый. – 2025. – URL: <https://moluch.ru> (дата обращения: 19.04.2026).
4. Экспертиза видеозаписей на дипфейк: правовые основы, методики и практические кейсы // Федерация судебных экспертов. – 2026. – URL: <https://sud-expertiza.ru> (дата обращения: 19.04.2026).
5. Папикян, А. П. Использование недопустимых доказательств в условиях цифровых технологий: правовые и этические аспекты / А. П. Папикян // Государственная служба и кадры. – 2024. – № 3. – С. 210–213.
6. Корнакова, С. В. Электронные доказательства в российском уголовном процессе: проблемные вопросы / С. В. Корнакова, Е. В. Чигрина // Юридический вестник Самарского университета. – 2025. – Т. 11, № 2. – С. 44–50. – DOI: 10.18287/2542-047X-2025-11-2-44-50.
7. Российская Федерация. Законы. Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18.12.2001 № 174-ФЗ (ред. от 08.03.2026) // Собрание законодательства РФ. – 2001. – № 52 (ч. I). – Ст. 4921. – URL: <https://www.consultant.ru> (дата обращения: 19.04.2026).
8. Допустимость доказательств в уголовном процессе. – М. : Проспект, 2025. – URL: <https://www.consultant.ru> (дата обращения: 19.04.2026).
9. Шихалиева, С. З. Отсутствие хэш-суммы как процессуальная ошибка, возникающая в судебной экспертизе при исследовании объектов в цифровой форме / С. З. Шихалиева // Правовое государство: теория и практика. – 2025. – № 1. – DOI: 10.33184/pravgos-2025.1.28.
10. Шеляшкова, А. А. Допустимость использования искусственного интеллекта в уголовном процессе. На что обратить внимание защите / А. А. Шеляшкова, Е. В. Исакова // Уголовный процесс. – 2026. – № 4. – URL: <https://e.ugpr.ru> (дата обращения: 19.04.2026).
11. Деева, К. Оппонент защищается документами из нейросети. Примет ли суд такие доказательства / К. Деева // Юридический справочник руководителя. – 2026. – URL: <https://e.law.ru> (дата обращения: 19.04.2026).
12. Алферов, А. В. Проблема «черного ящика» искусственного интеллекта в гражданском и арбитражном процессе: между судебным усмотрением и технологическим детерминиз-

мом / А. В. Алферов, В. М. Кирьянова. – URL: <https://cyberleninka.ru> (дата обращения: 19.04.2026).

13. К вопросу о принципе прозрачности искусственного интеллекта в контексте феномена «черного ящика» // Молодой ученый. – 2025. – URL: <https://moluch.ru> (дата обращения: 19.04.2026).

14. Туров, С. С. Проблема ответственности в сфере применения искусственного интеллекта / С. С. Туров, Н. В. Григорьева // Современное право. – 2025. – С. 131–134. – DOI: 10.25799/NI.2025.38.82.024.

15. Уголовно-правовая ответственность за преступления, совершенные с использованием систем искусственного интеллекта. – URL: <https://cyberleninka.ru> (дата обращения: 19.04.2026).

16. Соотношение средств доказывания в уголовном судопроизводстве и результатов работы алгоритмов искусственного интеллекта // InLibrary.uz. – 2025. – URL: <https://inlibrary.uz> (дата обращения: 19.04.2026).

17. Калиев, А. А. Искусственный интеллект в криминалистике: доказательственные перспективы и риски манипуляции / А. А. Калиев // Криминалистика и судебная экспертиза. – 2025. – № 4. – С. 76–89. – DOI: 10.51634/2307-5201_2025_4_76.

18. К вопросу о допустимости в уголовном судопроизводстве информации, генерируемой системами с элементами машинного обучения (на примере США) // Международное уголовное право и международная юстиция. – 2025. – № 1. – С. 23–26. – DOI: 10.18572/2071-1190-2025-1-23-26.

19. Сарсенбаева, Б. Б. Интеграция искусственного интеллекта в криминалистическую практику: от анализа данных к принятию решений / Б. Б. Сарсенбаева, А. К. Шаркемелов, С. А. Бегимбаев // Eurasian Scientific Journal of Law. – 2025. – URL: <https://esjl.turan-edu.kz> (дата обращения: 19.04.2026).

20. Костенко, Р. В. Проблемы нормативного обеспечения прозрачности экспертной деятельности при использовании новых технологий для анализа доказательств (на примере машинного обучения) / Р. В. Костенко, М. А. Духанова // Закон и право. – 2025. – № 5. – С. 210–214. – DOI: 10.24412/2073-3313-2025-5-210-214.

21. Singh, S. Reliability and Admissibility of AI-Generated Forensic Evidence in Criminal Trials / S. Singh // National Seminar on Criminal Law and Justice Reforms. – 2025. – P. 45–53.

22. Шайдуллин, Р. Р. О совершенствовании методического обеспечения применения технологий искусственного интеллекта в судебно-экспертной деятельности в условиях цифровизации / Р. Р. Шайдуллин // Вестник Института права Башкирского государственного университета. – 2026. – № 1. – DOI: 10.33184/vest-law-bsu-2026.29.26.

23. Использование нейросетевых языковых моделей в судебном следствии при производстве по уголовному делу // Российский судья. – 2026. – № 2. – С. 33–37. – DOI: 10.18572/1812-3791-2026-2-33-37.

24. Теория средств уголовно-процессуального доказывания о результатах работы алгоритмов систем искусственного интеллекта // Психолого-педагогические исследования. – 2025. – URL: <https://phsreda.com> (дата обращения: 19.04.2026).

25. Richmond, K. M. Explainable AI and Law: An Evidential Survey / K. M. Richmond, S. M. Muddamsetty, T. Gammeltoft-Hansen [et al.] // Digital Society. – 2024. – Vol. 3, № 1. – DOI: 10.1007/s44206-023-00081-z.

26.

© А. Д. Воронаев, В. М. Белов, Д. Л. Косов, 2026

А. В. Галлямова¹✉, В. М. Белов¹

Содержание блока психофизических характеристик специалиста в области информационной безопасности

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: allna.black@yandex.ru

Аннотация. В данной статье рассматривается проблема систематизации психофизических характеристик специалиста в области информационной безопасности (далее – ИБ) как основы для формирования базы знаний искусственного интеллекта (далее – ИИ), которая в свою очередь, сможет оказывать помощь в кадровых вопросах. На основании анализа международных нормативных документов, нормативных документов Российской Федерации, моделей компетенций, а также научной литературы по психологии труда и инженерной психологии определено содержание блока психофизических характеристик, которые могут относиться к профессиональной деятельности в сфере ИБ. Предложена многоуровневая структура блока, включающая когнитивные, личностные, психофизиологические и мотивационно-ценностные компоненты. Выделены профили для основных ролевых категорий согласно таксономии NICE Workforce Framework (National Initiative for Cybersecurity Education Workforce Framework). Результаты могут быть использованы при разработке онтологий предметной области и инструментов для автоматизированной оценки профессиональной пригодности.

Ключевые слова: информационная безопасность, человеческий фактор, психофизические характеристики, профессионально важные качества, база знаний, NICE Framework, психограмма специалиста информационной безопасности

A. V. Gallyamova¹✉, V. M. Belov

Contents of a Set of Psychophysical Characteristics of an Information Security Specialist

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: allna.black@yandex.ru

Abstract. This article examines the problem of systematizing the psychophysical characteristics of an information security (IS) specialist as a basis for developing an artificial intelligence (AI) knowledge base, which in turn can assist in personnel matters. Based on an analysis of international regulatory documents, Russian Federation regulations, competency models, and scientific literature on occupational psychology and engineering psychology, the content of a set of psychophysical characteristics that may be relevant to professional activity in IS is determined. A multi-level structure is proposed for this set, including cognitive, personality, psychophysiological, and motivational-value components. Profiles for key role categories were identified according to the NICE Workforce Framework (National Initiative for Cybersecurity Education Workforce Framework) taxonomy. The results can be used in the development of domain ontologies and tools for automated assessment of professional suitability.

Keywords: information security, human factors, psychophysical characteristics, professionally important qualities, knowledge base, NICE Framework, information security specialist psychogram

Введение

Современная концепция информационной безопасности акцентирует внимание не только на технических средствах, но и на роли человека, многочисленные исследования, в том числе отчеты аналитических компаний и государственных регуляторов, в сфере информационной безопасности, свидетельствуют о том, что множество инцидентов в области ИБ прямо или косвенно обусловлены действиями, бездействием, либо психологической уязвимостью персонала [1, 2], в связи с этим становится актуальной задача научно обоснованного определения требований к психофизическим характеристикам специалистов, деятельность которых непосредственно связана с обеспечением конфиденциальности, целостности и доступности информации.

В Российской и зарубежной практике существуют разносторонние подходы к описанию компетенций специалиста по ИБ, отраженные в профессиональных стандартах, квалификационных требованиях и отраслевых руководствах [3–5], однако в большинстве из них психофизический аспект отсутствует вовсе, либо представлен в обтекаемой и неконкретной форме. Это создает серьезную проблему при попытке построения интеллектуальных систем, в частности баз знаний, ориентированных на поддержку кадрового отбора, оценки и развития персонала в области ИБ [16].

Целью данной статьи является определение и структурирование содержания блока психофизических характеристик специалиста в области информационной безопасности, руководствуясь совокупностью нормативных, теоретических и эмпирических источников. Достижение данной цели позволит в дальнейшем выстраивать соответствующие знания в виде онтологии предметной области, пригодной для использования в системах искусственного интеллекта.

Методы и методики

Методологическая основа исследования состоит из системного анализа научной литературы и нормативно-технической документации в трех пересекающихся предметных областях: психология труда и инженерная психология, информационная безопасность и управление персоналом.

В качестве нормативной базы были использованы следующие документы:

NIST Special Publication 800-181 (NICE Workforce Framework) – наиболее полная на сегодняшний день таксономия рабочих ролей в области ИБ, содержащая детализированные перечни знаний, умений и способностей (KSAs) для каждой роли [3];

профессиональные стандарты Российской Федерации, утвержденные Министерством труда и социальной защиты: «Специалист по информационной безопасности», «Аналитик информационной безопасности», «Аудитор в области информационной безопасности» [4];

– руководящие документы ФСТЭК России и ФСБ России в части требований к персоналу, осуществляющему функции по обеспечению ИБ [5];

– ISO/IEC 27001:2022 и сопутствующие стандарты серии 27000 в части требований к компетентности персонала, вовлеченного в систему менеджмента информационной безопасности.

Теоретический анализ опирался на фундаментальные труды в области психологии профессиональной пригодности [6, 7], психодиагностики функциональных состояний [8], а также классические работы по эргономике и человеческому фактору [9]. Особое внимание уделялось источникам, раскрывающим специфику уязвимостей человеческого сознания в контексте социальной инженерии [10], поскольку они позволяют выявить качества, необходимые для предотвращения сопутствующих угроз безопасности информации.

Методика исследования включала контент-анализ требований к персоналу, зафиксированных в вышеперечисленных документах, с последующим распределением выявленных дескрипторов в категории, соответствующие традиционной структуре психограммы: когнитивные процессы, личностные черты, психофизиологические характеристики, мотивационно-ценностные ориентации. Для каждой ролевой категории, выделенной в NICE Workforce Framework, был составлен профиль соответствующих характеристик с учетом специфики выполняемых задач.

Результаты

Проведенный анализ позволил выделить основную структуру психофизических характеристик, значимых для большинства ролей в области ИБ, а также специфические требования, относящихся к разным функциональным категориям.

1. Основная структура психофизических характеристик специалиста по ИБ **Когнитивный блок:**

– аналитическое и дедуктивное мышление – способность выявлять закономерности при работе с большим объемом информации, строить причинно-следственные связи, видеть систему в целом. Для аналитиков угроз данная характеристика является критической, поскольку напрямую влияет на способность распознавания и выявления подозрительных событий ИБ;

– критичность мышления – умение быстро и эффективно обдумывать поступающую информацию, соотносить правдоподобность источников, распознавать попытки манипуляции и социальной инженерии. Можно отметить, что данное качество особенно актуально, так как атаки, эксплуатирующие доверчивость и когнитивные искажения, являются наиболее эффективными, основным примером этого можно считать работы Митника и Хэднаги [10];

– внимание (концентрация, устойчивость, переключаемость) – способность длительное время уметь концентрироваться на однотипной и монотонной деятельности (например, мониторинг событий безопасности), а также быстро переключаться между задачами при возникновении инцидента ИБ. Стандарт NIST SP

800-63, описывающий процедуры аутентификации, косвенно предполагает высокий уровень внимательности при работе с учетными данными [3];

- рабочая память и скорость обработки информации – необходимы для оперативного принятия решений в условиях максимальной срочности, характерного для реагирования на инциденты ИБ.

Личностный блок (черты, близкие к конструктам «Большой пятерки»):

- добросовестность – организованность, дисциплинированность, следование определенным правилам и регламентам. Требования ФСТЭК России и ФСБ России к работе с государственной тайной косвенно склоняются именно к этому качеству, подобно и другим стандартам, регулирующим требования к защите информации;

- эмоциональная стабильность (противоположный полюс — нейротизм) – устойчивость к стрессу, способность сохранять спокойствие в критических ситуациях (инциденты ИБ, давление со стороны злоумышленников при социотехнических атаках). Методология оценки функциональных состояний, разработанная А.Б. Леоновой [8], предоставляет способы для диагностики этого параметра;

- интернальный локус контроля (ответственность) – склонность приписывать ответственность за результаты деятельности собственным действиям, а не внешним обстоятельствам;

- бдительность и умеренная подозрительность к обстоятельствам – данное качество не является патологической паранойей, а профессионально обусловленная настороженность, готовность к обнаружению подозрительных событий в поведении пользователей и систем.

Психофизиологический блок:

- стрессоустойчивость – способность организма выдерживать длительные когнитивные и эмоциональные нагрузки без особого снижения эффективности осуществляемой деятельности. Например, для операторов центров мониторинга (SOC) характерна высокая когнитивная нагрузка, что требует особого внимания к данному параметру;

- работоспособность в условиях тяжелого режима работы, недостаток сна и большое количество монотонной работы, все это также относится к посменной работы в режиме 24/7 центра мониторинга.

Мотивационно-ценностный блок:

- профессиональная этика и лояльность – соответствие моральным нормам ИБ-сообщества, осознание социальной ответственности. Работы Е.А. Климова по профессиональному самоопределению [11] позволяют определить концепцию этого компонента как интегральную характеристику личности специалиста;

- мотивация достижения в сочетании с соблюдением правил — баланс между инициативностью и строгим следованием установленным правилам и регламентам.

2. Распределение характеристик по ролевым категориям (на основе NICE Workforce Framework)

Анализ KSAs (Knowledge, Skills, and Abilities), приведенных в NICE Workforce Framework, показывает, что для разных ролей принцип значимости отдельно взятых характеристик существенно отличается. В таблице 1 представлены профили для трех обширных категорий.

Таблица 1 – Приоритетные психофизические характеристики для различных ролей в области ИБ

Категория ролей (NICE)	Примеры ролей	Ключевые когнитивные характеристики	Ключевые личностные черты
Анализ и расследование (AN)	Threat/Warning Analyst, Cyber Defense Analyst	Аналитическое мышление, индуктивное/дедуктивное мышление, рабочая память, способность к построению гипотез	Открытость опыту (любопытность), настойчивость, бдительность
Эксплуатация и поддержка (OM)	System Administrator, Database Administrator	Внимание к деталям, процедурная память, способность к многозадачности	Добросовестность, дисциплинированность, методичность
Надзор и управление (OV)	Executive Cyber Leader, Program Manager	Стратегическое мышление, вербальный интеллект, способность оценивать риски	Эмоциональная стабильность, интернальный локус контроля, развитые коммуникативные навыки

3. Сопоставление с профессиональными стандартами Российской Федерации

Сравнительный анализ с профессиональными стандартами Российской Федерации [4] выявил высокую степень соответствия с описанными выше характеристиками, однако с некоторой спецификой. В отечественных документах больший акцент делается на нормативно-правовой компетентности и, косвенно, на качествах, связанных с добросовестностью и ответственностью, обусловленными требованиями законодательства о государственной тайне. Кроме того, требования ФСБ России [5] предполагают углубленную проверку биографических данных и психологическое тестирование, направленное на выявление склонности к негативному поведению.

Обсуждение

Полученная структура блока психофизических характеристик представляет собой совокупность требований, извлеченных из разных источников. Ее научная актуальность заключается в переходе от распространенных неоднозначных описаний к систематизированной модели, которая может быть в дальнейшем формализована в виде онтологии предметной области. Как отмечают Гаврилова Т.А. и Хорошевский В.Ф. [12], именно такая структура знаний является необходимым условием для построения эффективных баз знаний интеллектуальных систем.

Предложенный подход также позволяет решить проблему неоднозначной оценки: каждая характеристика должна быть проанализирована через психодиагностические методики (опросник 16PF Кеттелла, MMPI, тест структуры интеллекта Амтхауэра, корректурная проба Бурдона и др.), что обеспечит объективность и точность результатов. Важно подчеркнуть, что использование данных методик в составе системы ИИ должно строго соответствовать требованиям Федерального закона № 152-ФЗ «О персональных данных», особенно в части обработки специальных категорий персональных данных [17].

Ограничением настоящего исследования является его преимущественно теоретико-аналитический характер. Апробация предложенной модели требует проведения тщательных исследований, направленных на установление связи между выделенными характеристиками и объективными показателями успешности профессиональной деятельности (отсутствие инцидентов ИБ из-за ошибки специалиста, скорость и качество решения профессиональных задач).

Заключение

В результате проведенного исследования определено и структурировано содержание блока психофизических характеристик специалиста в области ИБ. Блок включает следующую структуру (когнитивные способности, личностные черты, психофизиологические показатели, мотивационно-ценностные ориентации), а также вариативную часть, распределенную по ролевым категориям в соответствии с международными и профессиональными стандартами Российской Федерации.

Практическая значимость полученных результатов состоит в возможности их использования в качестве основы для:

- разработки онтологической модели предметной области «Психофизический портрет специалиста по ИБ»;
- проектирования базы знаний интеллектуальной системы поддержки принятия кадровых решений;
- создания методических рекомендаций по профессиональному психологическому отбору и оценке персонала в сфере ИБ.

Дальнейшие исследования будут направлены на упорядочение модели на языке представления онтологий (OWL) и ее интеграцию с существующими таксономиями компетенций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Hadnagy C. Social Engineering: The Science of Human Hacking. 2nd ed. – Wiley, 2018. – 320 p.
2. Mitnick K.D., Simon W.L. The Art of Deception: Controlling the Human Element of Security. – Wiley, 2002. – 368 p.
3. NIST Special Publication 800-181 Rev. 1. Workforce Framework for Cybersecurity (NICE Framework). – National Institute of Standards and Technology, 2020.
4. Профессиональный стандарт «Специалист по информационной безопасности» (утв. приказом Минтруда России от 15.09.2016 № 522н).

5. Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений (утв. приказом ФСТЭК России от 11.04.2025 № 117).
6. Бодров В.А. Психология профессиональной пригодности: учеб. пособие для вузов. – М.: ПЕР СЭ, 2001. – 511 с.
7. Дружинин В.Н. Психология общих способностей: учебник для вузов. – 3-е изд. – М.: Юрайт, 2025. – 349 с.
8. Леонова А.Б. Психодиагностика функциональных состояний человека. – М.: Изд-во Моск. ун-та, 1984. – 200 с.
9. Человеческий фактор: в 6 т. Т. 1. Эргономика – комплексная научно-техническая дисциплина / под ред. Г. Салвенди. – М.: Мир, 1991. – 599 с.
10. Mitnick K.D., Vamosi R. The Art of Invisibility. – Little, Brown and Company, 2017. – 320 p.
11. Климов Е.А. Психология профессионального самоопределения: учеб. пособие. – 4-е изд. – М.: Академия, 2010. – 304 с.
12. Гаврилова Т.А., Хорошевский В.Ф. Базы знаний интеллектуальных систем. – СПб.: Питер, 2001. – 384 с.
13. Анастаси А., Урбина С. Психологическое тестирование. – 7-е изд. – СПб.: Питер, 2009. – 688 с.
14. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.
15. Gruber T.R. Toward principles for the design of ontologies used for knowledge sharing // International Journal of Human-Computer Studies. – 1995. – Vol. 43, № 5-6. – P. 907–928.
16. Рассел С., Норвиг П. Искусственный интеллект: современный подход. – 2-е изд. – М.: Вильямс, 2006. – 1408 с.
17. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 08.08.2024).

© А. В. Галлямова, В. А. Белов, 2026

Н. С. Демин¹✉, В. В. Селифанов¹

Оценка эффективности системы защиты значимого объекта критической информационной инфраструктуры на основе сравнительного анализа методик оценки

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: nikita.demin.1996@inbox.ru

Аннотация. В работе выполнено исследование подходов к оценке эффективности обеспечения информационной безопасности объектов критической информационной инфраструктуры Российской Федерации. Проведен сопоставительный анализ методики, утвержденной ФСТЭК России 11 ноября 2025 года, и положений ГОСТ Р 57580.2, регламентирующих процедуры оценки соответствия в области защиты информации. Установлено, что методика ФСТЭК носит преимущественно нормативно-контрольный характер и ориентирована на подтверждение соответствия минимально допустимому уровню защищенности, при этом характеризуется ограниченным набором оцениваемых показателей и недостаточной интеграцией с требованиями приказа ФСТЭК России № 239. В противоположность этому, из сферы финансового сектора взят ГОСТ Р 57580.2 реализующий развернутый процессный подход, включающий качественную оценку состояния и зрелости механизмов обеспечения безопасности. Обоснована необходимость модернизации методики ФСТЭК посредством расширения состава оцениваемых процессов и заимствования элементов качественной оценки.

Ключевые слова: критическая информационная инфраструктура, информационная безопасность, оценка эффективности, ФСТЭК России, ГОСТ Р 57580.2, зрелость процессов, методика оценки

N. S. Demin¹✉, V. V. Selifanov¹

Assessment of the Effectiveness of the Critical Information Infrastructure Protection System Based on Comparative Analysis of Assessment Methods

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: nikita.demin.1996@inbox.ru

Abstract. This paper examines approaches to assessing the effectiveness of information security at critical information infrastructure facilities in the Russian Federation. A comparative analysis is provided of the methodology approved by the Federal Service for Technical and Export Control (FSTEC) of Russia on November 11, 2025, and the provisions of GOST R 57580.2 which regulate compliance assessment procedures in the field of information security. It was established that the FSTEC methodology is primarily normative and control-oriented in nature and is focused on confirming compliance with the minimum permissible level of security. However, it is characterized by a limited set of assessed indicators and insufficient integration with the requirements of FSTEC Order No. 239. In contrast, GOST R 57580.2, adopted from the financial sector, implements a comprehensive process-based approach that includes a qualitative assessment of the state and maturity of security mechanisms. The need to modernize the FSTEC methodology by expanding the range of processes assessed and adopting elements of a qualitative assessment is substantiated.

Keywords: critical information infrastructure, information security, performance assessment, FSTEC of Russia, GOST R 57580.2, process maturity, assessment methodology

Введение

Когда говорят о критической информационной инфраструктуре (КИИ), обычно имеют в виду не просто набор информационных систем, а гораздо более сложную конструкцию – по сути, основу функционирования целых отраслей [1]. При этом важно понимать, что сбои в таких системах редко остаются локальными: чаще они «цепляют» связанные процессы и могут приводить к вполне ощутимым последствиям, в том числе экономическим.

Ситуация дополнительно усложняется тем, что в последние годы резко выросла степень цифровизации. Автоматизированные системы управления технологическими процессами (АСУ ТП) используются повсеместно, и зависимость от них уже трудно переоценить [2]. Даже кратковременные отклонения в их работе могут восприниматься как критические.

На этом фоне изменился и сам характер угроз. Если раньше атаки чаще носили массовый характер, то сейчас наблюдается другая тенденция: воздействия становятся более адресными. В ряде случаев злоумышленники заранее анализируют структуру объекта, его архитектуру, а иногда и организационные особенности [3]. Соответственно, требования к системе защиты тоже меняются.

Возникает вполне логичный вопрос – как оценить, насколько такая система действительно эффективна. Формальное наличие защитных механизмов уже не дает полной картины. Гораздо важнее понять, работают ли они в реальных условиях и способны ли противостоять актуальным угрозам [4].

В российской практике для этих целей используются разные подходы. Наиболее часто упоминаются методика ФСТЭК России (редакция 2025 года) [5] и стандарт ГОСТ Р 57580.2–2018 [6]. Дополнительно необходимо учитывать требования приказа ФСТЭК России № 239 [7], которые задают общий контур обеспечения безопасности КИИ. При этом сами методики, несмотря на схожую область применения, выстроены по разным принципам – и это важно учитывать.

Методика оценки эффективности ФСТЭК России

Если попробовать описать методику ФСТЭК России [5] «без формул», то она сводится к следующему: система защиты разбивается на отдельные элементы, и каждый из них оценивается через набор показателей.

Такие показатели отражают выполнение конкретных требований. Затем они группируются по направлениям, после чего формируется итоговая оценка защищенности $K_{зи}$. В расчетах учитываются весовые коэффициенты – это позволяет варьировать значимость отдельных направлений [7].

С одной стороны, все выглядит довольно логично. Есть четкая процедура, есть числовой результат, который можно интерпретировать. Для целей отчетности или контроля это, безусловно, удобно.

Источники данных тоже вполне понятны: результаты проверок, анализ документации, сведения о работе средств защиты [5, 8]. То есть формально оценка опирается на проверяемую информацию.

Но здесь возникает нюанс. Методика, по сути, фиксирует выполнение минимально установленных требований. Если требования выполнены – система считается защищенной. Насколько она устойчива к сложным сценариям атак – это уже не всегда очевидно [9].

Кроме того, не все процессы информационной безопасности получают достаточное внимание, наблюдается слабая интеграция с положениями приказа ФСТЭК России № 239. Например, управление уязвимостями или реагирование на инциденты учитываются, но скорее «по факту наличия», чем с точки зрения эффективности [7, 10]. На практике же именно эти процессы часто оказываются критичными.

Оценка соответствия по ГОСТ Р 57580.2

В ГОСТ Р 57580.2–2018 [6] логика построения оценки заметно отличается. Здесь система защиты рассматривается не как набор отдельных мер, а как совокупность процессов. Причем важно не только то, реализованы ли эти процессы, но и то, как именно они функционируют. Оценка проводится с учетом нескольких факторов: полноты внедрения, корректности выбора мер, согласованности процессов и устойчивости системы в целом [6, 11].

Отдельно вводится понятие зрелости процессов. Под ним понимается степень их формализации и управляемости, а также способность воспроизводиться в аналогичных условиях [12]. Это уже более «глубокий» уровень анализа. На практике это означает, что проверяется не только наличие регламентов, но и соответствие фактической деятельности этим регламентам, наличие механизмов контроля и, что немаловажно, способность системы адаптироваться к изменениям.

Такой подход дает более объемную картину. В ряде исследований отмечается, что именно процессная модель позволяет лучше выявлять реальные проблемы, а не только формальные несоответствия [13].

Сравнительный анализ методик

При сравнении двух подходов становится очевидно, что они решают разные задачи, хотя формально направлены на одно и то же. Методика ФСТЭК дает количественную оценку и позволяет быстро понять, выполнены ли требования [5]. Это ее сильная сторона. Но глубина анализа при этом ограничена. ГОСТ Р 57580.2, напротив, ориентирован на анализ процессов [6]. Здесь оценка менее «жесткая» в числовом смысле, зато позволяет увидеть, как система работает в целом.

Если упростить, различие можно сформулировать так: одна методика отвечает на вопрос «что сделано», другая – «как это работает». Различия проявляются и в деталях:

- уровень детализации анализа;

- учет изменений во времени;
- возможность выявления скрытых проблем;
- характер итоговой оценки.

При этом исследования показывают, что чисто количественные подходы не всегда отражают реальную устойчивость системы [14]. В то же время процессные модели лучше учитывают динамику и развитие системы защиты [15].

Направления совершенствования методики ФСТЭК России

С учетом выявленных особенностей представляется обоснованным развитие методики ФСТЭК России по следующим направлениям:

1. Расширение перечня оцениваемых процессов. Необходимо обеспечить включение в модель оценки процессов, регламентированных приказом № 239, что позволит повысить полноту анализа [7].
2. Введение градаций зрелости. Целесообразно дополнить количественную оценку качественными характеристиками, отражающими уровень развития процессов [6].
3. Интеграция качественных методов. Использование элементов процессного анализа позволит повысить аналитическую ценность результатов оценки.
4. Уточнение системы показателей. Расширение набора индикаторов должно быть направлено на учет организационных и управленческих аспектов обеспечения безопасности.
5. Формирование комбинированной модели. Перспективным представляется построение гибридной модели, сочетающей количественную формализацию и качественную интерпретацию результатов.

Заключение

Таким образом, говорить о том, что одна из методик «лучше», было бы не совсем корректно. Скорее, они дополняют друг друга.

Методика ФСТЭК удобна, когда требуется формализованная оценка – например, в рамках проверок. Она дает понятный результат, но не всегда позволяет глубоко проанализировать ситуацию.

ГОСТ Р 57580.2–2018 дает более развернутое представление о состоянии системы, поскольку учитывает процессы и их зрелость. Однако его применение требует более детального анализа.

На практике наиболее обоснованным выглядит комбинированный подход. Сочетание количественной оценки и процессного анализа позволяет получить более реалистичную картину и, соответственно, принимать более взвешенные решения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О безопасности критической информационной инфраструктуры Российской Федерации : федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ. – Текст : непосредственный.

2. ГОСТ Р ИСО/МЭК 27001–2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Введ. 2021–09–01. – Москва : Стандартинформ, 2021. – Текст : непосредственный.
3. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Управление рисками информационной безопасности. – Введ. 2011–01–01. – Москва : Стандартинформ, 2010. – Текст : непосредственный.
4. ISO/IEC 27004:2016. Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation. – Geneva : ISO, 2016. – Текст : непосредственный.
5. Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : утв. ФСТЭК России 11 нояб. 2025 г. – Текст : непосредственный.
6. ГОСТ Р 57580.2–2018. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Ч. 2. Методика оценки соответствия. – Введ. 2019–01–01. – Москва : Стандартинформ, 2018. – Текст : непосредственный.
7. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : приказ ФСТЭК России от 25 дек. 2017 г. № 239. – Текст : непосредственный.
8. Методические рекомендации по обеспечению информационной безопасности организаций банковской системы Российской Федерации / Банк России. – Москва, 2021. – Текст : непосредственный.
9. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В. Ф. Шаньгин. – Москва : ФОРУМ, 2020. – 416 с. – Текст : непосредственный.
10. Комаров, В. В. Оценка и мониторинг защищенности информационных ресурсов / В. В. Комаров, М. В. Буйневич // Информационные технологии и телекоммуникации. – 2023. – Т. 11, № 4. – С. 45–52. – Текст : непосредственный.
11. Анисимов, А. С. Оценка эффективности средств защиты информации / А. С. Анисимов, А. И. Козачок // Информационная безопасность. – 2021. – № 2. – С. 34–39. – Текст : непосредственный.
12. Кузнецов, В. М. Процессный подход к управлению информационной безопасностью / В. М. Кузнецов // Информационная безопасность. – 2020. – № 3. – С. 15–21. – Текст : непосредственный.
13. Полтавцева, М. А. Оценка защищенности систем обработки данных / М. А. Полтавцева, Д. П. Зегжда // Вопросы кибербезопасности. – 2025. – № 5. – С. 22–30. – Текст : непосредственный.
14. Голембиовский, М. М. Формализация оценки защищенности объектов КИИ / М. М. Голембиовский [и др.] // Информационная безопасность. – 2023. – № 4. – С. 27–33. – Текст : непосредственный.
15. Скрыль, С. В. Совершенствование процедур оценки защищенности КИИ / С. В. Скрыль [и др.] // Безопасность информационных технологий. – 2023. – № 2. – С. 41–48. – Текст : непосредственный.

© Н. С. Демин, В. В. Селифанов, 2026

К. А. Жуйков¹✉, А. В. Шабурова¹

Особенности синергии эффективных инструментов и подходов к управлению высокотехнологическими предприятиями

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: Zhuykov2002.16@gmail.com

Аннотация. В статье исследуется проблема интеграции двух фундаментальных инструментов управления жизненным циклом наукоемкой продукции, а именно системного анализа и управления рисками, в рамках синтеза инновационного и маркетингового подходов. Автор аргументирует, что автономное применение каждого из указанных инструментов генерирует противоположные по своей природе дефекты. Системный анализ, ориентированный на структурную рациональность, зачастую игнорирует поведенческие и конъюнктурно-рыночные факторы, тогда как управление рисками способствует чрезмерной консервации статус-кво и сдерживанию радикальных инноваций. В качестве решения предлагается концепция конвергенции данных инструментов посредством организации двунаправленного информационного обмена. Подобный синтез позволяет достичь синергетически-социального эффекта, проявляющегося на микроэкономическом, организационном и макросоциальном уровнях управления.

Ключевые слова: наукоемкая продукция, жизненный цикл продукции, системный анализ, управление рисками, инновационный подход, маркетинговый подход, синергический эффект

K. A. Zhuykov¹✉, A. V. Shaburova¹

Features of the Synergy of Effective Tools and Approaches to Managing High-Tech Enterprises

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: Zhuykov2002.16@gmail.com

Abstract. The article examines the problem of integrating two fundamental tools for managing the life cycle of high-tech products, namely system analysis and risk management, within the framework of synthesizing innovative and marketing approaches. The author argues that the autonomous application of each of these tools generates defects that are opposite in nature. System analysis, focused on structural rationality, often ignores behavioral and market-conjunctural factors, while risk management contributes to excessive conservation of the status quo and the suppression of radical innovations. As a solution, the concept of convergence of these tools is proposed through the organization of bidirectional information exchange. Such a synthesis makes it possible to achieve a synergistic-social effect that manifests itself at the microeconomic, organizational, and macrosocial levels of management.

Keywords: science-intensive products, product life cycle, system analysis, risk management, innovative approach, marketing approach, and synergistic effect

Введение

Высокотехнологичные отрасли экономики функционируют и базируются в граничных условиях ускоряющегося технологического прогресса, сокращения инновационных циклов и возрастающей сложности наукоемкой продукции.

Управление жизненным циклом продукции (ЖЦП) на предприятиях перестало быть линейным процессом и требует синергии разнородных инструментов: от маркетингового планирования до экологической оценки и цифрового мониторинга. Традиционные модели, ориентированные на отдельные аспекты – рыночную динамику, научно-технические разработки или устойчивое развитие, – в изолированном виде уже не обеспечивают необходимой эффективности. В связи с этим ключевой научно-практической проблемой становится поиск эффективной синергии подходов к управлению жизненного цикла продукции, способной отображать как экономические, так и технологические, экологические и социальные пользы.

Концепция жизненного цикла продукции прошла длительное становление. Как показано в материалах научного исследования, зарождение идеи относится к 1950-м годам, когда модель «внедрение – рост – зрелость – спад» легла в основополагающую суть стратегического маркетинга и планирования производства. В 1970-е годы подход формализуется в научных исследованиях: появляются количественные и качественные методики оценки, модели детализируются и начинают применяться для управления ассортиментом и инвестиционного капитала. В 1990-е годы модели жизненного цикла обогащаются аспектами управления качеством и инновациями, акцент направлен на адаптацию к рыночным изменениям и ускорение вывода новых высокотехнологических продуктов. С 2000-х годов под влиянием цифровизации 4.0 и принципов устойчивого развития в модели интегрируются эко-дизайн, социальная ответственность и сквозные цифровые технологии, что значительно расширяет границы применимости концепции.

Длительное время подходы развивались последовательно-параллельно, принадлежа разным функциональным областям: маркетингу, экологическому менеджменту, сервисному обслуживанию. Однако усовершенствование высокотехнологичной продукции, рост значимости «длинных» жизненных циклов (например, в авиастроении, медицинском оборудовании, программно-аппаратных комплексах) и необходимость одновременного обеспечения коммерциализации, инновационной динамики и устойчивости требуют перехода от разрозненного применения инструментов к их синергическому эффекту.

Таким образом, традиционные системы управления ЖЦП, основанные на доминировании одного из подходов, оказываются недостаточно гибкими и многофункциональными решениями. Возникает необходимость в формировании интегративной модели, позволяющей сочетать маркетинговую аналитику, инновационную творчество, экологическую оценку и сервисную поддержку в едином контуре управления, что в результате даст синергический эффект. Эффективность такого синтеза определяется не простым суммированием инструментов, а глубиной их синергии – взаимодополняющим использованием, создающим новые конкурентоспособные преимущества.

Целью настоящей статьи является выявление особенностей синергии эффективных инструментов и подходов к управлению высокотехнологическими предприятиями на основе анализа моделей ЖЦП и обоснование направлений их интеграции и комбинации. В работе рассматриваются теоретические предпосылки

объединения подходов для формирования синергической системы управления жизненным циклом, отвечающей современным специфике цифровой и устойчивой экономики в граничных условиях региона и отрасли.

Методы и материалы исследования

Методологическую базу статьи составили общенаучные методы анализа и синтеза, индукции и дедукции. Также в работе использовался системно-процессный подходы к анализу, а также объектно-субъектный метод, применяемый при построении систем управления жизненным циклом продукции.

Результаты и обсуждения

В процессе исследования установлено, что высокотехнологичные организации обладают рядом отличительных характеристик, которые фокусируют специфику управления ими. Высокотехнологичные предприятия характеризуются высокой наукоемкостью продукции и процессов, значительными инвестициями, сложными научно-технологическими процессами и продуктами, и необходимостью управления интеллектуальной собственностью. Так же стоит отметить динамичность внешней среды высокотехнологичных предприятий, короткие ЖЦП и технологий, быстрое изменение потребностей рынка, высокая интенсивность конкуренции и появления инноваций [6,7].

Синергия формируется в результате системного эффекта, при котором интегральный результат кооперативного взаимодействия компонентов сложной системы превышает сумму автономных результатов каждого из них, взятых в отдельности, что выражается в появлении новых положительных свойств, недостижимых при изолированном функционировании элементов [1].

Синергетический эффект достигается за счет формирования сквозных цифровых каналов связи между последовательными этапами ЖЦП, устраняющих информационные разрывы [5]. С помощью синергического подхода происходит согласование конструкторских, технологических и метрологических служб для повышения скорости обработки и принятия решения в управлении ЖЦП [4].

Эффективное управление ЖЦП требует комплексного подхода, ориентированного на интеграцию инновационных, производственных и управленческих процессов на всех этапах ЖЦ.

В условиях высокой технологической сложности и быстрого устаревания продуктов инструменты управления направлены на оптимизацию ресурсов, минимизацию рисков и повышение конкурентоспособности. Ключевые вызовы включают координацию научно-исследовательских и опытно-конструкторских работ (НИОКР), контроль качества и адаптацию к рыночным изменениям, что делает актуальными методы проектного управления, анализа затрат и цифровых технологий [9].

В контексте наукоемких отраслей продукция представляет собой результат трансформации междисциплинарных знаний в инновационное творчество. Ее управление сопряжено с преодолением фундаментальных противоречий между

необходимостью длительной научной валидации и динамичностью рынка, а также между стандартизацией и адаптацией к региональной специфике.

Процесс разработки концепции жизненного цикла является творческой работой, которая ограничена по времени и ресурсам, направлена на достижение конкретной инновационной цели и задачи. Следовательно, ядром управления на стадиях концепции, НИОКР и вывода на рынок выступают методологии проектного управления. Однако их выбор и адаптация носят критически важный характер [4].

Инновационный подход, лежит в основе современной разработки наукоемких продуктов и услуг, базируется на применении гибридной модели, которая интегрирует передовые технологические решения и человеко-ориентированные методологии.

Результатом внедрения инновационного подхода становится существенное улучшение ключевых бизнес-показателей: время вывода продукта на рынок сокращается на 25 – 40 %, а удовлетворенность пользователей растет на 25 %. Проработка этапов жизненного цикла помогает минимизировать ошибки на ранних стадиях разработки, более точного попадания в потребности аудитории и повышения доверия к бренду благодаря технологическим гарантиям безопасности.

Маркетинговый подход является дополнительным звеном инновационного подхода, строящийся на концепции персонализированного взаимодействия в реальном времени и охватывает несколько взаимосвязанных направлений. Подход реализует сегментацию на основе Big Data позволяет не просто делить аудиторию по стандартным демографическим и политическим признакам, а анализировать поведенческие бизнес-модели и создавать макросегменты – группы пользователей с очень схожими моделями поведения и потребностями [2].

Взаимодействие инновационного и маркетингового подходов реализуется через механизм непрерывной обратной связи в рамках ЖЦ наукоемкой продукции и проявляется на всех его стадиях. На ранних этапах исследования и разработки данные маркетинговых исследований формируют техническое задание для инновационных решений. Одновременно предиктивная аналитика выявляет неочевидные рыночные ниши, где передовые технологии могут дать максимальный социальный и экономический эффект. На стадии внедрения обеспечивается техническая безопасность наукоемкого продукта, но и становятся уникальным торговым предложением (УТП) в маркетинговых коммуникациях: подтверждение подлинности товара, прозрачность цепочки поставок или защита интеллектуальной собственности превращаются в аргументы для привлечения клиентов [5].

На стадии роста персонализация маркетинга ускоряет проникновение на рынок: целевые предложения, основанные на анализе поведения, повышают конверсию и снижают стоимость привлечения клиента.

Предиктивная аналитика прогнозирует и анализирует момент, когда продукт начнет терять актуальность, и подсказывает оптимальные сроки для радикального обновления и говорит о шаге спада или его обновлении.

Разработка высокотехнологичной продукцией выявляет неустойчивые закономерности: нарастание инновационной среды, что сопровождается наукоемкост-

ным ростом числа неконтролируемых переменных как в технической области, так и в сфере рыночного восприятия.

Одним из инструментов управления ЖЦП является системный анализ. Он построен на основе иерархических моделей взаимосвязей между подсистемами, компонентами и процессами. Инновационное содержание этого инструмента заключается в его способности на стадии концептуального проектирования генерировать альтернативные архитектурные конфигурации, выявлять точки бифуркации, где незначительное изменение одного параметра приводит к каскадным последствиям для ремонтпригодности, логистической поддержки и финальной утилизации [1]. Системный анализ позволяет формировать творческую составляющую разработки, но и выводит дисциплину целостного видения, препятствуя локальным оптимизациям, которые повышают сложность без адекватного приращения функциональной ценности [10].

Второй инструментарий, который рассматривается в работе – управление рисками. Инструмент предлагает интерпретации выходит за рамки традиционного инженерного анализа видов и последствий отказов. Его маркетинговое измерение раскрывается через постоянное отслеживание и унификацию вероятностных событий - рисков, способных исказить ЖЦ наукоемкой продукции [3].

Риск-менеджмент, интегрированный в контур управления жизненным циклом, позволяет ранжировать угрозы не только по научно-техническим, но и по рыночным критериям, вводя такие показатели, как «вероятность преждевременного выхода с рынка» или «эластичность спроса по риску сбоя».

Переход от раздельного применения к интеграции двух инструментов предполагает не механическое сложение, а создание встречных информационных потоков. Системный анализ передает в контур риск-менеджмента формализованные описания критических компонентов, деградация или отказ которых способны запустить цепочку нежелательных последствий. В результате системный анализ перестает быть самостоятельной теоретической конструкцией, а риск-менеджмент взаимосвязан с ним (рис. 1).

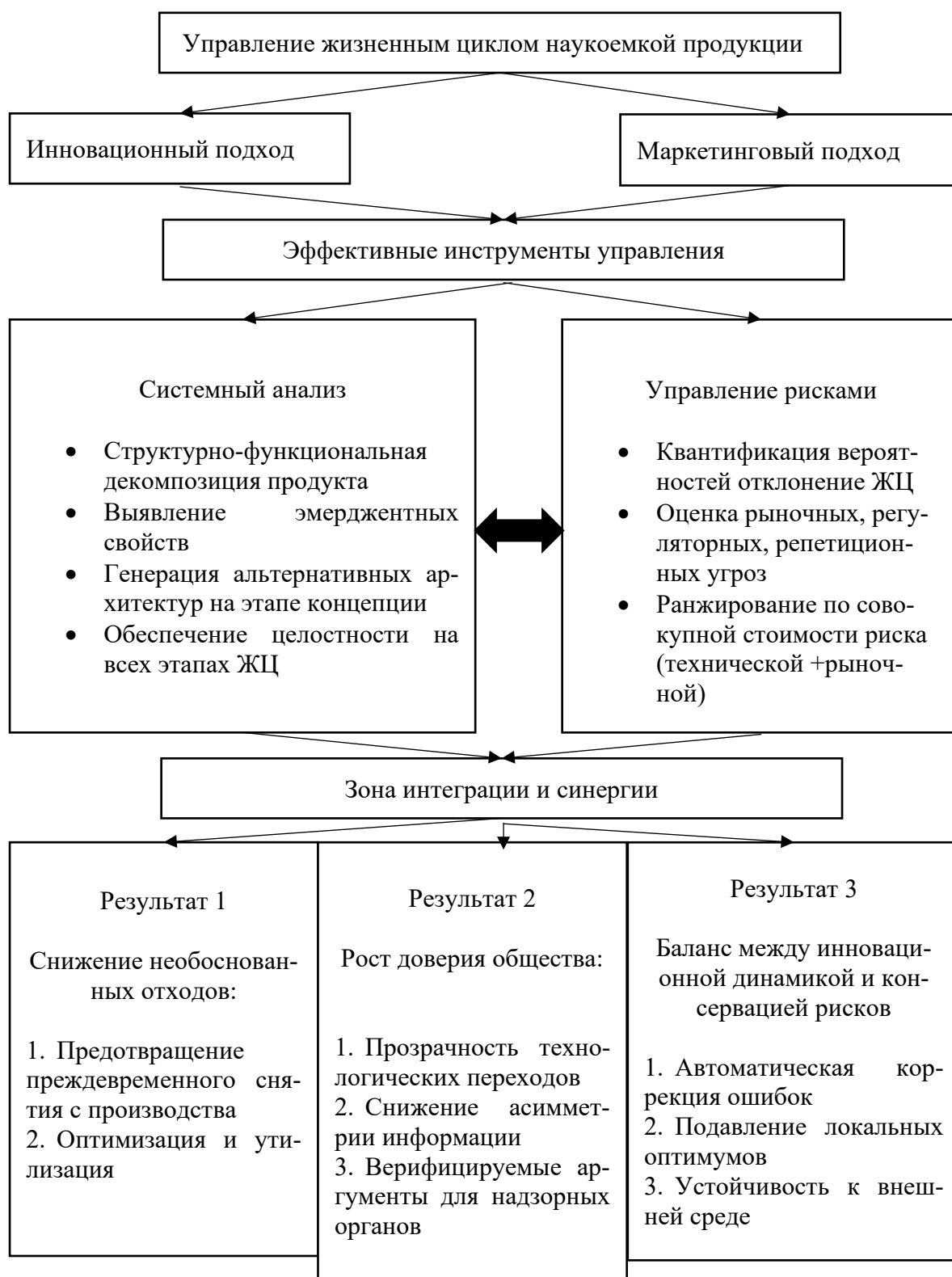


Рис. 1 Синергетический эффект с использованием инструментов управления жизненным циклом

Синергически-социальный эффект от такой конвергенции разворачивается на трех уровнях. На микроэкономическом уровне достигается сокращение не-

оправданных затрат на избыточное резервирование (системный анализ помогает отличить действительно критические риски от мнимых) и одновременно предотвращаются провалы, вызванные игнорированием человеческого фактора. На организационном уровне внутри компании формируется унифицированный понятийный аппарат, где инженеры и маркетологи начинают оперировать общими категориями «критичности узла», «вероятности отклонения» и «цены восстановления», что разрушает межведомственные барьеры и ускоряет внесение изменений в конструкторскую документацию под влиянием рыночных сигналов.

Таким образом, объединение системного анализа и управления рисками порождает не просто аддитивный, а именно синергетический результат, в котором целостность технического решения и чувствительность к рыночным неопределенностям взаимно усиливают друг друга [4]. Социальная размерность этого эффекта возникает из факта легитимации инноваций через прозрачную, воспроизводимую процедуру учета рисков, что для наукоемкой продукции с высокими ставками для общества является не факультативным требованием, а необходимым условием долгосрочного воспроизводства технологического суверенитета [7].

Такая интеграция превращает традиционную линейную модель ЖЦП в адаптивную, самообучающуюся систему. Это особенно важно для российских высокотехнологичных предприятий в условиях ускоренной цифровой трансформации, импортозамещения и необходимости обеспечения долгосрочной конкурентоспособности.

Заключение

Проведенное исследование показало, что эффективное управление высокотехнологическими предприятиями в современных условиях возможно только через синергию разнородных инструментов и подходов. Традиционные модели управления ЖЦП устарели; ключевым фактором конкурентоспособности становится глубина интеграции системного анализа и управление рисками становятся важным аспектом в граничных условиях региона и отрасли

Предложенная синергическая модель позволяет высокотехнологичным предприятиям одновременно сокращать время вывода продукции на рынок, минимизировать риски, повышать качество и обеспечивать устойчивость.

Практическая значимость работы заключается в том, что предложенная интегративная модель применима для высокотехнологичных предприятий авиастроения, медицинского приборостроения, энергетического машиностроения и других наукоемких отраслей, где цена ошибочного управленческого решения особенно высока.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бережнов Г. В. Методология управления по компетенциям как современный подход к управлению персоналом организации / Г. В. Бережнов, Ф. А. Ширяева // Экономические системы. – 2024. – Т. 17, № 4. – С. 135-145. – URL: <https://cyberleninka.ru/article/n/metodologiya->

upravleniya-po-kompetentsiyam-kak-sovremennyy-podhod-k-upravleniyu-personalom-organizatsii (дата обращения: 15.05.2026).

2. Бородулин А. И. Управление персоналом современных организаций // Вестник современных исследований. – 2024. – № 5. – С. 45-52. – URL: <https://cyberleninka.ru/article/n/upravlenie-personalom-sovremennyh-organizatsiy> (дата обращения: 15.05.2026).

3. Ажаханова Д. С. Современные подходы к стратегическому управлению // Вестник науки и образования. – 2013. – № 12. – С. 67-72. – URL: <https://cyberleninka.ru/article/n/sovremennye-podhody-k-strategicheskomu-upravleniyu> (дата обращения: 15.05.2026).

4. Игнатьева Т. С. Актуальные подходы к управлению современной организации / Т. С. Игнатьева, Е. В. Разумова // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2024. – № 2(165). – С. 18-22. – URL: <https://cyberleninka.ru/article/n/sovremennye-podhody-k-upravleniyu-vysokotekhnologichnymi-organizatsiyami> (дата обращения: 15.05.2026).

5. Грачева К. А. Роль цифровой трансформации в управлении предприятиями: анализ цифровых кейсов // Экономика и управление. – 2023. – № 4. – С. 112-120. – URL: <https://cyberleninka.ru/article/n/rol-tsifrovoy-transformatsii-v-upravlenii-predpriyatiyami-analiz-tsifrovyyh-keysov> (дата обращения: 15.05.2026).

6. Мелехов К. А. Проблемы повышения эффективности управления высокотехнологичными организациями в современных условиях // Вестник МИРБИС. – 2023. – № 3(35). – С. 66-74. – URL: <https://cyberleninka.ru/article/n/sovremennye-podhody-k-upravleniyu-vysokotekhnologichnymi-organizatsiyami> (дата обращения: 15.05.2026).

7. Крапивин И. О. Современные тенденции развития методологии стратегического планирования на предприятиях высокотехнологичных отраслей промышленности // Вестник науки и образования. – 2023. – № 10. – С. 112-118. – URL: <https://cyberleninka.ru/article/n/sovremennye-tendentsii-razvitiya-metodologii-strategicheskogo-planirovaniya-na-predpriyatiyah-vysokotekhnologichnyh-otrasley> (дата обращения: 15.05.2026).

8. Климовских Н. В. Инновационные подходы в управлении персоналом современной организации // Вестник университета. – 2018. – № 5. – С. 89-95. – URL: <https://cyberleninka.ru/article/n/innovatsionnye-podhody-v-upravlenii-personalom-sovremennoy-organizatsii> (дата обращения: 15.05.2026).

9. Ахмадуллин А. Р. Применение методов сокращения времени цикла производства Just-in-Time, Kanban при производстве металлочерепицы // Студенческий вестник. – 2023. – № 12. – С. 78-85. – URL: <https://cyberleninka.ru/article/n/primenenie-metodov-sokrascheniya-vremeni-tsikla-proizvodstva-just-in-time-kanban-pri-proizvodstve-metallocherepitsy> (дата обращения: 15.05.2026).

10. Чупина Ж. С. Основные подходы к созданию интеллектуальной системы управления высокотехнологичными проектами в современных экономических условиях развития Российской Федерации // Финансовый менеджмент. – 2024. – № 9. – С. 338-347. – URL: <https://cyberleninka.ru/article/n/instrumenty-intellektualnoy-sistemy-integrativnogo-upravleniya-innovatsionnymi-proektami> (дата обращения: 15.05.2026).

© К. А. Жуиков, А. В. Шабурова, 2026

В. А. Захаров^{1✉}, А. В. Троеглазова¹

Сравнительный анализ нормативных подходов и практик управления киберрисками в кредитно-финансовых организациях

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: vzakharov60@yandex.ru

Аннотация. В работе анализируются актуальные проблемы информационной безопасности финансового сектора, который испытывает нарастающее давление изоощренных кибератак. Отмечается, что рост числа инцидентов, уязвимостей и финансовых потерь, наряду с существенными затратами на внедрение рекомендованных стандартов (ГОСТ Р 57580.3-2022, ГОСТ Р 57580.4-2022), фактически сводит их применение к рекомендательному уровню. Особое внимание уделяется дефициту методик для оценки рисков, связанных с операциями без добровольного согласия, недостатками традиционных подходов к оценке рисков информационной безопасности в условиях динамично меняющегося ландшафта киберугроз. Подчеркивается возрастающая роль математического моделирования. Для повышения киберустойчивости финансовых организаций и эффективного управления рисками дальнейшая работа должна быть направлена на создание специализированных методик, развитие количественных подходов к оценке киберрисков и стимулирование интеграции систем управления ими в общую структуру риск-менеджмента.

Ключевые слова: кибер-риски, анализ рисков, управление рисками, операционная надежность, киберустойчивость, операция без добровольного согласия

V. A. Zakharov^{1✉}, A. V. Troeglazova¹

Comparative Analysis of Regulatory Approaches and Practices for Managing Cyber Risks in Credit and Financial Organizations

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: vzakharov60@yandex.ru

Abstract. The paper analyzes the current problems of information security in the financial sector, which is experiencing increasing pressure of sophisticated cyberattacks. It is noted that the growing number of incidents, vulnerabilities, and financial losses, along with the significant costs of implementing the recommended standards (GOST R 57580.3-2022, GOST R 57580.4-2022), effectively reduces their implementation to a recommended level. Special attention is paid to the lack of methods for assessing risks associated with operations without voluntary consent, and the shortcomings of traditional approaches to assessing information security risks in a dynamically changing cyberthreat landscape. The increasing role of mathematical modeling is emphasized. To enhance the cyber resilience of financial institutions and effectively manage risks, further efforts should focus on developing specialized methodologies, promoting quantitative approaches to cyber risk assessment, and encouraging the integration of cyber risk management systems into the overall risk management framework.

Keywords: cyber risks, risk analysis, risk management, operational reliability, cyber resilience, non-consensual operations

Введение

Современный финансовый рынок функционирует в условиях постоянного давления со стороны киберпреступности. Статистика последних пяти лет демонстрирует устойчивую тенденцию к увеличению интенсивности и сложности кибератак на финансовые организации. Несмотря на усиление мер защиты, в 2025 году количество целевых атак останется на критически высоком уровне, что свидетельствует об адаптации злоумышленников к современным системам безопасности.

Анализ данных за 2025 год по сравнению с 2024 годом выявил следующие количественные показатели:

1) Зафиксирован 20 % рост уязвимостей ПО в кредитно-финансовых организациях (рис. 1) [1];

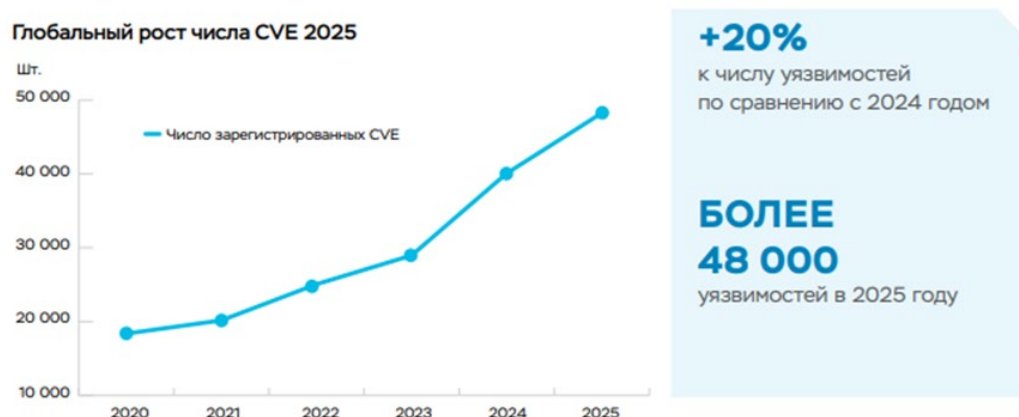


Рис. 1. Динамика зарегистрированных уязвимостей в 2025 году в организациях кредитно-финансовой сфере

2) Фиксируется рост инцидентов операционной надежности, связанных с невозможностью оказывать банковские и финансовые услуги, на 58 % по сравнению с 2024 годом (рис. 2) [1];

3) Объем похищенных денежных средств злоумышленниками у клиентов кредитных организаций вырос на 6,4 % (до 29,3 млрд руб.) [1].

Построение действенной системы обеспечения информационной безопасности в условиях ограниченных ресурсов, времени, а также с учетом ценности активов, их уязвимостей и потенциальных угроз, является критически важным. Выбор адекватных мер защиты для достижения необходимого уровня безопасности должен базироваться на результатах анализа рисков информационной безопасности. Эти результаты служат отправной точкой для внедрения и поддержания эффективного управления информационной безопасностью, а также играют ключевую роль при формировании политики безопасности и создании системы управления рисками. Снижение вероятности киберугроз требует от организаций способности к развитию своей деятельности, что обеспечивается готовностью противодействовать им, возможностью оперативного реагирования и наличием средств для восстановления после атак, то есть киберустойчивостью [3].



Рис. 2. Статистика инцидентов операционной надежности и их динамика 2024-2025 годы

Киберриски в финансовой сфере включают в себя прямые финансовые потери клиентов, подрывающие доверие к современным технологиям; нарушение операционной надежности, приводящее к репутационным ущербам и социальной напряженности; и, как следствие, возможность системного кризиса при возникновении серьезных инцидентов в значимых финансовых организациях.

Управление этими рисками предполагает наличие процедур для оценки, контроля и управления ими на уровне, соответствующем масштабам деятельности организации. Этот процесс включает:

- идентификацию активов, рисков, угроз и уязвимостей;
- анализ рисков путем оценки активов, последствий, вероятности угроз и степени уязвимостей;
- оценку уровня рисков для их последующего ранжирования.

Проведенный анализ литературных источников показал, что вопросы управления рисками информационной безопасности в кредитно-финансовой сфере широко представлены в публикациях: О.В. Бойченко [2, 3], А.А. Гуковской [4], Н.В. Щербаковой [5], М.А. Масловой [6], М.А. Польченко [7], Е.А. Беляева [8,9], М.Р. Белалова [10], Д.С. Кошкина [11], Н.В. Долбни [12] и других.

В контексте современной финансовой сферы представлен широкий спектр методик, стандартов, различных положений, разработанных для управления киберрисками. Примечательно, что, несмотря на наличие этих разнообразных подходов и накопленный опыт, наблюдается неуклонный рост самих киберугроз, что продолжает ставить перед организациями финансовой сферы сложные задачи по совершенствованию существующих моделей управления рисками информационной безопасности с учетом возникновения новых угроз.

В связи с этим целью настоящей работы является проведение сравнительного анализа нормативной базы, требований регуляторов в области защиты информации и сложившейся практики управления рисками информационной безопасности в кредитно-финансовых организациях. В рамках исследования будут рассмотрены преимущества и ограничения применяемых подходов в условиях

новых угроз, а также особенности их практической реализации, влияющие на возможности организаций по совершенствованию моделей управления рисками.

Анализ текущих подходов к управлению рисками развивает понимание киберрисков и проблем, указывая на потребность в совершенствовании существующих методов и практик управления киберрисками.

Материалы и методы исследования

Исследование опирается на системный подход к анализу нормативно-правового обеспечения информационной безопасности в финансовой сфере РФ (изучены и сопоставлены ключевые документы Банка России, ГОСТы). Использовались методы сравнительного анализа стандартов, регуляторных актов и практики управления рисками, экспертные оценки, а также изучение научной литературы, включая концепции цифровой экономики и системных рисков.

Результаты

При рассмотрении способов снижения вероятности возникновения киберугроз важным фактором является способность организации обеспечить развитие деятельности (устойчивость предприятия) за счет готовности противодействия к кибер-угрозам, возможности реагирования на них, средств восстановления после кибератак, называемая киберустойчивостью [2].

К важнейшим составляющим киберрисков в финансово-кредитной сфере можно отнести:

- прямые финансовые потери;
- нарушение операционной надежности и непрерывности предоставления финансовых услуг;
- развитие системного кризиса в случае возникновения инцидентов информационной безопасности [4].

Система управления рисками нарушения информационной безопасности предполагает установление процедур, обеспечивающих оценку, контроль и управление риском на том уровне, который соответствует масштабам деятельности банка и включает следующие этапы:

- 1) Идентификация риска: идентификация активов, рисков, значимых угроз, уязвимостей, существующих контролей;
- 2) Анализ рисков: оценка активов с учетом последствий от нарушения их свойств, вероятности реализации угроз и величины уязвимостей;
- 3) Оценка уровня рисков: оценка рисков заключается в определении количественных и качественных значений уровня риска, в формировании реестра рисков и их ранжировании [5, 7].

Оценка рисков начинается с определения ценных ИТ-активов, а сами риски возникают при реализации угроз через уязвимости, что требует анализа частоты событий, вероятности ущерба и его величины. Актуальность такого анализа обусловлена необходимостью защиты конфиденциальной информации, репутации и безопасности пользователей, поскольку угрозы, исходящие от их источников, могут привести к утрате свойств информационной безопасности активов [7].

В отличие от других сфер деятельности, организации кредитно-финансовой сферы находятся в зоне более сложного регулирования. Банк России разработал

Положение от 08.04.2020 года №716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» [13], в котором особое внимание уделено управлению риском информационной безопасности и риском информационных систем. Положение определило необходимость в проведении различных оценок по информационной безопасности, использования новых стандартизированных подходов к оценке операционных рисков для расчета достаточности капиталов, требование к ведению баз данных о событии операционного риска, в том числе риска информационной безопасности [8, 9].

Процедура исследования данной работы строилась на поэтапном сравнительном анализе указанных методик с целью выявления их применимости, сильных и слабых сторон в условиях цифровизации финансовой сферы. В рамках работы был проведен анализ следующих документов и стандартов (табл. 1).

Таблица 1 – Сравнительный анализ методик, стандартов и нормативных документов по управлению рисками

Метод/ Краткое описание	Положительные стороны	Отрицательные стороны	Применимость
ГОСТ Р 71034-2023 «Менеджмент риска. Риск-аппетит и ключевые индикаторы риска». Описание концепции риск-аппетита и подходов к определению/использованию ключевых индикаторов риска	Универсален. Позволяет показать прямую взаимосвязь рисков и бизнес-целей. Может использовать существующие показатели. Способствует своевременному воздействию на риск. Позволяет анализировать показатели во времени. Определяет лимиты рисков. Использует качественные и количественные метрики	Может быть избыточным и труднореализуемым для малых организаций. Описывает общие подходы, не учитывает специфику отрасли	Универсальный (любая организация)
РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности». Методика оценки рисков нарушения ИБ на основе качественных оценок степени возможности реализации угроз (СВР) и степени тяжести последствий (СТП)	Распространенность в организациях банковской сферы РФ. Позволяет оценивать риски в количественной (денежной) форме. Описаны защитные меры. Рекомендован для построения / совершенствования системы ИБ	Основана на экспертной оценке (зависимость от квалификации, субъективность). Привлечение внешних экспертов влечет финансовые расходы. Не отражает все современные векторы атак (документ 2009 года). Содержит устаревшие нормативные ссылки (СТО БР ИББС-1.0-2010 утратил силу)	Банковская сфера РФ

Окончание табл. 1

Метод/ Краткое описание	Положительные стороны	Отрицательные стороны	Применимость
ГОСТ Р ИСО/МЭК 27005-2010 «Информационные технологии. Методы и средства обеспечения безопасности. Управление рисками информационной безопасности». Стандарт, предлагающий детальный структурированный подход к управлению рисками ИБ на протяжении всего жизненного цикла	Детальный, структурированный подход. Адаптивность. Основа для построения надежной системы. Применим к организациям всех типов. Описывает весь жизненный цикл управления рискам	Требует глубокого понимания теории и практики. Может быть объемным и ресурсоемким. Требует значительных ресурсов экспертизы.	Любые типы организаций
ГОСТ Р 58771-2019 «Менеджмент риска. Технологии оценки риска». Руководство по выбору и применению технологий оценки риска; общий подход к оценке вероятности и последствий	Руководство по выбору технологий оценки риска. Общий подход к оценке вероятности и последствий. Полезен при принятии решений в условиях неопределенности. Устанавливает единый набор терминов Применим во всех сферах, где осуществляется управление рисками	Отсутствие описания процессов или практических инструкций. Не учитывает специфику отраслей	Универсальный (любая сфера)
Положения Банка России (№ 716-П, № 850-П и др.) и ФЗ № 161-ФЗ	Устанавливают обязательные нормативные требования. Охватывают ключевые области: операционный риск, надежность, защиту информации, платежные системы, противодействие переводам без согласия клиента	Фокус на регуляторных требованиях, может не охватывать все лучшие практики или новые угрозы. Специфичны для российского финансового сектора	Финансовый сектор РФ

Однако, несмотря на обилие исследований и наличие нормативно-правовой базы, практическое внедрение эффективных систем управления рисками информационной безопасности в финансовой сфере сталкивается с рядом нерешенных проблем.

Единственным документом, который определяет порядок оценки рисков информационной безопасности организаций кредитно-финансовой сферы, являются рекомендации в области стандартизации Банка России РС БР ИББС-2-2.2-2009 [14]. Методика разработана в 2009 году и в последующем не актуализировалась. Документ не содержит определенный перечень рассматриваемых угроз информационной безопасности, аналогичный банку данных угроз ФСТЭК [8].

В феврале 2023 года вступили в силу ГОСТ Р 57580.3-2022 «Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» [15] и ГОСТ Р 57580.4-2022 «Обеспечение операционной надежности. Базовый состав организационных и технических мер» [16]. Данные стандарты рекомендованы Банком России для управления рисками и обеспечения операционной надежности и призваны повысить устойчивость к кибератакам, а также улучшить качество обслуживания клиентов. Данные документы содержат положения политики управления рисками информационной безопасности, меры по их выявлению, оценке и мониторингу. В них описаны стратегии снижения рисков, планы реагирования на киберинциденты и восстановления после них, правила взаимодействия с поставщиками ИТ-услуг и проведения киберучений.

Настоящие стандарты применяются путем включения нормативных ссылок на них в нормативных актах Банка России и (или) прямого использования устанавливаемых в них требований во внутренних документах финансовых организаций, а также договорах [14,15]. В марте 2024 года Банк России утвердил методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности № 7-МР [17], которые предусматривают обеспечение реализации уровней защиты, определенных пунктом 6.8. раздела 6 ГОСТ Р 57580.3-2022. Таким образом, кредитным организациям рекомендуется осуществить внедрение данных ГОСТов до конца 2025 и 2026 годов в зависимости от значимости кредитной организации. Но до настоящего времени нет нормативных актов Банка России, содержащих ссылки на данные ГОСТы и официального документа, который бы регламентировал порядок и критерии оценки соответствия требованиям этих стандартов.

Необходимо отметить также, что стандартом Банка России СТО БР БФБО-1.7-2023. Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств [18] событием риска реализации информационных угроз является операция без добровольного согласия, которая стала возможной в результате реализации атак социальной инженерии, либо в результате успешной реализации компьютерной атаки на информационную инфраструктуру клиента.

С точки зрения события операционного риска реализации угроз информационной безопасности, обусловленного с нарушением операционной надежности, основным критерием для классификации является превышение допустимой доли деградации технологического процесса, связанного с предоставлением банковских услуг. При этом событием риска является исключительно реализация информационных угроз в виде компьютерного инцидента. В настоящее время отсутствуют специализированные методики оценки рисков, связанных с операциями без добровольного согласия.

Обсуждение

Результаты исследования подтверждают эскалацию угроз кибербезопасности в финансовом секторе, что выражается в неуклонном росте как количества

кибератак, так и финансового ущерба от них. Рассматриваемые в работе актуальные проблемы в области оценки киберрисков подчеркивают необходимость совершенствования подходов к управлению рисками информационной безопасности в кредитно-финансовых организациях. Среди них можно выделить следующие ключевые аспекты.

1) Субъективность экспертных оценок и отсутствие прогнозирования угроз являются ключевыми методологическими недостатками в оценке рисков информационной безопасности. Милославская Н.Г. справедливо подчеркивает, что эти недостатки указывают на острую необходимость применения математического моделирования для более точной оценки таких рисков [20].

2) По мнению О.В. Бойченко и М.А. Масловой основой построения эффективной системы обеспечения информационной безопасности, особенно при ограниченных ресурсах (кадровых, финансовых), является грамотный анализ рисков. Их подход предполагает интеграцию как количественных методов (оценка последствий в числовом выражении), так и качественных (балльные шкалы для определения уровня риска и мер по его снижению). Такой комплексный подход, по их мнению, позволяет выбрать действительно оптимальные меры защиты информации [3, 6].

3) Исследования М.Р. Белалова, Д.С. Кошкина и Н.В. Долбени свидетельствуют о недостаточной проработке существующей методологической базы для количественной оценки киберрисков. Авторы указывают на нехватку стандартов в этой области, что, по их мнению, может привести к принятию ошибочных решений при выборе мер защиты [10–12].

4) Вопрос универсальности существующих методик оценки рисков информационной безопасности, исследовался в работах Е.А. Беляева, в которых он приходит к мнению, что не всегда они могут служить универсальным эталоном для всех сфер производственной деятельности [8].

Заключение

Настоящее исследование выявило ряд актуальных проблем обеспечения информационной безопасности, в условиях постоянно растущего числа и изощренности кибератак на финансовые организации:

1) динамика роста числа инцидентов, объем похищенных средств и увеличение уязвимостей в программном обеспечении за последние годы свидетельствуют о необходимости совершенствования существующих подходов к управлению рисками;

2) Существующие нормативные акты Банка России не содержат ссылки на ГОСТ Р 57580.3-2022, ГОСТ Р 57580.4-2022, следовательно, их соблюдение носит рекомендательный характер, что, в свою очередь, затрудняет их обязательное внедрение;

3) применение указанных стандартов требует значительных финансовых затрат на приобретение информационной системы управления рисками финансовой организации и интеграцию с системой управления рисками реализации ин-

формационных угроз, и на выделение необходимого ресурсного (кадрового и финансового) обеспечения;

4) в настоящее время отсутствуют специализированные методики оценки рисков, связанных с операциями без добровольного согласия. Используемые на практике методические рекомендации носят исключительно уведомительный характер, направленный на повышение осведомленности клиентов об актуальных угрозах в финансовом секторе, и не предлагают инструментов для формализованной оценки таких рисков;

5) существенно возрастает роль применения на практике математического моделирования оценки и прогнозирования рисков информационной безопасности в кредитно-финансовой сфере.

Для дальнейшего укрепления кибербезопасности финансового сектора представляется целесообразным:

- разработка специализированных методик оценки рисков, в особенности для операций без добровольного согласия;

- развитие количественных подходов к оценке киберрисков на основе математического моделирования;

- поиск эффективных путей интеграции систем управления рисками реализации информационных угроз в систему управления рисками финансовой организации, что в совокупности будет способствовать повышению общей устойчивости финансового сектора к киберугрозам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Центральный банк Российской Федерации. Аналитический отчет. Киберугрозы и кибератаки в 2025 году. Оценка рисков и тенденций. – 2024. – Текст : электронный // Официальный сайт Банка России. – URL: https://cbr.ru/Collection/Collection/File/59655/Attack_2025.pdf (дата обращения: 16.11.2025). – Режим доступа: свободный.

2. Бойченко, О.В. Киберустойчивость финансовых организаций / О. В. Бойченко, О. V. Boychenko // Научный вестник: финансы, банки, инвестиции. – 2025. – № 1 (70). – С. 105–114. – ISSN 2312-5330. – Текст : электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/372007> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

3. Бойченко, О.В. Система управления рисками кибербезопасности кредитно-финансовой деятельности / О. В. Бойченко, О. V. Boychenko // Научный вестник: финансы, банки, инвестиции. – 2024. – № 3 (68). – С. 55–65. – ISSN 2312-5330. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/368069> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

4. Гуковская, А.А. Оценка киберрисков: проблемы и методы. Актуальные проблемы управления в условиях цифровой экономики России: Всерос. науч. конф. Москва, 2020 г. : материалы конференции / под редакцией Н. И. Архиповой. – Москва : РГГУ, 2020 – Часть 1 : (VII Сперанские чтения; Гуманитарные чтения РГГУ – 2020) – 2020. – 220 с. – ISBN 978-5-7281-2883-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/384914> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

5. Щербакова, Н. В. Цифровые технологии в банковском секторе РФ: особенности и сопутствующие угрозы / Н. В. Щербакова // Вестник КемГУ. Серия: Политические, социологи-

ческие и экономические науки. – 2021. – № 1. – С. 136–146. – ISSN 2500-3372. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/323153> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

6. Маслова, М.А. Анализ и определение рисков информационной безопасности / М. А. Маслова // Научный результат. Информационные технологии. – 2019. – № 1. – С. 31–37. – ISSN 2518-1092. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/311845> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

7. Польшенко, М.А. Анализ рисков в информационной среде / М. А. Польшенко, М. А. Polchenko // Молодой исследователь Дона. – 2023. – № 3 (42). – С. 55–62. – ISSN 2500-1779. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/354992> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

8. Беляев, Е. А. Анализ методик оценки рисков информационной безопасности кредитно-финансовых организаций / Е. А. Беляев, О. А. Емельянова, И. И. Лившиц // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т. 21, № 3. – С. 437–441. – DOI 10.17586/2226-1494-2021-21-3-437-441. – EDN BCSBTV.

9. Беляев Е.А., Емельянова О.А. (науч. рук. Лившиц И.И.) Подходы к управлению рисками информационной безопасности в кредитно-финансовых организациях согласно рекомендациям базельского комитета (БАЗЕЛЬ III) // Сборник тезисов докладов конгресса молодых ученых. Электронное издание. – СПб: Университет ИТМО, [2021]. URL: <https://kmu.itmo.ru/digests/article/6434> (дата обращения: 17.04.2026). – Режим доступа: для авториз. пользователей.

10. Белалов, М.Р. Киберриски как новый класс операционных рисков банков: экономическая оценка, моделирование потерь и оптимизация затрат на защиту / М. Р. Белалов // Вестник Евразийской науки. – 2025. – Т 17. – № s4. – URL: <https://esj.today/PDF/14FAVN425.pdf> (дата обращения: 17.04.2026).

11. Кошкин Д. С., Шерстов А. В., Фильо В. В. Киберриски: перспективные инструменты контроля (на примере киберстрахования) / Д. С. Кошкин // Искусство и общество. – 2023. – Т. 18. – № 1. – URL: <https://artsoc.jes.su/s207751800024767-2-1/> (дата обращения: 17.04.2026).

12. ЦИФРОВАЯ УЯЗВИМОСТЬ БИЗНЕСА: ЭВОЛЮЦИЯ КИБЕРУГРОЗ / Н. В. Долбня, N. Dolbnya, Г. Е. Шпак, G. Shpak // Новое в экономической кибернетике. – 2025. – № 4. – С. 93–110. – ISSN 2523-448X. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/375460> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

13. Положение № 716-П от 08 апреля 2020 г. «О требованиях к системе управления операционным риском в кредитной организации и банковской группе(с изменениями на 22 октября 2024 года): утверждено Центральным банком Российской Федерации (Банком России). – Москва: Центральным банком Российской Федерации (Банком России), 2009: введен впервые: дата введения 2020–04–08 / Центральным банком Российской Федерации (Банком России)–, 2019. – Текст : электронный // Консорциум Кодекс : сайт Электронный фондправовых и нормативно-технических документов. – URL: <https://docs.cntd.ru/document/564859689> (дата обращения: 16.11.2025). – Режим доступа: свободный.

14. РС БР ИББС-2.2-2009 РС БР ИББС-2.2-2009 Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушений информационной безопасности: утверждены и введены в действие распоряжением Банка России от 11 ноября 2009 г. № Р-1190: введены впервые: дата введения 2009–11–11 / разработаны Центральным банком Российской Федерации (Банком России). – Москва: Центральным банком Российской Федерации (Банком России), 2009. – Текст : электронный // ЦБ : сайт Центральный банк Российской Фе-

дерации (Банк России). – URL: https://cbr.ru/statichtml/file/59420/st22_09.pdf (дата обращения: 25.11.2025). – Режим доступа: свободный.

15. ГОСТ Р 57580.3 – 2022 Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2022 г. № 1548-ст: введен впервые: дата введения 2023–02–01 / разработан Центральным банком Российской Федерации (Банком России). – Москва: ФГБУ Институт стандартизации, 2023. – Текст : электронный // Росстандарт : сайт Федерального агентства по техническому регулированию и метрологии. – URL: <https://protect.gost.ru/gost/details/1c8a4cba-f1b9-4eec-a32b-cf6bf0637b72> (дата обращения: 16.11.2025). – Режим доступа : свободный.

16. ГОСТ Р 57580.4 – 2022 Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2022 г. № 1549-ст: введен впервые: дата введения 2023–07–01 / разработан Центральным банком Российской Федерации (Банком России). – Москва: ФГБУ Институт стандартизации, 2023. – Текст : электронный // Росстандарт : сайт Федерального агентства по техническому регулированию и метрологии. – URL: <https://protect.gost.ru/gost?year=2026&month=4&search=57580.4> (дата обращения: 17.04.2026). – Режим доступа: свободный.

17. Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности : № 7-МР от 21.03.2024. / Центральный банк Российской Федерации (Банк России). – Москва, 2024. – Текст : электронный // Официальный сайт Банка России. – URL: <https://cbr.ru/Crosscut/LawActs/File/7712> (дата обращения: 17.04.2026). – Режим доступа: свободный.

18. СТО БР БФБО-1.7-2023. Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств : стандарт Банка России : официальное издание : принят и введен в действие Приказом Банка России от 1 марта 2023 г. № ОД-335 / разработан Центральным банком Российской Федерации (Банком России). – Москва : Центральный банк Российской Федерации, 2023. – Текст : электронный // Официальный сайт Банка России : сайт Центрального банка Российской Федерации. – URL: <https://cbr.ru/Crosscut/LawActs/File/6150> (дата обращения: 17.04.2026). – Режим доступа : свободный.

19. Беляев Е.А., Емельянова О.А. (науч. рук. Исаев А.С.) Проблемы применения методических документов Банка России при осуществлении оценки рисков информационной безопасности кредитно-финансовых организаций // Сборник тезисов докладов конгресса молодых ученых. Электронное издание. – СПб: Университет ИТМО, [2020]. URL: <https://kmu.itmo.ru/digests/article/3887> (дата обращения: 17.04.2026). – Режим доступа: для авториз. пользователей.

20. Милославская, Н. Г. , Толстой А.И., Управление рисками информационной безопасности. Учебное пособие для вузов. – 4-е издание, переработанное и дополненное – Москва : Горячая линия – Телеком, 2024. – 292 с.: ил.– С. 126–128. – ISBN 978-5-9912-1037-9.

© В. А. Захаров, А. В.Троеглазова, 2026

В. И. Ковынев¹✉, Е. А. Усанькова¹

Специфика механизма управления развитием наукоёмких производств в микроэлектронике

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: vlad.kovynev.03@mail.ru

Аннотация. В условиях традиционной инструментальной промышленной политики, основанной исключительно на прямом бюджетном финансировании, демонстрируется ограниченная эффективность, что дает актуальность сфере поиска специфических механизмов управления инновационным циклом. В статье будет представлено состояние отрасли на текущий момент. Основное внимание уделено проблемам, ограничивающим стабильное развитие отрасли микроэлектроники, проблемам сферы управления развитием наукоёмкого производства Российской Федерации, институциональные и организационные специфики управления развитием, отличающие данную сферу от классических секторов экономики, пути ввода новых технологий, на основе появления искусственного интеллекта в производстве и способы модернизации, приводящие к увеличению производственных мощностей в будущем, предложены рекомендации по оптимизации и сглаживанию проблем сопутствующих отрасли микроэлектроник.

Ключевые слова: микроэлектроника, искусственный интеллект, технологический суверенитет, научно-исследовательские и опытно-конструкторские работы

V. I. Kovynev¹✉, E. A. Ysankova¹

The Specifics of the Mechanism for Managing the Development of Science-Intensive Production in Microelectronics

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: vlad.kovynev.03@mail.ru

Abstract. In the context of traditional instrumental industrial policy, which is based solely on direct budgetary financing, limited efficiency is demonstrated, which makes it relevant to search for specific mechanisms for managing the innovation cycle. This article will present the current state of the industry. The main attention is paid to the problems that limit the stable development of the microelectronics industry, the problems of managing the development of science-intensive production in the Russian Federation, and the institutional and organizational specifics of development management that distinguish this sector from classical sectors of the economy, ways of introducing new technologies based on the emergence of artificial intelligence in production, and methods of modernization leading to an increase in production capacity in the future. Recommendations are proposed for optimizing and smoothing out the problems associated with the microelectronics industry.

Keywords: microelectronics, artificial intelligence, technological sovereignty, research and development work

Введение

Развитие наукоёмкого производства – это неотъемлемый процесс, которым необходимо управлять. Каждый день разрабатывается, дорабатывается, патенту-

ется и создается определенное новшество, область микроэлектроники не является в этом исключением. За промежуток в пять лет объем выпуска электроники по миру увеличился в несколько раз. Развитие сферы микроэлектроники движется с высокой скоростью, обусловлено этой высокой потребностью продукции данной отрасли на мировом рынке. Она непрерывно сопутствует и помогает нам как в повседневной жизни, так и в работе. На отечественном рынке данной отрасли выделяют значительное внимание. Только за промежуток в 4 года, данная отрасль получила финансовую поддержку и по сей день продолжают поступать финансовые импульсы, направленные на развитие.

Методы и материалы

Из данных представленных «Ассоциацией разработчиков и производителей электроники» Российский рынок электронных компонентов упал на 25 % по сравнению с предыдущим годом. Данные по вложению инвестиций в отрасль микроэлектроники представлены в таблице 1.

Таблица 1 – Доля отечественной продукции от суммы инвестиций

Год	Объем рынка продукции, млрд. руб.	Доля отечественной продукции в %	Объем рынка отечественной продукции, млрд. руб.
2022	256,8	27,1	69,5
2023	310,1	32	99,2
2024	384,6	26,7	102,6
2025	288	26	74,9

Обзор текущих проблем отрасли микроэлектроники

С другой стороны, исходя из исследований «Ассоциации разработчиков и производителей электроники» рынок микроэлектроники Российской Федерации на момент 2026 года находится в структурном кризисе. Только за прошлый год видны падения объема на четверть, коснулось это и крупнейшего производителя микроэлектроники компанию «Элемент». В этом аспекте есть три основные проблемы, выделяемые экспертами. Основной парадокс наблюдается в доле отечественной компонентной базы, доля которой на рынке на протяжении нескольких лет уменьшается. Так, к примеру, в 2023 она составляла 32 процента, в 2024 снизилась до 26,7 процента, а по итогам 2025 года составила около 26 процентов. По мнению главы АРВЭ Ивана Покровского, на падения рынка повлияло сокращение инвестиционных программ заказчиков в условиях высокой банковской ставки, дефицита бюджетов и неопределенных перспектив, а также сокращения объема госзаказов [1]. Вторым направлением является «разрыв спроса» или «узко направленность» отрасли отечественной микроэлектроники, подразумевающей под собой довольно обширное различие между гражданской и военной отраслью в непосредственной необходимости продукции микроэлектроники. Разница колоссальна и с экономической точки зрения гипертрофированный крен в сторону ОПК создает обстоятельства того, что отрасль попадает в «ловушку специализа-

ции»: критическая зависимость от государственных заказов делает её уязвимой в бюджетных циклах, что и привело, как было сказано ранее к падению рынка. Одновременно с этим блокируется механизм коммерциализации и эффекта масштаба. Без массового гражданского спроса невозможна окупаемость НИОКР, как следствие себестоимость остается хронологически высокой, а стимуляции к инновациям слабыми. В результате формируется институциональная ловушка, где оборонный сектор вытягивает кадры и субсидии, а гражданский – не создает достаточной добавленной стоимости, консервируя технологическое отставание, а не сокращая его. Третьим фактором является «Дефицит кадров». По итогам 2025 года нехватка специалистов превысила пять тысяч человек, а к 2030 году по оценкам экспертов может достигнуть десяти тысяч [2]. Самыми востребованными и одновременно с этим дефицитными вакансиями является инженер-технолог, инженер-конструктор.

Следовательно, перечисленные вызовы не представляется возможным преодолеть только за счёт наращивания пакета инвестиций. Наукоемкое производство при отсутствии эффективного механизма управления развитием лишь консервирует отсутствие прогресса. Возникает вопрос: какой вид должна иметь система управления, для видоизменения замкнутого круга производства, представленного на данный момент, в спираль технологического роста.

Обсуждение

Проведенный анализ позволяет перейти к формулированию рекомендаций, направленных на устранение недочетов и достижения технологического суверенитета страны в ряде технических отраслей после ухода иностранных компаний [3]. Данные предлагаемые меры опираются на оценки профильных организаций, данные аналитических центров, и поручений по реализации плановых мероприятий от вышестоящих органов власти.

Системная трансформация кадрового обеспечения отрасли микроэлектроники требует кардинального пересмотра подготовки специалистов [4]. Для решения проблемы необходимо налаживать взаимодействие компаний – разработчиков отечественной микроэлектроники с вузами и колледжами. В данной сфере уже проводятся эксперименты и изменения, как пример «Минцифры» в сентябре 2025 года эксперимент по поддержке профильного образования крупными ИТ-компаниями. Фирмы с годовой выручкой более 1 млрд рублей и численностью сотрудников более 100 человек будут отчислять 5 % от средств, сэкономленных благодаря налоговым льготам, на поддержку образования в сфере ИТ [5]. Эти средства пойдут на оплату преподавательской деятельности сотрудников, на практико-ориентированную корректировку учебных курсов высшего и среднего профобразования, на организацию стажировок для студентов в ИТ-компаниях, старших классов по ИТ-тематике. Модернизация и запуск новых магистерских и аспирантских программ, а также преподавательские и студенческие стажировки могут способствовать существенному сокращению кадрового разрыва. Данное предложение отметил ректор УрФУ Илья Обабок [6]. Первый вы-

пуск инженеров, проходивших подготовку в соответствии с обновленной программой, ожидается в 2027 году.

В отношении разрыва между спросом на продукцию микроэлектронику со стороны гражданского потребления и военного комплекса разница колоссальна и для изменения ситуации необходимы конкретные меры стимуляции отрасли гражданской микроэлектроники. Важно запустить регуляторные стимулы для внедрения доверенных программно-аппаратных комплексов на основе использования российских микропроцессоров. Стратегические расчеты из документа АРПЭ в отношении доверенных аппаратных платформ предполагают, что такая система позволит увеличить долю гражданского производства, вследствие чего за счет льгот, финансирования со стороны государства и применения механизмов автономного обучения специалистов, представленных «Минцифрами» гражданский сектор микроэлектроники, сможет стать конкурентоспособным на мировом рынке.

Заключение

Абсолютная самостоятельность в отрасли микроэлектроники недостижима ни для одной из стран мира. Не раз исследования экспертов доказывали, что на первый план выходит задача формирования экосистемы, которая позволит быстро создавать и внедрять инновации в производство и саму продукцию. Одним из последних таковых является исследование Strategy Pether's [3], в котором подчеркивается важность сотрудничества с ведущими странами и кооперации в вопросах модернизации, а также сотрудничество позволяет быстрее пройти этапы развития за счет возможности обмена опытом между ведущими производствами микроэлектроники. Особенно важно обеспечить совместимость программного обеспечения с доверенным оборудованием на российских микросхемах. В перспективе пяти лет это даст порядковый рост числа внедрений и объема поставок отечественных микросхем [7].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. CNews. Рынок российской микроэлектроники рухнул на четверть. Текст : электронный. – URL : <https://zoom.cnews.ru/news/item/672052> (дата обращения 14.05.2026)
2. Intelligent enterprise. Перспективы развития производства 21 века. Текст : электронный. – URL: <https://www.iemag.ru/opinions/detail.php> (дата обращения 29.04.2026).
3. Strategy Perthners. Суверенитет российской микроэлектроники. Текст : электронный. – URL: <https://strategy.ru/research/research/suverenitet-rossijskoj-mikroelektroniki-s-chego-nachat/> (дата обращения 03.05.2026).
4. COMNEWS. Микроэлектроника подтянулась по уровню заработной платы к сектору IT. Текст : электронный. – URL: <https://www.comnews.ru/content/245045/2026-04-30/2026w18/1007/mikroelektronika-podtyanulas-zarplatam-k-it-sektoru-i-zhdet-sistemnogo-zakaza> (дата обращения 03.05.2026).
5. СЕТЕВОЕ ИЗДАНИЕ НАЦИОНАЛЬНАЯ СИСТЕМА КВАЛИФИКАЦИИ РОССИИ. О новых подходах организации наукоемкого производства. Текст : электронный. – URL: <https://journal.nark.ru/articles/spk/o-novykh-podkhodakh-k-organizatsii-vzaimodeystviya-spk-fumo-i-professionalnogo-soobshchestva-v-oblas/> (дата обращения 29.04.2026).

6. Уральский федеральный университет. Подготовка новых кадров и кадровый голод.
Текст : электронный. – URL: <https://soc.urfu.ru/ru/glavnaja/novosti/?news=56401&cHash=4b8b6da714117d67f288f8a85479d1c0> (дата обращения 03.05.2026).

7. ТЕХНОСФЕРА Россия. Как в России за 10 лет полностью изменить IT- сферу.
Текст : электронный. – URL : <https://tehnoomsk.ru/archives/16940> (дата обращения 06.05.2026).

© В. И. Ковынев, Е. А. Усанькова, 2026

С. С. Кузьмин^{1✉}, А. Н. Поликанин¹

Сравнительный анализ способов обнаружения БПЛА

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: tvoypapik4@gmail.com

Аннотация. В статье рассматриваются существующие виды систем обнаружения БПЛА и производится их анализ, выделение метрик и сравнение. Среди видов систем выделяют системы радиомониторинга, оптические системы и акустические системы. Каждый вид обладает своими преимуществами и недостатками и их следует рассматривать не только по отдельности, но и по возможности объединения для покрытия недостатков друг друга. Наиболее часто встречаемые в использовании системы RF мониторинга, стоят больших денег и имеют крайне серьезную слепую зону, что и объясняет необходимость искать оптимальные комбинации систем. Поскольку акустические и оптические работают на схожих расстояниях, стоят меньше, обладают хорошим взаимодействием и способны работать совместно в портативных системах, их и следует рассматривать как оптимальный вариант систем обнаружения БПЛА.

Ключевые слова: БПЛА, системы обнаружения БПЛА, системы радиомониторинга, акустические системы, оптические системы, радиолокация

S. S. Kuzmin^{1✉}, A. N. Polikanin¹

Comparative Analysis of UAV Detection Methods

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: tvoypapik4@gmail.com

Abstract. This article examines the existing types of UAV detection systems and analyzes them, identifies metrics and compares them. Among the types of systems, radio monitoring systems, optical systems and acoustic systems are distinguished. Each type has its own advantages and disadvantages, and they should be considered not only separately, but also combined, if possible, to cover each other's disadvantages. The most commonly used RF monitoring systems cost a lot of money and have an extremely serious blind spot, which explains the need to look for optimal combinations of systems. Since acoustic and optical systems operate at similar distances, cost less, have good interaction and are able to work together in portable systems, they should be considered as the best option for UAV detection systems.

Keywords: UAVs, UAV detection systems, radio monitoring systems, acoustic systems, optical systems, radiolocation

Введение

В настоящее время использование БПЛА стало повсеместным, применение их можно увидеть как в гражданском, так и в военном секторе. Вместе с ними развиваются и используются системы обнаружения БПЛА, однако компаний, которые занимаются разработкой систем обнаружения мало, а цены на разработанные системы крайне высоки. По причине высокой цены не все

участники целевой аудитории имеют возможность закупить необходимое оборудование обнаружения БПЛА, одновременно с тем системы обнаружения, распространенные на рынке, имеют слепые зоны не смотря на свою высокую цену.

Использование оптимальных систем с наименьшим количеством слепых зон является желаемым результатом для любой выстроенной системы защиты. В настоящее время было выделено несколько различных видов систем обнаружения БПЛА, основанных на разных физических свойствах исследуемого объекта обнаружения.

Среди видов систем обнаружения БПЛА можно выделить следующие классы:

- системы радиомониторинга;
- оптические системы;
- акустические системы [1].

Развитие современных технологий приносит множество новых способов решения ранее нерешаемых задач. По причине активного использования БПЛА в военных целях, были обнаружены способы обхода самых популярных в настоящее время для использования радиотехнических систем обнаружения БПЛА. По причине полного отсутствия у данных систем способа решения своей слепой зоны все чаще стали применять комбинированные варианты систем дополняя возможности и закрывая слепые зоны популярного метода обнаружения.

Актуальностью данной работы является рассмотрение характеристик, определение наличия слепых зон различных видов систем обнаружения БПЛА и выделение оптимальных видов для сочетания в комбинированной системе.

Цель: выделить и провести анализ существующих видов систем обнаружения БПЛА, выделить ключевые метрики оценивания, определение оптимальных вариантов систем.

Системы радиомониторинга

В класс систем радиомониторинга входят активные системы радиолокации и системы пассивного RF (Radio Frequency) мониторинга.

Активная радиолокация работает по принципу отправления радиоволнового сигнала в пространство и принятия отраженного от твердого физического объекта сигнала для определения местоположения объектов окружающей среды [2].

RF мониторинг в отличие от активной радиолокации не выпускает никакого сигнала, а только принимает исходящие от других объектов сигналы [3].

Активная радиолокация хороша тем, что она способна довольно точно определять присутствие объекта на большом расстоянии, даже если объектом является не электронное устройство, а живое существо. Однако сам принцип работы системы активной радиолокации и является одним из ее самых главных недостатков. Поскольку если система сама излучает свой сигнал в пространство, то ее сигнал можно уловить и определить точное местоположение посылаемого

сигнала, что может привести к целенаправленному устранению оборудования [4].

Пассивный RF мониторинг, как и радиолокация хорош тем, что дистанция его работы может достигать нескольких километров. За счет того, что принцип его работы основан на улавливании сторонних радиосигналов, он способен обнаруживать управляемые дистанционно БПЛА и даже местоположение операторов БПЛА. По причине того, что данный вид систем работает на большие расстояния, действует пассивно и способен точно определять любой привычный БПЛА, этот вид систем используется чаще всего. Однако по причине возможности поиска объектов лишь по радио сигнатурам этот вид систем не способен обнаружить БПЛА, отправленный напрямую по оптоволокну, что является полной слепой зоной данного вида.

Для систем радиочастотного мониторинга чаще всего требуются громоздкие и дорогостоящие комплексы оборудования.

Оптические системы

Оптические системы обнаружения БПЛА используют различные камеры (видимого спектра, инфракрасные, тепловизоры, лазерные локаторы, лидары) для визуального обнаружения БПЛА [5].

Преимуществом данных с систем является то, что они пассивны по принципу обнаружения, точны в определении, довольно портативны и способны работать в инфракрасном диапазоне. Однако данные системы в отличие от систем радиомониторинга способны работать в меньшем диапазоне, зависят от просматриваемости местности и крайне ресурсоемки в плане средств обработки [6].

Акустические системы

Акустические системы обнаружения БПЛА работают по принципу улавливания в звуковом пространстве, издаваемых техническими компонентами дронов звуков и последующему определению присутствия БПЛА [7].

Такие системы, как и оптические имеют схожий ограниченный радиус обнаружения объекта до 250–500 метров, портативны, а также крайне ресурсоэффективны в плане средств обработки. Недостатком же является малая дистанция обнаружения и зависимость от шума [8].

Комбинированные системы

Комбинированные системы не столько отдельный вид, сколько общее название систем обнаружения созданных из объединения оптических систем, акустических систем или систем радиомониторинга [9].

Комбинирование систем как принцип существует для того, чтобы:

- сохранить положительные качества первоначальных систем;
- повысить точность обнаружения;
- избавиться от слепых зон первоначальных систем.

По причине того, что системы RF мониторинга используются в настоящее время чаще всего, в комбинированных системах также берут RF мониторинг системы за основу для комбинированных систем. Среди существующих комбинированных систем чаще всего встречаются именно варианты RF мониторинга и оптической системы с камерой. Дополнив систему RF мониторинга камерой, они исправляют слепую зону данной системы по отношению к БПЛА, отправленным по оптоволоконному кабелю, и увеличивают точность обнаружения [10].

Сравнительный анализ систем

Чтобы рассмотреть отличительные характеристики различных систем обнаружения БПЛА были выделены следующие метрики сравнения:

- дальность обнаружения;
- скрытность работы;
- устойчивость к РЭБ (средства радиоэлектронной борьбы);
- стоимость.

Из выделенных метрик была создана табл. 1.

Таблица 1 – Характеристики систем обнаружения БПЛА

Критерий оценки	Активная радиолокация	RF мониторинг	Оптические системы	Акустические системы
Дальность обнаружения	До 10 км	До 10 км	До 1 км	До 500 м
Скрытность работы	нет (излучает)	да	да	да
Устойчивость к РЭБ	нет	нет	да	да
Стоимость	100–200 млн рублей	1–10 млн рублей	100–150 тыс. рублей	40–100 тыс. рублей

Заключение

По причине роста повсеместного использования БПЛА, стали появляться и развиваться системы обнаружения. Однако в соответствии тому, как были созданы средства обнаружения БПЛА, стали находиться и новые способы обходить данные системы. Одним из основных способов противодействия обхода систем обнаружения стало создание комбинированных систем обнаружения. Среди комбинированных систем самым популярным является объединение RF мониторинга и оптических средств. Но данная комбинированная система имеет смысл своего существования начиная с минимального из двух расстояний. В то время как RF мониторинг способен вести обнаружение до 10 километров, оптическая часть системы способна дополнять свою работу лишь с расстояния до 500 метров. Желаемым к рассмотрению комбинации систем имеет смысл

объединение оптико-акустической системы. Объединение оптической и акустической систем в одну закрывает слепые зоны друг друга, одновременно с тем увеличивая точность обнаружения. Оптико-акустическая система обнаружения будет многократно дешевле чем система с участием RF мониторинга, обе составляющие данной системы работают на схожей дистанции, а также каждый элемент способен работать на портативных вычислительных устройствах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Красненко Н. П., Богушевич А. Я., Кураков С. А., Раков А. С., Рыбаков И. А. Обнаружение беспилотных летательных аппаратов: существующие решения и возможности – Текст : непосредственный // Всероссийские открытые Армандовские чтения: Современные проблемы дистанционного зондирования, радиолокации, распространения и дифракции волн. – 2024. – № 1. – С. 429-440.
2. Будкин Н. Д. Средства обнаружения беспилотных летательных аппаратов и перспективы их развития – Текст : непосредственный // Вестник науки. – 2024. – № 12. – С. 1564-1568.
3. Фалилеев В. Ю., Шатовкин Р. Р. Анализ существующих автоматизированных комплексов защиты от дронов – Текст : непосредственный // Воздушно-космические силы. Теория и практика. – 2020. – № 14. – С. 130-139.
4. Бомбизов А. А., Петров А. Б., Лоцилов А. Г. Исследование электромагнитного и акустического излучения беспилотных летательных аппаратов в области низких частот – Текст : непосредственный // Доклады ТУСУР. – 2018. – № 1. – С. 57-61.
5. Шайдаев М. Ш. Лазерные системы для борьбы с беспилотными летательными аппаратами: преимущества и недостатки – Текст : непосредственный // Академическая мысль. – 2023. – № 4. – С. 157-161.
6. Макаренко С. И., Тимошенко А. В., Васильченко А. С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 1. Беспилотный летательный аппарат как объект обнаружения и поражения – Текст : непосредственный // Системы управления, связи и безопасности. – 2020. – № 1. – С. 109-145.
7. Тихонов В. А., Карташов В. М., Олейников В. Н., Леонидов В. И., Тимошенко Л. П., Селезнев И. С., Рыбников Н. В. Обнаружение-распознавание беспилотных летательных аппаратов с использованием составной модели авторегрессии их акустического излучения – Текст : непосредственный // Вісник НТУУ «КПІ». Серія Радіотехніка, Радіоапаратобудування. – 2020. – № 81. – С. 39-46.
8. Гончаренко Б. И., Кузьменков В. Ю., Котов А. Н. Экспериментальное исследование особенностей формирования спектра шумов беспилотного летательного аппарата – Текст : непосредственный // Noise Theory and Practice. – 2020. – № 4. – С. 49-59.
9. Горячев Н.В., Избасов А.Г., Мельничук А.И., Мухамбетов А.М., Юрков Н. К. К Проблеме синтеза системы противодействия малогабаритным беспилотным летательным аппаратам – Текст : непосредственный // Надежность и качество сложных систем. – 2024. – № 2. – С. 64-71.
10. Ловцов Д. А., Гаврилов Д. А. К Эффективная автоматизированная оптико-электронная система аэрокосмического мониторинга – Текст : непосредственный // Правовая информатика. – 2019. – № 2. – С. 26-39.

© С. С. Кузьмин, А. Н. Поликанин, 2026

А. В. Кукса^{1✉}, Е. А. Усанькова¹

Конструкторско-технологическая оптимизация как инновационный подход к процессу производства

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: anyuta.kuksa2003@mail.ru

Аннотация. Объектом исследования является процесс изготовления авиационной детали. Предмет исследования – методы и результаты оптимизации конструкции и технологии изготовления авиационной детали. Цель работы – определить основные подходы и методы усовершенствования выпускаемой авиационной продукции, провести анализ традиционных подходов к проектированию и изготовлению авиационных узлов, выявить их преимущества и недостатки. Обосновано, что в условиях высокой наукоемкости отрасли и ужесточения требований к качеству, наиболее эффективным методом повышения производственной эффективности является сокращение количества входящих элементов конструкции за счет перехода к интегральным (монокристаллическим) решениям. Показано, что данный подход обеспечивает снижение трудоемкости, повышение качества продукции, сокращение производственного цикла и улучшение экономических показателей производства.

Ключевые слова: конструкторско-технологическая оптимизация, авиационная промышленность, оптимизация производства, интегральные конструкции

A. V. Kuksa^{1✉}, E. A. Usankova¹

Design and technological optimization as an innovative approach to the production process

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: anyuta.kuksa2003@mail.ru

Abstract. The object of the study is the manufacturing process of an aircraft component. The subject of the study is the methods and results of optimizing the design and manufacturing technology of an aircraft component. The goal of the work is to identify the main approaches and methods for improving manufactured aircraft products, analyze traditional approaches to the design and manufacture of aircraft components, and identify their advantages and disadvantages. It has been substantiated that, given the industry's high research intensity and increasingly stringent quality requirements, the most effective method for improving production efficiency is reducing the number of input design elements by transitioning to integrated (monolithic) solutions. This approach has been shown to reduce labor intensity, improve product quality, shorten the production cycle, and improve economic performance.

Keywords: design and technological optimization, aviation industry, production optimization, integrated designs

Введение

Снижение себестоимости и сокращение сроков технологической подготовки производства (ТПП) изделий напрямую зависят от эффективности кон-

структурско-технологической оптимизации (КТО). Быстрая сменяемость модификаций и жесткие требования к эксплуатационным характеристикам деталей делают традиционное проектирование менее эффективным. Это предопределяет необходимость внедрения интегрированного подхода, обеспечивающего совершенствование геометрических и прочностных параметров конструкций, и технологий их изготовления.

Практическая реализация КТО базируется на принципах системного анализа, взаимодействия и применения сквозных цифровых технологий, включая методы численного моделирования и алгоритмы многокритериального поиска. Такой подход обеспечивает повышение коэффициента использования материала (КИМ), снижение материалоемкости и трудоемкости производства и повышение технологичности конструкций без ухудшения их эксплуатационных характеристик.

Авиастроение является наукоемкой и высокотехнологичной отраслью, которая функционирует в условиях жестких стандартов безопасности и глобальной конкуренции. Современные вызовы авиационной индустрии требуют минимизации временных и материальных затрат при одновременном повышении надежности, долговечности и ресурса авиационной техники. В связи с этим оптимизация конструктивно-технологических решений становится доминирующим вектором обеспечения устойчивого развития отрасли.

Целью исследования является научно-практическое обоснование метода оптимизации конструкции и технологических параметров изготовления детали авиационного назначения для повышения КИМ, сокращения цикла механической обработки и обеспечения нормативных эксплуатационных характеристик изделия.

Методы и материалы

Традиционная оптимизация в авиастроении направлена на совершенствование механической обработки: минимизацию припусков и подбор рациональных режимов резания. Это, безусловно, позволяет сократить машинное время и улучшить свойства поверхностного слоя детали. Однако классическое проектирование, основанное на испытаниях физических моделей, экономически неэффективно [1]. Это обуславливает необходимость активного внедрения методов, учитывающих современные производственные технологии, включая процессы сборки [2]. Актуальной задачей является разработка метода, позволяющего оптимизировать процесс проектирования изделий на ранних стадиях.

Локальная оптимизация режимов резания не решает системных проблем многокомпонентных конструкций. Сборные детали увеличивают производственный цикл, массу изделия и риск ошибок оператора. Решением этой проблемы является переход от сборных узлов к монолитным деталям и интегральным конструкциям, что исключает трудоемкие операции сборки [3].

Результаты

Сопряженное проектирование и КТО позволяют сократить сроки научно-исследовательских и опытно-конструкторских работ (НИОКР) и снизить себестоимость изготавливаемой техники [4, 6].

В основе КТО лежит применение принципов DFM (проектирование для производства) и DFA (проектирование для сборки). Это предполагает переход от многокомпонентности к монолитности деталей, что позволяет снизить конструктивную сложность изделия и исключить сборочные операции из технологического маршрута. Эффективность монолитных конструкций подтверждается следующими факторами:

1. Снижение трудоемкости за счет исключения заготовительно-сборочных переходов.
2. Сокращение производственного цикла благодаря уменьшению количества технологических операций.
3. Повышение надежности из-за ликвидации зон стыка и нахлеста – потенциальных источников трещин, коррозии и дефектов швов.

В отличие от локальной оптимизации режимов обработки или внедрения контроля качества, КТО дает системный эффект на всех этапах ТПП, снижая затраты на исправление брака. Для авиастроения переход к интегральным конструкциям является одним из важных условий обеспечения конкурентоспособности производства [5].

Обсуждение

Эффективность производства авиационных деталей определяется оптимизацией архитектуры изделия. Классические методы оптимизации (например, концепции процессного управления К. Б. Герасимова) сфокусированы на локальных организационных задачах, не уточняя конструктивную сложность узлов. Внедрение цифрового моделирования и аддитивных технологий повышает точность формообразования (С. С. Клименков, В. В. Рубаник), но многокомпонентная структура изделия ограничивает их потенциал. Согласно мнению А. С. Шапикна, передовые методы проектирования ускоряют производственный цикл [7]. Однако стандартные CAD/CAM-системы, по оценке Е. И. Яблочникова, решают только задачи параметрической оптимизации, не меняя конструктивно-технологическую схему.

Решением проблемы является переход к интегральным конструкциям на принципах DFM/DFA. Сокращение номенклатуры деталей исключает сборочные операции, которые, по мнению В. И. Бехметьева, создают наибольшую трудоемкость и погрешности. Внедрение таких инноваций требует системного управления ТПП [8]. При этом методы обеспечения качества, такие как анализ видов и последствий отказов (FMEA) и статистическое управление процессами (SPC), лишь снижают брак при сборке, но не устраняют первопричину дефектов – избыточное количество соединений [9].

Заключение

Проведенный анализ показывает, что существующие методы оптимизации производства деталей самолетов не решают ключевых проблем, связанных со сложностью конструкции изделия. Конструкторско-технологическая оптимизация представляет собой инновационный подход, позволяющий внедрять и модер-

низировать процессы проектирования и производства. Наиболее эффективным способом такой оптимизации является сокращение числа входящих элементов конструкции. Переход к более упрощенным сборочным конструкциям снижает трудозатраты и издержки, повышает качество и надежность, сокращает жизненный цикл и увеличивает конкурентоспособность продукции.

Таким образом, минимизация числа входящих элементов и переход к монолитным конструкциям следует рассматривать как приоритетное направление в развитии современного авиастроения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Сарымсаков Х. Г., Султанов Н. З. Системы автоматизированного проектирования самолета. М., – 1985. – 50 с.
2. Мантусов М. Н., Ривин Г.Л. Оптимизация конструкторско-технологического проектирования авиационных конструкций с использованием информационных технологий : статья. – Самара. : Известия Самарского научного центра РАН, 2011. – 410 с.
3. Бойцов Б. В. Автоматизация технологических процессов в авиастроении / Б. В. Бойцов. – М. : Машиностроение, 2019. – 296 с.
4. Арепьев Ю. И. Организация и управление авиационным производством / Ю. И. Арепьев. – М. : Инфра-М, 2021. – 428 с.
5. Портер М. Конкурентное преимущество : Как достичь высокого результата и обеспечить его устойчивость / М. Портер. – М. : Альпина Паблишер, 2021. – 715 с.
6. Баранчев В. П. Управление инновациями : учебник / В. П. Баранчев, Н. П. Масленникова, В. М. Мишин. – М. : Юрайт, 2022. – 747 с.
7. Шапкин А. С. Проектирование технологических процессов в авиастроении / А. С. Шапкин. – М. : Машиностроение, 2021. – 367 с.
8. Новиков Д. А. Механизмы управления инновационными проектами / Д. А. Новиков. – М. : Ленанд, 2019. – 336 с.
9. Голубков Е. П. Инновационный менеджмент : учебник / Е. П. Голубков. – М. : Юрайт, 2021. – 392 с.

© А. В. Кукса, Е. А. Усанькова, 2026

А. С. Лаптева¹✉, Е. С. Агеенко¹

Необходимость и проблематика внедрения 3D-формата в процесс территориального планирования

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: sidorasinka@gmail.com

Аннотация. Актуальность исследования обусловлена цифровой трансформацией государственного и муниципального управления в Российской Федерации, в частности реализацией концепции «Умный город» и формированием Национальной системы пространственных данных, которые предполагают использование «цифровых двойников» территорий. Показано, что действующая система подготовки документов базируется на устаревших двумерных методах, что приводит к ошибкам: невозможности учета рельефа, противоречивости исходных данных из различных информационных систем, отсутствию интеграции с развивающимся 3D-кадастром. В работе проанализирована иерархия документов градостроительной деятельности согласно Градостроительному кодексу РФ, выявлено несоответствие между формально закрепленной вертикальной структурой и фактическими матричными связями. Обосновано, что проект планировки территории (ППТ) функционально является продолжением генерального плана, поэтому внедрение 3D-формата в территориальное планирование невозможно без интеграции с 3D-моделями ППТ. На основе анализа российских (проект «ТОМСК 3D», создание пространственной модели с. Чеповш) и зарубежных (Virtual Singapore, Helsinki 3D+) практик систематизированы основные барьеры внедрения: нормативно-правовые, технологические, кадровые и экономические. Сформулированы предварительные рекомендации по поэтапному переходу к 3D-формату.

Ключевые слова: 3D-формат, 3D-модель, территориальное планирование, генеральный план, проект планировки территории, цифровой двойник

A. S. Lapteva¹✉, E. S. Ageenko¹

Necessity and Problems of Implementing the 3D Format in the Territorial Planning Process

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: sidorasinka@gmail.com

Abstract. The relevance of the study is determined by the digital transformation of state and municipal governance in the Russian Federation, particularly through the implementation of the «Smart City» concept and the formation of the National Spatial Data System, both of which presuppose the use of «digital twins» of territories. It is shown that the current system of document preparation is based on outdated two-dimensional methods, which leads to errors: the inability to account for terrain relief, inconsistency of initial data from various information systems, and the lack of integration with the developing 3D cadastre. The paper analyzes the hierarchy of urban planning activity documents according to the Town Planning Code of the Russian Federation and reveals a discrepancy between the formally established vertical structure and the actual matrix-based relationships. It is substantiated that the territory planning project (TPP) functionally serves as a continuation of the master plan; therefore, the implementation of the 3D format in territorial planning

is impossible without integration with 3D models of TPPs. Based on an analysis of Russian (the «TOMSK 3D» project, the creation of a spatial model of the village of Cheposh) and foreign (Virtual Singapore, Helsinki 3D+) practices, the main barriers to implementation are systematized: regulatory, technological, personnel, and economic. Preliminary recommendations for a phased transition to the 3D format are formulated.

Keywords: 3D format, 3D model, territorial planning, master plan, territory planning project, digital twin

Введение

Современный этап пространственного развития Российской Федерации характеризуется цифровой трансформацией различных отраслей, в том числе, в сфере государственного и муниципального управления. Концепция «Умный город» и формирование Национальной системы пространственных данных (НСПД) предполагают переход к управлению территориями на основе актуальных трехмерных моделей – «цифровых двойников» [1]. Однако реальная практика подготовки документов по-прежнему базируется на традиционных двумерных подходах.

Цель исследования – обосновать необходимость внедрения 3D-формата в документы территориального планирования (далее – ДТП) и систематизировать основные проблемы, препятствующие этому переходу.

Методы и материалы

Исследование выполнено с использованием методов анализа нормативно-правовых документов, обобщения научной литературы и сравнительного анализа практических примеров внедрения 3D-формата. Материалами послужили: Градостроительный кодекс РФ [2], Концепция проекта цифровизации городского хозяйства «Умный город» [1]; научные публикации по теме 3D-моделирования в градостроительстве [3-8]; а также опыт реализации проекта «ТОМСК 3D» [7] и создания пространственной модели части села Чепош Республики Алтай [4].

Результаты

Прежде чем анализировать возможности внедрения 3D-формата в подготовку документов по планированию, использованию и развитию территории муниципального образования, необходимо определить место рассматриваемых документов в системе градостроительной деятельности.

Градостроительный кодекс Российской Федерации (ГрК РФ) определяет градостроительную деятельность как деятельность по развитию территорий, в том числе городов и сельских поселений [2]. В соответствии с нормами ГрК РФ, градостроительную деятельность в зависимости от решаемых задач можно разделить на три последовательных уровня: территориальное планирование, градостроительное зонирование и планировка территории [2]. На первый взгляд, эта структура предполагает строгую вертикальную иерархию: от стратегического целеполагания через правовое зонирование к детальной планировке. Однако ана-

лиз содержания документов и практика их реализации показывают, что реальная логика градостроительного регулирования сложнее.

Территориальное планирование (первый уровень) реализуется для определения направлений развития территорий на долгосрочную перспективу. Результатом этого уровня является установление функциональных зон, которые задают вектор развития территории – например, жилая, рекреационная или производственная функция территории без точного юридического описания границ и режимов ее использования.

Градостроительное зонирование (второй уровень) обеспечивает деление территории на территориальные зоны с определенными правовыми режимами использования (через установление градостроительных регламентов), зафиксированными в Правилах землепользования и застройки (ПЗЗ). Важно подчеркнуть, что связь между функциональными и территориальными зонами не является вертикальным спуском «сверху вниз» в чистом виде. Функциональная зона – это стратегический ориентир, а территориальная зона – инструмент его реализации, однако одна функциональная зона может включать несколько территориальных. Более того, сведения о территориальных зонах вносятся в реестр границ ЕГРН, тогда как функциональные зоны такой юридической силы не имеют. Это означает, что ПЗЗ как документ обладает самостоятельным значением и не является простой «детализацией» генерального плана.

Планировка территории (третий уровень) реализуется посредством подготовки проекта планировки территории (ППТ) и проекта межевания территории (ПМТ). Подготовка проектов планировки территории осуществляется для выделения элементов планировочной структуры, установления границ территорий общего пользования и зон размещения объектов капитального строительства, а также определения характеристик и очередности развития территории [2]. Проекты межевания подготавливают в отношении застроенных или подлежащих застройке территорий, расположенных в границах элементов планировочной структуры. Они предназначены для определения местоположения границ образуемых и изменяемых земельных участков, устранения недостатков в конфигурации объектов (вклинивание, чересполосица, изломанность границ), а также установления, изменения или отмены красных линий на застроенных территориях, где не планируется новое строительство [2]. Таким образом, именно на этом этапе определяется, где, когда и какие объекты будут возведены.

Здесь возникает принципиальный момент: согласно ст. 18 ГрК РФ, к документам территориального планирования относятся только схемы территориального планирования и генеральные планы [2]. ППТ формально отнесен к документации по планировке территории (глава 5 ГрК РФ) и не входит в перечень документов территориального планирования. Однако в практической градостроительной деятельности сложилась иная логика. Генеральный план определяет назначение территорий, но не устанавливает красные линии и не формирует элементы планировочной структуры с точностью, достаточной для строительства. Эту задачу решает именно ППТ, который функционально продолжает и конкретизирует генеральный план. Без ППТ генеральный план остается «декларацией

о намерениях», не имеющей инструментов реализации на уровне отдельных кварталов и улиц.

Таким образом, если формально (юридически) иерархия документов является трехуровневой с четким разделением, то содержательно (функционально) ППТ выступает следующим звеном в цепочке пространственного развития, начатой генеральным планом. Как следствие, внедрение 3D-формата в территориальное планирование невозможно без интеграции с 3D-моделями проектов планировки.

С учетом изложенного, в рамках настоящей статьи под территориальным планированием в широком смысле понимается совокупность генерального плана и проектов планировки территории как взаимосвязанных документов, обеспечивающих переход от стратегического целеполагания к параметрически заданной планировочной структуре.

Если представить описанные взаимосвязи графически, возникает не линейная вертикальная структура, а более сложная конфигурация (рис. 1).

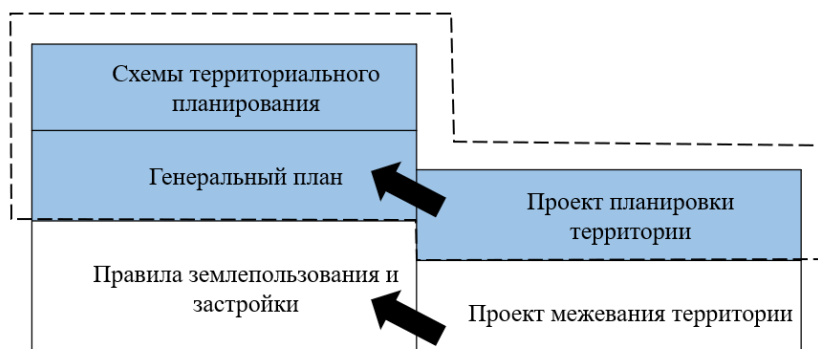


Рис. 1. Схема взаимосвязей документов в системе градостроительной деятельности

Схемы территориального планирования и генеральный план образуют верхний уровень – стратегическое целеполагание. Правила землепользования и застройки (ПЗЗ) располагаются на другом уровне, замыкая на себя вопросы градостроительного зонирования и правового режима использования земельных участков. Между этими двумя уровнями, в «переходной зоне», находятся проект планировки территории (ППТ) и проект межевания территории (ПМТ). В свою очередь проект планировки территории выступает связующим звеном, которое: принимает целевые установки от генерального плана, учитывает градостроительные регламенты, заданные ПЗЗ (виды разрешенного использования, предельные параметры застройки) и одновременно формирует планировочную структуру, которая затем может уточняться или корректироваться при разработке ПМТ.

Таким образом, связи между уровнями носят не чисто вертикальный, а матричный (сетевой) характер. Генеральный план влияет на ПЗЗ, но и ПЗЗ мо-

жет обратно влиять на реализацию генерального плана (например, через внесение изменений). ППТ находится на пересечении этих влияний, интегрируя стратегические решения с местными градостроительными регламентами.

Обсуждение

Анализ существующей практики позволяет выделить несколько ключевых недостатков 2D-подхода. Первый – невозможность учета ситуации и рельефа. В двумерных генеральных планах и проектах планировки территории (ППТ) границы функциональных зон и земельных участков отображаются на плоскости без учета рельефа. Как показано в исследовании [3], при подготовке ППТ для села Прокудское Новосибирской области оценка пешеходной доступности объектов социальной инфраструктуры (школ, детских садов) по нормативным радиусам (500 м) в 2D-формате не учитывала реальные маршруты движения, перепады высот и наличие естественных препятствий (овраги, водные объекты и проч.). В результате формально «доступные» объекты оказывались фактически недоступными. Аналогичная проблема описана в работе [4] при планировании строительства водного спортивного сооружения: земельный участок, выбранный по 2D-плану, оказался непригодным из-за перепада высот 37,2 м и уклона 12 градусов (рис. 1 в [4]).

Второй недостаток – разрозненность и противоречивость исходных данных. Формирование ДТП требует интеграции сведений из Единого государственного реестра недвижимости (ЕГРН), информационных систем обеспечения градостроительной деятельности (ИСОГД) и федеральной государственной информационной системы территориального планирования (ФГИС ТП). Однако, как отмечают авторы работы [4], эти данные часто противоречат друг другу. Например, сведения о правилах землепользования и застройки (ПЗЗ) Чеповского сельсовета во ФГИС ТП датированы 26.10.2017 г., а на официальном сайте администрации – 16.05.2025 г. Такая ситуация ставит под сомнение актуальность и достоверность информации, используемой для планирования.

Третий недостаток – отсутствие интеграции с 3D-кадастром. Объекты капитального строительства (ОКС) имеют трехмерную структуру, однако кадастровый учет в России ведется преимущественно в 2D-формате. Как обосновывает А.В. Чернов [5], развитие 3D-кадастра является необходимым вектором развития кадастровой системы, но без перехода ДТП на 3D-формат интеграция этих систем невозможна.

Зарубежные исследования [6] показывают, что детализированные 3D-модели городов (Virtual Singapore, Helsinki 3D+) стали ключевым инструментом для решения градостроительных, экологических и транспортных задач. В России наиболее продвинутым примером является проект «ТОМСК 3D» [7]. Цифровая платформа, разработанная в Томске, позволяет не только визуализировать градостроительные проекты, но и проводить анализ паводковой ситуации, а также вовлекать граждан в процессы «соучаствующего проектирования». Однако, как подчеркивает В.И. Корнев [7], платформа не имеет официального статуса юридически значимого документа территориального планирования.

Практический пример создания пространственной модели территории приведен в работе [4] на примере села Чепош Республики Алтай. Авторами разработана технологическая схема, включающая аэрофотосъемку с БПЛА (DJI Phantom 4 Pro+), геодезическое координирование опорных и контрольных точек, фотограмметрическую обработку в Agisoft Metashape и последующее 3D-моделирование.

На основе анализа источников [1-8] авторами систематизированы основные группы проблем. Первая – нормативно-правовые проблемы. Градостроительный кодекс РФ не содержит требований к разработке 3D-моделей в составе ДТП. Юридический статус 3D-модели (является ли она официальным документом или вспомогательной визуализацией) не определен. Отсутствует также нормативное закрепление требований к точности, форматам данных и уровню детализации (LOD). Аналогичная ситуация наблюдается в кадастровой сфере: несмотря на международный стандарт LADM (Land Administration Domain Model) [8], его адаптация в российское законодательство находится на начальной стадии научной проработки.

Вторая группа проблем – технологические и методические проблемы. На сегодняшний день отсутствует единый национальный стандарт формата пространственных данных для ДТП. Используются различные подходы (лазерное сканирование, фотограмметрия по данным с БПЛА, тахеометрическая съемка), что приводит к несовместимости моделей. Кроме того, как показано в работе Аврунева Е.И., Гармаша В.В., Гоголева Д.В. и Чернова А.В. [4], даже при корректной обработке возможен систематический сдвиг ортофотоплана (в данном случае по оси X), который может остаться незамеченным без контрольных точек.

Третья группа проблем – кадровые проблемы. Подготовка специалистов в области 3D-моделирования для целей территориального планирования практически отсутствует. В государственных и муниципальных учреждениях нет кадров, способных разрабатывать и сопровождать 3D-модели. Существующие образовательные программы по направлениям «Землеустройство и кадастры» и «Градостроительство» требуют серьезной модернизации с включением дисциплин по 3D-моделированию, фотограмметрии и ГИС.

Четвертая группа – экономические проблемы. Создание высокоточной 3D-модели даже для небольшого поселения (как с. Чепош) требует затрат на аэрофотосъемку, геодезическое оборудование, программное обеспечение и квалифицированных исполнителей. Бюджеты большинства муниципальных образований не предусматривают таких расходов.

Предварительные рекомендации и направления дальнейших исследований. Авторы полагают, что переход к 3D-формату в территориальном планировании должен быть поэтапным:

Законодательный этап: внесение изменений в Градостроительный кодекс РФ, закрепляющих возможность (а для крупных городов – обязанность) разработки 3D-моделей в составе ППТ.

Нормативно-технический этап: разработка национального стандарта (ГОСТ Р) на 3D-модели для целей территориального планирования, включая требования к точности, форматам, уровням детализации и метаданным.

Пилотный этап: реализация пилотных проектов в муниципальных образованиях разного типа с государственным софинансированием и публикацией методических рекомендаций.

Образовательный этап: введение в профильных вузах дисциплин по 3D-моделированию, фотограмметрии с БПЛА и работе с цифровыми двойниками территорий.

Заключение

Проведенное исследование позволяет сделать следующие выводы:

Применение 2D-формата при разработке документов территориального планирования приводит к ошибкам, связанным с невозможностью учета рельефа, противоречивостью исходных данных и отсутствием интеграции с 3D-кадастром.

Российский и зарубежный опыт (проекты «ТОМСК 3D», создание пространственной модели с. Чепош) демонстрирует технологическую возможность перехода на 3D-формат.

Основными барьерами внедрения являются нормативно-правовые (отсутствие правового статуса 3D-модели), технологические (отсутствие стандартов), кадровые (дефицит специалистов) и экономические (высокая стоимость реализации).

Переход на 3D-формат требует внесения изменений в законодательство, разработки национальных стандартов, подготовки кадров и финансирования пилотных проектов.

Дальнейшие исследования должны быть направлены на разработку методики подготовки документов территориального планирования в 3D-формате, оценки экономической эффективности внедрения 3D-формата и создание типовых требований к цифровым двойникам муниципальных образований разного типа.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приказ Минстроя России от 25.12.2020 № 866/пр «Об утверждении Концепции проекта цифровизации городского хозяйства «Умный город».
2. Градостроительный кодекс Российской Федерации от 29.12.2004 № 190-ФЗ (ред. от 28.04.2023).
3. Аврунев Е.И., Лаптева А.С., Агеенко Е.С. Перспективы применения 3D-формата для разработки градостроительной документации // Регулирование земельно-имущественных отношений в России. – 2024. Т. 1. С. 32-38.
4. Аврунев Е.И., Гармаш В.В., Гоголев Д.В., Чернов А.В. Разработка технологической схемы создания пространственной модели территориального образования для подготовки документов территориального планирования // Геодезия и аэрофотосъемка. – 2025. (в печати / принята к публикации).

5. Чернов А.В. Трехмерный кадастр – основной вектор развития успешной кадастровой системы. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/trehmernyy-kadastr-osnovnoy-vektor-razvitiya-uspeshnoy-kadaastrovoy-sistemy>
6. Biljecki F., Stoter J., Ledoux H., Zlatanova S., Coltekin A. Applications of 3D City Models: State of the Art Review // ISPRS Int. J. Geo-Inf. – 2015. № 4. С. 2842-2889.
7. Коренев В.И. Использование цифровых технологий и 3D-моделирования в градостроительной деятельности (на примере города Томска) // Вестник ТГАСУ. – 2020. Т. 22. № 6. С. 70-82.
8. Lemmen C., van Oosterom P., Kara A., Kalogianni E. The Land Administration Domain Model (LADM): An Overview // FIG Publication. – 2023. № 84.

© А. С. Лантева, Е. С. Агеенко, 2026

П. О. Лозовский¹✉, А. В. Шабурова¹

Роль организаций как операторов персональных данных

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: lozovskiy.log@mail.ru

Аннотация. Ежегодно в России правовое регулирование защиты персональных данных претерпевает изменения. Вносимые корректировки направлены на совершенствование нормативной базы и обеспечение соответствия высоким международным стандартам. Такая динамика позволяет эффективнее обеспечивать права и свободы граждан, прежде всего – право на неприкосновенность частной жизни. Особое значение в реализации этих гарантий приобретают организации – операторы персональных данных. Именно на них возлагаются обязанности по сбору, хранению, обработке и защите информации. В связи с растущими требованиями к конфиденциальности возникает необходимость детального анализа таких организаций, их функций и ответственности. Настоящая работа посвящена исследованию роли организаций как операторов персональных данных и выявлению проблемных аспектов их деятельности в контексте законодательства Российской Федерации.

Ключевые слова: Персональные данные, информация, защита, интернет, организация

P. O. Lozovsky¹✉, A. V. Shaburova¹

The Role of Organizations as Personal Data Controllers

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: lozovskiy.log@mail.ru

Abstract. Every year, the legal regulation of personal data protection in Russia undergoes changes. The adjustments being introduced are aimed at improving the regulatory framework and ensuring compliance with high international standards. Such dynamics make it possible to more effectively ensure the rights and freedoms of citizens, above all – the right to privacy. Of particular importance in the implementation of these guarantees are organizations acting as personal data controllers. They are entrusted with the obligations to collect, store, process, and protect information. Due to the growing requirements for confidentiality, there is a need for a detailed analysis of such organizations, their functions, and their responsibility. This paper focuses on examining the role of organizations as personal data controllers and identifying problematic aspects of their activities in the context of the legislation of the Russian Federation.

Keywords: Personal data, information, protection, internet, organization

Введение

В процессе оформления трудовых отношений по запросу работодателя сотрудник передает значительный объем документации и заполняет анкеты, содержащие разделы, которые относятся не только к профессиональной деятельности, но и затрагивают аспекты частной жизни: сведения о состоянии здоровья, наличие или отсутствие судимости, биометрические данные. При этом работник мо-

жет возражать против того, чтобы эти сведения становились известными широкому кругу лиц.

В связи с увеличением числа случаев хищения персонифицированной информации личные данные физического лица нуждаются в защите от несанкционированного доступа третьих лиц. В связи с этим проблема обработки и хранения персональных данных работника попадает в сферу особого внимания любой организации. При заключении трудовых отношений с работником организация приобретает статус оператора персональных данных и, принимая на себя обязанности по их защите, становится поднадзорной контролирующим органам [1].

В целях защиты конфиденциальной информации в Российской Федерации действует специальный правовой режим. Для его обеспечения в 2006 году был принят Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Кроме того, в статье 3 указанного Федерального закона закрепляется понятие «конфиденциальность персональных данных». «Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания» [4].

Цель данной научной статьи рассмотреть роль организаций как оператора персональных данных.

Методы и материалы

Развитие компьютерных технологий и глобальной сети Интернет привело к значительному увеличению количества информационных систем и баз данных, которые сегодня охватывают практически все сферы общественной жизни. Параллельно с этим компьютеры и Интернет обеспечили переход к более эффективным и быстрым процедурам сбора, хранения и структурирования персональной информации.

Существуют базы данных социального обеспечения, медицинской информации, правоохранительных органов, государственных, муниципальных информационных систем, компаний выпускающих кредитные карты и мобильные операторы. Организации являются активными потребителями этих данных и имеют решающее значение для успеха многих операций. Они фиксируют привычки, предпочтения и другие модели индивидуальной деятельности, которые помогают им разрабатывать, продвигать и продавать продукты и услуги.

В этой статье мы проанализируем роль организаций защиты персональных данных, при которой конфиденциальность по-прежнему защищена. Описание и анализ обезличивания персональных данных показывают надежную систему, которая может обеспечить такой уровень защиты конфиденциальности, который не мешает правительствам и организациям проводить статистические исследования. Эти данные важны и собираются для статистических целей.

Методами данного исследования является анализ литературы, синтез и обработка результатов анализа.

Результаты

В настоящее время организации в Российской Федерации приходится иметь дело с законами и нормативными актами о защите данных [1-5]. Такая фрагментация представляет собой дорогостоящее административное бремя, которое затрудняет доступ многих организаций, особенно малых и средних, к новым рынкам.

Согласно законодательству Российской Федерации, одной из основных обязанностей всех организаций, включая малые и средние предприятия, выступающие в качестве контролеров или обработчиков данных, является обеспечение безопасности персональных данных [4].

В частности, согласно внутреннему регламенту организаций, безопасность в равной степени охватывает конфиденциальность, целостность и доступность и должна рассматриваться с учетом рисков: чем выше риск, тем более строгие меры должен принимать контролер (для управления риском). Хотя такой подход к оценке рисков не является новой концепцией, было внедрено лишь несколько специальных систем оценки рисков для конфиденциальности, которые в основном сосредоточены на оценке рисков, связанных с персональными данными, и принятии соответствующих мер безопасности [10].

В то время как крупные организации имеют возможность реагировать на эти системы и внедрять их надлежащим образом, малые и средние предприятия не всегда обладают необходимыми знаниями и ресурсами для этого.

На самом деле, во многих случаях малым и средним предприятиям трудно понять конкретные риски, связанные с обработкой персональных данных, а также оценить эти риски и управлять ими, используя формальную методологию. Это может нанести ущерб малым и средним предприятиям, и в то же время затруднить выполнение ими юридических обязательств в соответствии с внутренним регламентом организаций.

На сегодняшний день существуют правовые, организационные, технические и программные методы защиты персональных данных сотрудников в организации [7].

Организационные меры – основа системы защиты персональных данных. К ним относятся:

Назначение ответственного за обработку персональных данных. Эту роль может выполнять кадровый сотрудник, юрист или привлеченная сторонняя организация. На указанное лицо возлагаются следующие функции: контроль за соблюдением правовых требований, разъяснение работникам правил обработки данных, а также рассмотрение обращений граждан по вопросам, связанным с их персональными данными. [11].

Данная мера предполагает четкое определение круга лиц, которым доступ к персональным данным необходим для выполнения должностных обязанностей. Утверждается перечень таких сотрудников, и с каждого из них берется подписка о неразглашении. В зависимости от типа данных и специфики организации к

числу уполномоченных лиц могут относиться руководители подразделений, специалисты определенных отделов или иные сотрудники [15].

Для каждой категории лиц или роли определяется минимальный набор прав, необходимый для выполнения рабочих задач. Например, в ролевой модели управления доступом права предоставляются на основе бизнес-функций, а не личности или стажа сотрудников [6].

Реализация технических мер осуществляется посредством применения средств защиты информации.

В рамках обеспечения информационной безопасности необходимо использование сертифицированных средств защиты. К числу таких средств относятся антивирусы, межсетевые экраны и системы обнаружения вторжений, каждое из которых обязано иметь актуальный сертификат ФСТЭК России либо ФСБ России [19].

Сертификация средств защиты информации проводится государственными и аккредитованными органами, а испытания – специализированными аккредитованными лабораториями, в отдельных случаях – на базе разработчика. Порядок аккредитации регулируется установленными нормативами. Органы сертификации и испытательные центры несут ответственность за корректность процедур, сохранность конфиденциальной информации и соблюдение прав заявителя.

Системы управления доступом (IAM) обеспечивают безопасное управление идентификацией, аутентификацией и авторизацией пользователей в ИТ-среде. Они предусматривают строгую (в том числе двухфакторную) аутентификацию, позволяют точно идентифицировать действия пользователей и предоставляют доступ к данным только уполномоченным лицам по принципу минимально необходимых прав [20].

IAM разграничивает права доступа: сотрудникам предоставляются только необходимые функции (например, просмотр или редактирование), что снижает риск ошибок и обеспечивает стабильную работу. Также в IAM входят компоненты, работающие вместе для обеспечения безопасности и организации процесса:

Защита каналов передачи данных и шифрование. Вся передача персональных данных по открытым каналам связи (в том числе при удаленной работе) должна шифроваться. [12]

Уведомление Роскомнадзора. До начала обработки персональных данных организация обязана уведомить Роскомнадзор о намерении их обрабатывать. Форма уведомления утверждена Приказом Роскомнадзора от 28.10.2022 № 180 [5].

Получение согласия субъекта на обработку данных. Согласие требуется, если это не вытекает из закона или договора. В обязательном порядке согласие нужно для распространения данных, в том числе для публикации на сайте [8].

Заключение договоров с подрядчиками. Если данные передаются на аутсорсинг (например, в облако), договор должен обязывать подрядчика защищать информацию так же, как это делает организация.

Обсуждение

Мы остановимся на управлении идентификацией и доступом (IAM) в облаке как основной мере защиты персональных данных сотрудников.

Выявим основные проблемы данного метода защиты.

Ниже перечислены основные проблемы, с которыми сталкиваются организации при управлении идентификацией и доступом (IAM) в облаке:

1. Управление большим количеством пользователей и устройств.

В облачных средах множество пользователей, устройств и приложений, которым необходим доступ. Отслеживание того, кто и что может делать для каждого пользователя и устройства, может очень быстро стать сложной задачей, особенно по мере роста организации [16].

2. Работа с несколькими облачными провайдерами (мультиоблачная среда).

Многие организации используют более одного облачного сервиса (например, Mail облако, Yandex диск, Google Cloud). Управление доступом на всех этих различных платформах с помощью собственных инструментов IAM может быть сложным и запутанным, а обеспечение согласованности – непростой задачей.

3. Обеспечение надлежащего уровня доступа.

Предоставление пользователям слишком большого доступа рискованно, но предоставление слишком малого доступа может заблокировать работу. Найти правильный баланс (так называемый «минимальный уровень привилегий») и обеспечить обновление доступа по мере изменения ролей – большая проблема.

4. Защита от угроз безопасности.

Облачные системы постоянно подвергаются кибератакам. Система управления идентификацией и доступом (IAM) должна быть достаточно надежной, чтобы предотвратить несанкционированный доступ пользователей, но хакеры постоянно находят новые способы это сделать. Кража учетных данных, фишинг или внутренние угрозы затрудняют эту задачу [14].

Фишинг представляет собой метод социальной инженерии, при котором злоумышленники посредством поддельных электронных сообщений, имитирующих письма банков и иных организаций, побуждают пользователей раскрывать персональные и конфиденциальные данные. Данный вид атак становится все более опасным из-за усложнения методов обмана пользователей [9].

5. Управление жизненным циклом идентификации.

Существенная динамика увольнений и найма в организации накладывает ответственную роль на системы управления. Системы управления идентификацией и доступом (IAM) должны быстро обновляться или удалять доступ, чтобы избежать сохранения старых или некорректных разрешений, создающих риски безопасности [17].

6. Соблюдение нормативных требований и аудит.

Во многих отраслях действуют строгие правила относительно того, кто имеет доступ к каким данным. Системы управления идентификацией и доступом (IAM) должны надлежащим образом отслеживать и регистрировать все доступы, чтобы организации могли доказать соблюдение этих правил во время аудитов.

7. Сложность интеграции.

Система управления идентификацией и доступом (IAM) должна бесперебойно взаимодействовать со множеством различных облачных сервисов, приложений и локальных систем.

Заключение

В целях защиты персональных данных и соблюдения права на неприкосновенность частной жизни организации обязаны создать и обеспечить необходимую техническую и административную инфраструктуру.

Кроме того, им необходимо реализовать все необходимые правовые нормы в отношении действий, которые следует предпринять при получении персональных данных третьими лицами.

Внутренняя сеть организации объединяет все компоненты информационных систем организации и часто предоставляет точки подключения к внешним сетям. Она является как точкой входа, так и средством распространения атак. Поэтому защита внутренней сети имеет решающее значение [12].

Защита персональных данных должна быть интегрирована в цикл ИТ-разработки, начиная с этапа проектирования и для конфигураций по умолчанию, чтобы предоставить субъектам данных лучший контроль над своими данными и ограничить ошибки, потери, несанкционированные изменения или неправильное использование их данных в приложениях.

Любое действие, совершенное по неосторожности и содержащее ошибку, способно повлечь за собой, что неуполномоченные лица получают доступ к персональным данным, нарушая тем самым право субъектов данных на неприкосновенность частной жизни. Кроме того, организации, имеющие доступ к серверам, через которые передается информация, могут иметь доступ к их содержимому или метаданным.

Обработка данных, выполняемая обработчиком от имени контролера, должна быть обеспечена достаточными мерами предосторожности, в частности, с точки зрения безопасности. Оператор данных должен быть осведомлен о деталях мер безопасности, применяемых его обработчиками [18].

Чтобы иметь возможность идентифицировать мошеннический доступ или неправомерное использование персональных данных, а также определить причину инцидента, необходимо регистрировать определенные события, выполняемые в ИТ-системах.

Без принятия дополнительных мер каналы передачи данных (электронная почта, системы обмена мгновенными сообщениями, платформы хранения файлов) не являются безопасными средствами связи для передачи персональных данных [13].

Государство уделяет особое внимание обеспечению защиты персональных данных. Законодательное регулирование охватывает процессы сбора, хранения и обработки данных, включая персональные сведения граждан. Важным направлением является создание систем, обеспечивающих надежную защиту персональных данных, а также формирование сервисов, гарантирующих безопасность

информации граждан в цифровом взаимодействии. Таким образом, персональные данные выступают одновременно объектом регулирования, ресурсом для развития и приоритетом в сфере информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации от 12 декабря 1993 г. (в ред. от 05.10.2022 28.02.2025) [Электронный ресурс]. URL: <http://government.ru/docs/all/98196/> (дата обращения: 05.05.2026).
2. Гражданский Кодекс Российской Федерации от 26.11.2001 №146-ФЗ (в ред. от 08.08.2024) // Гарант [Электронный ресурс]. URL: <http://www.kremlin.ru/acts/bank/17547> (дата обращения: 05.05.2026).
3. Трудовой Кодекс Российской Федерации от 30 декабря 2001 №197-ФЗ (в ред. от 01.03.2026) // Гарант [Электронный ресурс]. URL: <https://docs.cntd.ru/document/901807664> (дата обращения: 05.05.2026).
4. Федеральный Закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 28.02.2025) // Гарант [Электронный ресурс]. URL: <http://www.kremlin.ru/acts/bank/24154> (дата обращения: 05.05.2026).
5. Приказ Роскомнадзора от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных» (ред. от 28.10.2022) // Гарант [Электронный ресурс]. URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=438326> (дата обращения: 05.05.2026).
6. Аверченков, В. И. Защита персональных данных в организации / В.И. Аверченков. - М.: Флинта, 2022. - 682 с.
7. Благодаров, Андрей Витальевич Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем / Благодаров Андрей Витальевич. - М.: Горячая линия - Телеком, 2020. - 134 с.
8. Бойкова, Ольга Феоктистовна Защита персональных данных: касается всех! Практическое пособие. Выпуск № 142 / Бойкова Ольга Феоктистовна. - М.: Либерея, 2018. - 434 с.
9. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников и др. - Москва: Огни, 2021. - 536 с.
10. Информационная безопасность открытых систем. В 2 томах. Том 2. Средства защиты в сетях / С.В. Запечников и др. - Москва: Высшая школа, 2019. - 560 с.
11. Информационная безопасность систем организационного управления. Теоретические основы. В 2 томах. Том 1. - М.: Наука, 2018. - 496 с.
12. Кин, Эндрю Ничего личного. Как социальные сети, поисковые системы и спецслужбы используют наши персональные данные для собственной выгоды / Эндрю Кин. - М.: Альпина Пабlishер, 2021. - 224 с.
13. Мещеряков, Роман Валерьевич Защита персональных данных в организациях здравоохранения: моногр. / Мещеряков Роман Валерьевич. - М.: Горячая линия - Телеком, 2021. - 950 с.
14. Новая парадигма защиты и управления персональными данными в РФ и зарубежных странах в условиях развития систем обработки данных в сети Интернет / Коллектив авторов. - Москва: СИНТЕГ, 2019. - 296 с.
15. Новая парадигма защиты и управления персональными данными. - Москва: Наука, 2022. - 651 с.

16. Право доступа [Электронный ресурс]. URL: https://rt-solar.ru/products/solar_inrights/blog/4636/ (дата обращения: 10.05.2026).
17. Управление идентификацией и доступом. Руководство по IAM для начинающих [Электронный ресурс]. URL: <https://selectel.ru/blog/what-is-iam/> (дата обращения: 10.05.2026).
18. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2023. - 304 с.
19. Федоров, А. В. Информационная безопасность в мировом политическом процессе / А.В. Федоров. - М.: МГИМО-Университет, 2018. - 220 с.
20. Филиппов, П. Б. Использование и защита персональных данных в социальных сетях Интернета / П.Б. Филиппов. - М.: Синергия, 2023. - 106 с.

© П. О. Лозовский, А. В. Шабурова, 2026

А. Я. Маршинина¹✉, В. В. Селифанов¹

Проблемные аспекты разработки и внедрения системы управления информационной безопасностью в IT-компаниях

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: marshinina-a@mail.ru

Аннотация. В статье рассматриваются проблемные аспекты разработки и внедрения системы управления информационной безопасностью в IT-компаниях. Основной проблемой исследования является противоречие между требованиями информационной безопасности и высокой скоростью изменения IT-среды. Целью работы является выявление ключевых организационных, технологических, экономических и кадровых барьеров при внедрении системы управления информационной безопасностью в IT-компанию. В качестве основных методов исследования использованы системный и сравнительный анализ, анализ нормативных документов и обобщение практического опыта внедрения системы управления информационной безопасностью в IT-среде. В результате исследования установлено, что ключевыми проблемами внедрения системы управления информационной безопасностью является низкий уровень интеграции безопасности в процесс разработки, низкая автоматизация контрольных процедур, дефицит квалифицированных кадров и сложности адаптации международных стандартов к динамической IT-среде. Также было установлено, что наиболее эффективным подходом является переход к модели непрерывного обеспечения безопасности, основанной на принципах DevSecOps. Основной вывод работы заключается в том, что успешное внедрение системы управления информационной безопасностью в IT-компанию возможно только при комплексной интеграции безопасности во все процессы разработки, эксплуатации и управления инфраструктурой компании с переходом к гибким и автоматизированным моделям.

Ключевые слова: система управления информационной безопасностью, информационная безопасность, информационные технологии, IT-компания, DevSecOps, кибербезопасность

A. Y. Marshinina¹✉, V. V. Selifanov¹

Problematic Aspects of Developing and Implementing of Information Security Management System Processes in IT Company

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: marshinina-a@mail.ru

Abstract. The article discusses the problematic aspects of developing and implementing an information security management system in IT companies. The main research problem is the contradiction between the requirements of information security and the high rate of change in the IT environment. The goal of the study is to identify the key organizational, technological, economic, and personnel barriers to implementing an information security management system in an IT company. The main research methods used are system and comparative analysis, analysis of regulatory documents, and generalization of practical experience in implementing an information security management system in the IT environment. The study found that the key challenges in implementing an information security management system are the low level of security integration into the development process, the low level of automation of control procedures, the shortage of qualified

personnel, and the difficulties in adapting international standards to a dynamic IT environment. The study also found that the most effective approach is to transition to a continuous security assurance model.

Keywords: information security management system, information security, information technologies, IT companies, DevSecOps, cybersecurity

Введение

В условиях стремительного развития цифровых технологий информационная безопасность становится одним из основных факторов устойчивого функционирования компании. Большие объемы обрабатываемых данных, рост распределенных систем и усиление зависимости бизнеса от IT сферы обуславливает необходимость системного подхода к обеспечению защиты информации в IT-компаниях.

Именно внедрение системы управления информационной безопасностью (здесь и далее СУИБ) позволит сделать обеспечение безопасности системной. СУИБ основаны на международных стандартах и лучших практиках и позволяют сделать информационную безопасность более эффективной.

Согласно стандарту ГОСТ Р ИСО/МЭК 27000-2021, СУИБ является частью общей системы менеджмента организации, основанной на подходе управления рисками. Основной ее целью является создание, внедрение, использование, мониторинг и постоянное улучшение информационной безопасности предприятия [1]. В ГОСТ Р ИСО/МЭК 27001-2021 закреплены основные требования к таким системам. Они включают в себя обязательное документирование процессов, оценку рисков и внедрение определенных мер защиты [2].

Актуальность исследования обусловлена тем, что, несмотря на наличие нормативной базы и большого количества методических материалов, процесс разработки и внедрения СУИБ в IT-компаниях связан с некоторыми сложностями. Эти компании существуют в условиях высоких скоростей изменений. Релизы программного обеспечения могут происходить многократно за сутки, инфраструктура использует подходы Infrastructure as Code, а команды разработки работают по привычным методологиям. В таких условиях классические подходы к внедрению СУИБ часто оказываются недостаточно эффективными.

Исследования А. Д. Назарова указывают на рост числа киберугроз в условиях цифровой трансформации, что требует от организации более гибких и адаптивных механизмов защиты [3].

Н. Ю. Изварина отмечает необходимость комплексного подхода к экономической безопасности, частью которой является информационная безопасность [4].

А. Д. Георгиевский и Ю. Ю. Черемухина также подчеркивают, что внедрение СУИБ в информационную безопасность постоянно необходимо актуализировать под существующие условия в компании [5].

Несмотря на большое количество исследований, остаются незакрытыми вопросы, связанные с применением стандартов СУИБ в IT-компаниях. Слабо рассмотрена интеграция систем в гибкие методологии разработки и оценка эффек-

тивности такого внедрения. Помимо этого, все еще недостаточно изучены организационные барьеры, которые возникают в процессе внедрения СУИБ в организациях.

В качестве цели данного исследования выбран анализ проблемных аспектов разработки и внедрения СУИБ в ИТ-компаниях и формирование основных рекомендаций по устранению с учетом их специфики. Для достижения поставленной цели будут решаться следующие задачи:

- провести анализ существующих подходов к построению СУИБ;
- выявить основные проблемы внедрения СУИБ;
- предложить практические решения, которые будут обеспечивать эффективность функционирования СУИБ.

Методы и материалы

В процессе исследования использовался комплекс научных методов, позволяющих всесторонне проанализировать обозначенную проблему. Проводился анализ нормативно-правовой базы, позволяющий определить основные требования к построению СУИБ. Благодаря сравнительному анализу научных публикаций, были выявлены общие тенденции различия в подходах к внедрению СУИБ. Через системный анализ была рассмотрена СУИБ как комплексная система, включающая организационный, технический и управленческие аспекты. Благодаря этому выявлена взаимосвязь между различными компонентами системы и определены основные точки возникновения проблем.

Были проанализированы национальные стандарты РФ, связанные с СУИБ - ГОСТ Р ИСО/МЭК 27002-2012, ГОСТ Р ИСО/МЭК 27001-2006, ГОСТ Р ИСО/МЭК 27005-2010.

Помимо этого, использовался метод кейс-стади, демонстрирующий практический опыт внедрения СУИБ в ИТ-компаниях.

Результаты

В ходе проведенного исследования были обозначены основные группы проблем, которые возникают при разработке и внедрении СУИБ в ИТ-компаниях.

К числу наиболее значимых относятся организационные проблемы. Во многих компаниях наблюдается недостаточно вовлеченность в процесс как руководства, так и сотрудников. Этот фактор делает внедрение СУИБ формальным процессом. Система существует лишь на уровне документации, не отражая реальные бизнес-процессы. Также наблюдается сопротивление со стороны персонала, связанное с увеличением количества регламентов и ограничений. Команды разработки зачастую привыкли работать по Agile методологиям и ориентированы на быстрый запуск функционала [6]. В то время как СУИБ требует формализации процессов и соблюдение определенных регламентов и времени. Согласно статистике, внедрение СУИБ в компании требует от 12–18 месяцев [7]. Это приводит к сопротивлению со стороны сотрудников и попыткам обхода мер безопасности. Также было установлено, что большая часть проблем возникает на этапе интеграции уже в существующие бизнес-процессы. Компании необходимо перестра-

ивать процессы, что требует дополнительных ресурсов и времени. И этот момент также может снова вызвать сопротивление со стороны персонала.

Также возникают проблемы при интеграции СУИБ в текущие DevOps-процессы. ИТ-компании функционируют на основе DevSecOps подхода, который предполагает внедрение механизма безопасности на всех этапах жизненного цикла разработки [6].

Наглядно представлено на рисунке (Рис. 1).



Рис. 1. Интеграция СУИБ в жизненный цикл разработки

Но на практике этот процесс сталкивается с определенными трудностями:

- внедрение автоматизированных инструментов онлайн анализа кода (SAST, DAST);
- обеспечение безопасности зависимостей;
- защита CI/CD-пайплайнов от компрометации;
- управление «секретами» (ключами, токенами, паролями) [8].

Технологические проблемы проявляются в момент интеграции СУИБ в уже существующую инфраструктуру ИТ. В разных ИТ-компаниях используются разные программные решения, облачные сервисы и распределенные системы, которые не позволяют быстро внедрять единые стандарты безопасности. Дополнением выступает и быстрое развитие технологий, требующих постоянного обновления средств защиты.

В ряде ИТ-компаний применяется модель разделения ответственности, при которой функции по обеспечению информационной безопасности распределяются между облачным провайдером и самой организацией. В таком случае особенно важно определить зоны ответственности каждой стороны и выстроить понятную систему контроля доступа.

Серьезным ограничением при внедрении СУИБ остается экономический фактор. Затраты связаны не только с внедрением самой системы, но и с ее встраиванием в уже действующие автоматизированные процессы компании. Это, как правило, увеличивает общий объем инвестиций, поскольку дополнительные ресурсы требуются также на обучение сотрудников и адаптацию рабочих процессов.

Также имеют место быть и методологические проблемы. Они обусловлены тем, что международные стандарты в области информационной безопасности не всегда в полной мере учитывают особенности деятельности ИТ-компаний. Обычно такие стандарты разрабатываются как универсальные и поэтому слабо соотносятся с гибкими подходами к разработке, включая Agile и DevOps. Таким образом, компаниям необходимо самостоятельно подстраивать требования, что значительно увеличивает сложность внедрения [10].

Еще одной существенной проблемой является дефицит квалифицированных специалистов, способных участвовать во внедрении и сопровождении СУИБ. Без автоматизации процессов, выращивания кадров внутри компании и упрощения регуляций внедрение СУИБ рискует остаться формальным: компания тратит бюджеты, но остается уязвимой к реальным угрозам из-за нехватки экспертизы. Согласно статистическим данным, в 2025 году 88% компаний столкнулись с нехваткой специалистов в сфере ИБ [11]. При этом спрос на квалифицированные кадры продолжает существенно опережать предложение, что ведет к росту расходов на их поиск, привлечение и удержание сотрудников.

Обсуждение

Полученные результаты подтверждают выводы исследователей о том, что внедрение СУИБ является важным, сложным и многоэтапным процессом.

Так А. Д. Назарова подчеркивает, что в цифровой трансформации возрастает значение гибкости и адаптивности систем информационной безопасности [3]. Это согласуется с обозначенными в ходе исследования проблемами, связанными с адаптацией стандартов.

В сравнении с работами авторов, которые ориентированы на экономическую безопасность организации, было выявлено, что в ИТ-компаниях на первый план выходят технологические и организационные аспекты.

В случаях, когда внедрение новой системы воспринимается как препятствие и будет обходиться специалистами, она не будет эффективно реализована. Внедрение различных концепций требует значительных изменений в организационной культуре и в процессах в целом.

Также важным является использование инструментов автоматического мониторинга и реагирования для обеспечения безопасности в условиях высокой скорости изменения ИТ-сферы.

Заключение

Проведенное исследование показало, что разработка и внедрение СУИБ в ИТ-компаниях сопровождаются рядом как объективных, так и управленческих

трудностей, связанных со спецификой применяемых стандартных моделей, особенностями внутренних информационных систем и условиями функционирования современной ИТ-среды

Основными проблемами являются конфликт между необходимостью высокой скорости разработки и эксплуатации решений и соблюдением требований информационной безопасности, сложности интеграции СУИБ в DevOps процессы, риски, связанные с облачными инфраструктурами, и нехватка квалифицированных специалистов. Для повышения эффективности СУИБ в ИТ-компаниях рекомендуется внедрять принципы DevSecOps, автоматизировать процессы контроля безопасности, интегрировать инструменты безопасности CI/CD, развивать культуру информационной безопасности в командах разработки и совершенствовать механизмы управления доступами и защиту конфиденциальных данных. Для минимизации указанных проблем необходимо сочетать стратегический подход (дорожная карта, цикл PDCA, управление рисками) с технической согласованностью решений и регулярной оценкой эффективности системы через аудиты и метрики.

Перспективным направлением дальнейших исследований видятся разработка адаптивных модулей СУИБ, предназначенных для динамично изменяющихся сред, в которых функционируют ИТ-компании.

Таким образом, успешное внедрение СУИБ в ИТ-компании возможно только при переходе от преимущественно статических моделей управления безопасностью к гибким, интегрированным и автоматизированным подходам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р ИСО/МЭК 27000-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. - М.: Российский институт стандартизации, 2021.
2. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. - М.: Российский институт стандартизации, 2021. – С. 1-8.
3. Назарова А. Д. Вызовы и решения в области кибербезопасности в эпоху цифровой трансформации / Назарова А. Д. // Столыпинский вестник. -2023. – №5. – С. 2212-2214.
4. Изварина Н. Ю. Использование комплексной системы экономической безопасности в практической работе компании / Н. Ю. Изварина, А. Ю. Серикова, А. А. Уварова, А. Г. Голубова // Экономика и бизнес: теория и практика. 2022. – №7 (89). – С. 82-85.
5. Георгиевский А. Д., Черемухина Ю. Ю. Система обеспечения информационной безопасности и внедрение механизмов управления // Компетентность / Competency (Russia). 2025. – № 10.
6. Построение СУИБ: С чего начать? – URL: <https://habr.com/ru/artides/233315/> (дата обращения 18.04.2026). – Текст: электронный.
7. ISO 27001 Framework: Полное руководство + Практические советы. – URL: <https://foundor.ai/ru/blog/iso-27001> (дата обращения 18.04.2026). – Текст: электронный.
8. Ким М. Е. Организация системы управления информационной безопасностью на предприятии / М. Е. Ким, С. Г. Самохвалова // Вестник Амурского государственного университета. Серия: Гуманитарные науки. 2025. – С. 101-105.

9. Дербин Е. А. Информационное противоборство: концептуальные основы обеспечения информационной безопасности : учебное пособие / Е.А. Дербин, А.В. Царегородцев. – Москва : ИНФРА-М, 2024. – 267 с.

10. Платонов В. В. Технологии машинного обучения в кибербезопасности : учебное пособие / В. В. Платонов. - Москва ; Вологда : Инфра-Инженерия, 2024. – 140 с.

11. SC2 Cybersecurity Workforce Study 2025. – URL: <https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study> (дата обращения 18.04.2026). – Текст: электронный.

© А. Я. Мариинина, В. В. Селифанов, 2026

Н. А. Мжельский¹✉, Т. Н. Хацевич^{1,2}

Анализ оптических систем современных миниатюрных объективов для камер смартфонов

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация

² ООО «Оптическое Расчетное Бюро», г. Новосибирск, Российская Федерация
e-mail: nikolayandreevi4@mail.ru

Аннотация. В статье рассматривается анализ оптических систем современных миниатюрных объективов для камер смартфонов, которые являются одним из ключевых направлений развития прикладной оптоэлектроники. Актуальность работы обусловлена необходимостью обеспечения высокого качества изображения при крайне ограниченных габаритных размерах оптических модулей и росте требований к разрешающей способности, углу поля зрения и светосиле. Целью исследования является выявление закономерностей формирования параметров оптических систем и выбора оптических материалов на основе анализа современных патентных решений. В качестве методов исследования использован сравнительный анализ патентных разработок в области миниатюрных объективов, включающий систематизацию параметров оптических систем, исследование используемых оптических материалов. Обработка данных выполнялась с использованием табличных методов и компьютерного анализа. В результате исследования установлено, что фокусные расстояния объективов находятся в диапазоне от 1,46 до 5,59 мм; относительные отверстия – от 1:2,29 до 1:1,45; угловые поля – от 70 до 142 градусов; количество линз в объективах – от пяти до девяти. Выявлено 16 марок полимерных материалов, применяемых в объективах сформированной выборки. Среди марок флинтовой группы наиболее распространенной является материал с показателем преломления 1,68, коэффициентом средней дисперсии 19,2; среди марок кроновой группы – материал с показателем преломления 1,55; коэффициентом средней дисперсии 56,1.

Ключевые слова: миниатюрный объектив, камера смартфона, широкоугольный объектив, асферические поверхности, оптические полимерные материалы

N. A. Mzhelskiy¹✉, T. N. Khatsevich^{1,2}

Analysis of the Optical Systems of Modern Miniature Smartphone Camera Lenses

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

² Optical Design Office, LLC, Novosibirsk, Russian Federation
e-mail: nikolayandreevi4@mail.ru

Abstract. The article considers the analysis of optical systems of modern miniature lenses for smartphone cameras, which are one of the key areas of development of applied optical engineering. The relevance of the work is due to the need to ensure high image quality with extremely limited dimensions of optical modules and increasing requirements for resolution, field of view angle and aperture ratio. The aim of the study is to identify patterns in the formation of optical system parameters and the selection of optical materials based on the analysis of modern patent solutions.

The research methods used are a comparative analysis of patent developments in the field of miniature lenses, including the systematization of optical system parameters, and the study of the optical materials used. Data was processed using tabular methods and computer analysis. As a result of the study, it was established that the focal lengths of the lenses are in the range from 1,46 to 5,59 mm; relative apertures - from 1: 2,29 to 1: 1,45; angular fields - from 70 to 142 degrees; the number of lenses in the lenses is from five to nine. Sixteen grades of polymer materials used in the lenses in the sample were identified. Among the flint grades, the most common is a material with a refractive index of 1,68 and a mean dispersion coefficient of 19,2; among the crown grades, the most common is a material with a refractive index of 1,55 and a mean dispersion coefficient of 56,1.

Keywords: miniature optical lens, smartphone imaging system, wide-angle lens, aspheric surfaces, polymer optical materials

Введение

За четвертьвековую историю возникновения и совершенствования объективы для камер смартфонов вошли в число ключевых направлений развития прикладной оплотехники. К оптическим системам объективов современных смартфонов предъявляются высокие требования к качеству формируемого изображения, включая высокую разрешающую способность, широкое угловое поле зрения, низкий уровень aberrаций, при крайне ограниченных габаритных размерах оптического модуля. Это обуславливает необходимость разработки и совершенствования миниатюрных объективов, способных обеспечивать высокие оптические характеристики в условиях жестких конструктивных ограничений [1].

Развитие объективов для камер смартфонов сопровождается активной патентной деятельностью ведущих мировых компаний, что отражает интенсивный поиск оптимальных конструктивных и оптических решений. В современных патентных документах [2-12] целевыми показателями разработок выступают: поиск оптимального дизайна асферических линз, образующих оптическую систему, включая их количество и используемые материалы, повышение качества изображения, уменьшение габаритных размеров оптической системы, повышении углового поля и относительного отверстия.

Учитывая большое количество существующих решений, нашедших отражение в патентной литературе, представляется актуальным провести их сравнительный анализ, позволяющий выявить общие тенденции развития, определить наиболее часто применяемые материалы для линз объективов, эффективные конструктивные приемы в дизайне оптических схем. В частности, представляет интерес сопоставление таких параметров, как фокусное расстояние, размер изображения, размер используемого совместно с объективом приемника излучений, сопоставление частотно-контрастных характеристик и дисторсии.

Цель статьи – представить результаты анализа оптических систем миниатюрных объективов для камер смартфонов по ограниченной выборке патентных решений.

Методы и материалы

В качестве исходных данных для проведения сравнительного анализа использованы современные патентные разработки в области миниатюрных объек-

тивов для камер смартфонов, опубликованные в 2019–2024 гг. [3, 4], [7-10], [12-15]. Отбор патентов осуществлялся по критерию принадлежности к классу МПК G02B (оптические системы и элементы), а также наличия описания оптической схемы и параметров системы.

Для анализа была сформирована выборка из 11 патентов, в которой анализировались основные параметры оптических систем, включая фокусное расстояние, формат фотоприемника, конструктивные особенности объективов. Обработка данных выполнялась с использованием табличного процессора Microsoft Excel. Для удобства анализа основные характеристики объективов представлены в табл. 1.

Таблица 1 – Технические характеристики миниатюрных объективов

№	f' , мм	$f':D$	2ω , градус	Формат приемника из- лучений	Общая длина, мм	Коли- чество линз	Год	Источник
1	2,4	2,00	95,0	—	4,80	5	2019	[15]
2	5,29	1,45	79,4	1/1,79"	7,25	7	2022	[3]
3	4,5	1,90	78,6	1/1,46"	4,07	5	2022	[13]
4	4,53	—	78,6	1/2,12"	5,50	8	2022	[4]
5	6,61	—	82,4	1/1,34"	7,80	8	2023	[7]
6	1,46	2,29	142,2	1/2,37"	5,74	6	2023	[6]
7	5,49	1,85	79,0	1/2,32"	6,10	6	2023	[12]
8	6,92	—	85,3	1/1,28"	8,00	9	2024	[14]
9	3,51	—	70,0	1/2,38"	3,98	7	2024	[10]
10	3,39	1,78	82,2	—	4,28	5	2024	[8]
11	4,92	—	77,4	1/2,02"	5,55	7	2024	[9]

Оценка изображающих характеристик объективов проводилась на основе анализа графиков частотно-контрастной характеристики (ЧКХ) и дисторсии, представленных в патентных документах [3, 4], [6-10], [12-15]. Для обеспечения сопоставимости результатов выполнено сравнение характеристик для различных оптических систем при близких значениях поля зрения и формата матрицы.

Сравнительный анализ включал сопоставление параметров оптических систем и оценку влияния конструктивных решений на качество изображения. Особое внимание уделялось применению асферических поверхностей, распределению оптической силы между линзовыми элементами и особенностям построения многолинзовых систем.

Для анализа используемых оптических материалов были изучены патентные источники, содержащие данные о параметрах линзовых элементов миниатюрных объективов. Из описаний оптических систем извлекались значения показателя преломления и коэффициента средней дисперсии (числа Аббе), применяемых в линзах материалов. На основе полученных данных была сформирована выборка, включающая уникальные комбинации оптических параметров материалов. В случаях повторения одинаковых значений показателя преломления и

числа Аббе в различных патентных решениях такие материалы учитывались как идентичные по своим оптическим характеристикам. Для наглядного представления распределения материалов построен график зависимости показателя преломления и коэффициента средней дисперсии (диаграмма Аббе). Полученная выборка отражает совокупность материалов, применяемых в современных миниатюрных объективах.

Результаты и обсуждения

В табл.2 представлены основные оптические характеристики органических оптических стекол (полимерных материалов), используемых в оптических системах миниатюрных объективов для смартфонов, включенных в исследуемую патентную выборку [2-15].

Таблица 2 – Оптические характеристики полимерных материалов

Материал	m1	m2	m3	m4	m5	m6	m7	m8
Показатель преломления	1,55	1,68	1,54	1,70	1,62	1,61	1,75	1,72
Число Аббе	56,10	19,2	55,9	30,3	60,3	61,2	44,9	29,6
Материал	m9	m10	m11	m12	m13	m14	m15	m16
Показатель преломления	1,65	1,67	1,64	1,54	1,62	1,64	1,60	1,59
Число Аббе	23,5	20,4	23,5	55,7	25,9	24,0	29,89	32,92

Поскольку в описании патентов часто отсутствуют названия марок полимерных материалов, а приводятся только их основные оптические характеристики, то в табл.2 используемым материалам присвоены условные обозначения: m1...m16. Положение материалов на диаграмме Аббе иллюстрирует рис.1.

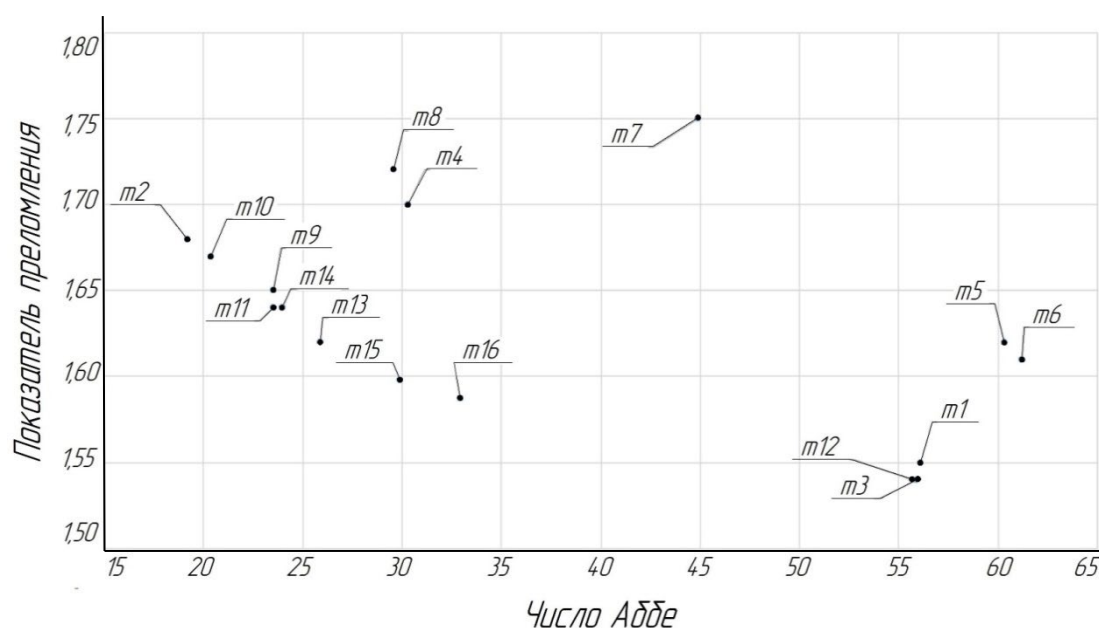


Рис. 1. Оптические характеристики 16 полимерных материалов, применяемых в оптических системах объективов для смартфонов по патентам [2-12]

Распределение материалов на диаграмме Аббе позволяет четко выделить среди них две группы: кроновую группу из 5 марок, и флинттовую группу из 11 марок материалов. При этом показатели преломления материалов находятся в диапазоне от 1,55 до 1,72, а диапазон коэффициентов средней дисперсии составляет от 19,2 до 61,2.

В целом при общем количестве оптических элементов, превышающем 66, число материалов составляет 16. Установлено, что одни и те же комбинации марок материалов повторяются в различных патентных решениях. Диаграмма, приведенная на рис.2, иллюстрирует частоту использования конкретных материалов в анализируемой выборке патентов.

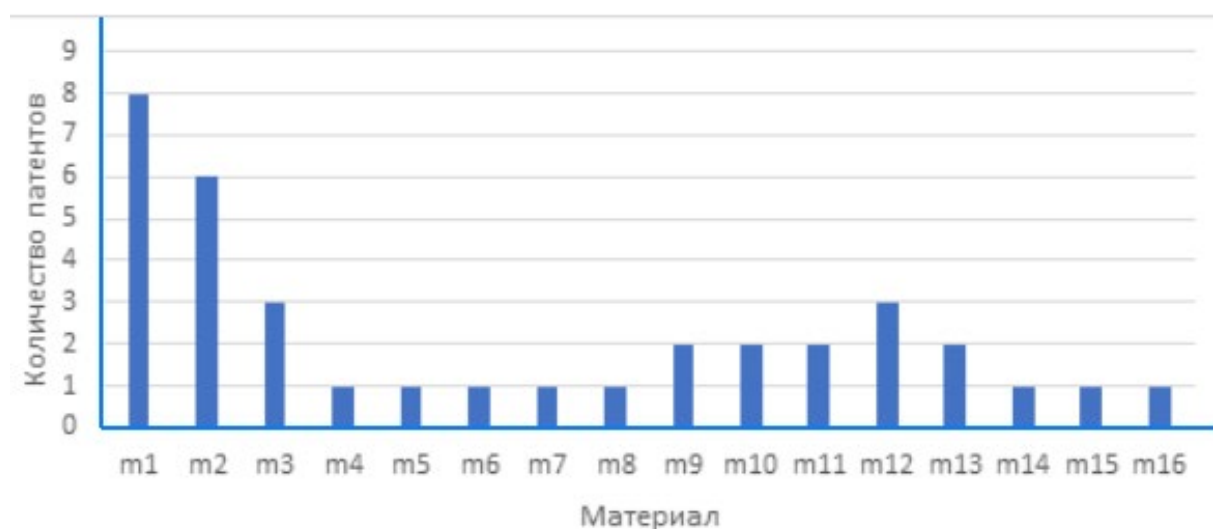


Рис. 2. Частота использования материалов в оптических системах

Положение марок материалов m1, m2, наиболее часто используемых в исследуемой выборке патентов, на диаграмме, приведенной на рис.1, свидетельствует о том, что они составляют устойчивую ахроматическую пару среди полимерных материалов, применяемых в оптических системах миниатюрных объективов. Общее количество марок материалов в конкретной оптической системе в 80% патентных решений составляет четыре-пять, но имеются оптические системы, построенные только из марок m1 и m2 [2, 4]. Сопоставление оптических характеристик марок m1 и m2 с известными марками полимерных материалов различных производителей позволило найти наиболее близкие к ним: это EP10000 и APL5014C (Япония).

Таким образом, в современных миниатюрных объективах применяется ограниченный набор марок полимерных оптических материалов, обусловленный их технологическими свойствами и оптическими характеристиками. Наблюдаемая повторяемость параметров материалов указывает на наличие устойчивых оптимальных решений, используемых при проектировании объективов для камер смартфонов.

В работе [1] приведен ретроспективный анализ оптических систем миниатюрных объективов для мобильных телефонов, на основании которого составлена табл.3, отражающая изменение оптических характеристик объективов.

Таблица 3 – Развитие оптических схем миниатюрных объективов

Тип объектива	Год	Эквивалентное фокусное расстояние, мм	Угловое поле зрения, градус	Диафрагменное число	Количество линз
Широкоугольный	2004	35	62	2,9	3
Широкоугольный	2008	28	75	2,6	5
Широкоугольный	2012	28	75	2,2	6
Телеобъектив	2016	55	42	2,4	5
Широкоугольный	2016	28	75	1,7	6
Телеобъектив	2020	28	38	2,8	5
Широкоугольный	2020	65	75	1,7	6
Сверхширокоугольный	2020	15	120	2,1	6

В качестве фокусного расстояния в табл. 3 приведены значения, эквивалентные по угловым полям объективу, сопрягаемому с традиционным для фотографической оптики приемником – пленкой формата 35 мм.

Информация, приведенная в табл.3, подтверждает, что развитие оптических систем миниатюрных объективов направлено на расширение углового поля и светосилы объективов. В оптических системах до 2020 г. количество линз в объективах не превышало 6. По мере применения в камерах мобильных телефонов приемников большого размера количество линз увеличивается до девяти из-за необходимости коррекции аберраций при расширении углового поля в пространстве предметов.

Оптический дизайн объективов для смартфонов отражает смену парадигмы в фундаментальной компоновке объективов фотографической оптики [1]. Разработчик оптических систем Д. Шейфер в [16] отмечает следующее: «Мой вывод из этого исследования заключается в том, что в обычных моделях мобильных телефонов с очень волнистой асферикой используются аберрации чрезвычайно высокого порядка для компенсации неисправимых аберраций более низкого порядка из-за неоптимального распределения третьего и пятого порядков внутри конструкций».

Анализ оптических систем, приведенных в анализируемой выборке (табл.1), свидетельствует, что при проектировании особое внимание уделяется развитию широкоугольных объективов, что приводит к увеличению углов поля зрения при одновременном росте аберраций. Это требует применения более сложных многолинзовых схем и использования асферических поверхностей. В современных оптических системах миниатюрных объективов большинство преломляющих поверхностей являются асферическими, многие из которых имеют немонотонный профиль с несколькими точками перегиба.

На рис. 3 представлены результаты моделирования оптических систем двух объективов, представленных в патентах [6, 15].

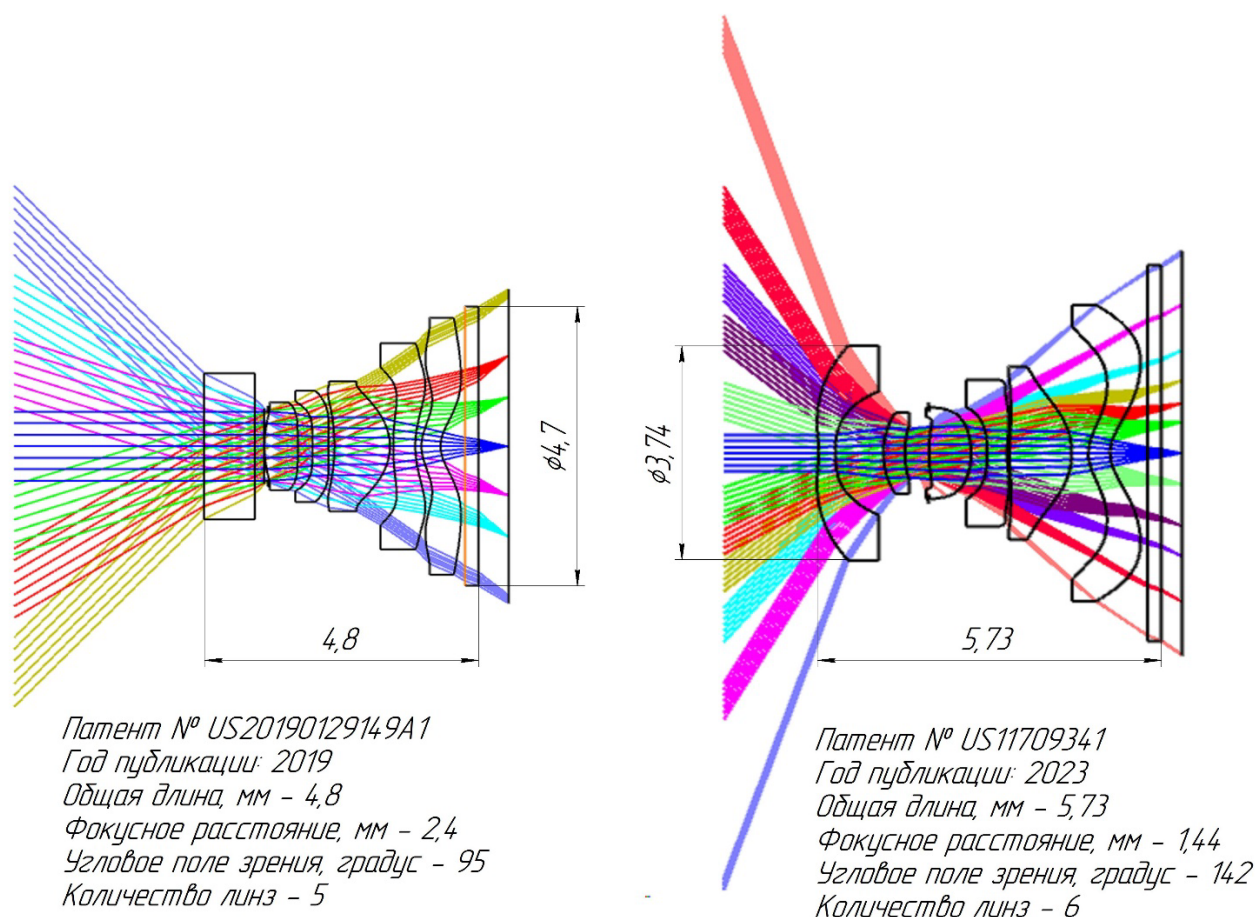


Рис.3. Примеры оптических схем миниатюрных объективов:
 а) US 2019/01,291,49 A1 [15]; б) US 11,709,341 B2 [6]

Для уменьшения диаметра первой линзы в оптической системе, приведенной на рис. 3 а, апертурная диафрагма расположена на первой линзе, что приводит к несимметричному расположению линзовых компонентов относительно апертурной диафрагмы и требует дополнительных усилий по коррекции хроматизма увеличения и aberrаций широких наклонных пучков. Все преломляющие поверхности являются асферическими с коэффициентами асферик до двадцатого порядка. Форма последних линз в системе такова, что их оптическая сила по мере удаления от оптической оси меняет знак: от отрицательной в центре до положительной на зоне и краю линзы. Такая форма линз получила образное название «крыло чайки». Общая длина вдоль оптической оси от первой поверхности защитного стекла до плоскости чувствительных элементов приемника излучений составляет 4,8 мм.

В оптической системе, приведенной на рис. 3 б, со сверхширокоугольным полем зрения апертурная диафрагма расположена внутри системы, что привело к увеличению диаметра первой линзы до 3,74 мм. Общая длина вдоль оптической оси от первой поверхности защитного стекла до плоскости чувствительных элементов приемника излучений составляет 5,73 мм. Для коррекции полевых аберраций также используется профиль типа «крыла чайки». Все преломляющие поверхности в системе являются асферическими.

Асферический профиль поверхностей становится более сложным, что позволяет компенсировать монохроматические аберрации (такие как сферическую аберрацию, кому, астигматизм, кривизну поля) более высоких порядков. Это особенно важно, когда речь идет о широкоугольных или сверхширокоугольных объективах, которые на текущий момент активно используются в современных смартфонах и с каждым годом требования к ним становятся все более жестче.

На основании анализа качества изображения, формируемого оптическими системами миниатюрных объективов для мобильных телефонов, приведенных в исследуемой выборке патентов, установлено, что оценка качества изображения проводится по ЧКХ в диапазоне пространственных частот до 200 лин/мм. Коэффициент передачи контраста на указанной пространственной частоте составляет от 0,25 до 0,65.

Можно отметить, что развитие оптических систем объективов камер смартфонов характеризуется переходом к более сложным многолинзовым системам, обеспечивающим баланс между компактностью конструкции и высоким качеством изображения.

Заключение

На основании проведенного анализа оптических систем объективов для камер смартфонов, включенных в составленную ограниченную выборку патентных решений, датированных 2019–2024 гг., установлено, что фокусные расстояния объективов находятся в диапазоне от 1,46 до 5,59 мм; относительные отверстия – от 1:2,29 до 1:1,45; угловые поля – от 70 до 142 градусов; количество линз в объективах – от пяти до девяти. При этом все преломляющие поверхности являются асферическими, профиль которых является немонотонным с несколькими точками перегибов. Все линзы в оптических системах являются одиночными, без наличия склеенных линз. Выявлено 16 марок полимерных материалов, применяемых в объективах сформированной выборки. Среди марок флинтовой группы наиболее распространенной является материал с показателем преломления 1,68, коэффициентом средней дисперсии 19,2, среди марок кроновой группы – материал с показателем преломления 1,55; коэффициентом средней дисперсии 56,1. Наиболее близкими характеристиками к выявляемым материалам являются марки полимерных материалов EP10000 и APL5014C японского производства.

Для оценки качества изображения, формируемого оптическими системами объективов для камер смартфонов, используется ЧКХ, при этом критерием вы-

ступает значение коэффициента передачи контраста не менее 0,25 на пространственной частоте 200 лин/мм.

Полученные в процессе исследования данные будут полезны для перспективных разработок оптических систем миниатюрных объективов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Blahnik, V., Schindelbeck, O. Smartphone imaging technology and its application // Journal of Optical Engineering. – 2021. – Vol. 10, № 3. – P. 145-232.
2. US 11,927,727 B2. Camera apparatus : пат. US 11,927,727 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 12.03.2024. – 42 с.
3. US 11,237,366 B2. Optical imaging lens system : пат. US 11,237,366 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 01.02.2022. – 32 с.
4. US 11,460,671 B2. Optical imaging lens system : пат. US 11,460,671 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 04.10.2022. – 35 с.
5. US 11,971,523 B2. Optical imaging system : пат. US 11,971,523 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 30.04.2024. – 39 с.
6. US 11,709,341 B2. Imaging lens module : пат. US 11,709,341 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 18.07.2023. – 37 с.
7. US 11,579,406 B2. Optical imaging lens assembly : пат. US 11,579,406 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 14.02.2023. – 41 с.
8. US 12,000,992 B2. Camera optical system : пат. US 12,000,992 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 11.06.2024. – 44 с.
9. US 12,055,686 B2. Optical lens module : пат. US 12,055,686 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 30.07.2024. – 38 с.
10. US 12,135,409 B2. Wide-angle optical imaging system : пат. US 12,135,409 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 22.10.2024. – 43 с.
11. US 11,662,556 B2. Imaging lens system : пат. US 11,662,556 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 30.05.2023. – 36 с.
12. US 11,733,487 B2. Optical imaging system : пат. US 11,733,487 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 22.08.2023. – 35 с.
13. US 11,487,090 B2. Optical imaging lens system : пат. US 11,487,090 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 01.11.2022. – 38 с.
14. US 12,111,448 B2. Optical imaging lens system : пат. US 12,111,448 B2, United States. МПК: G02B 13/00; G02B 9/60; H04N 5/225. – Оpubл. 08.10.2024. – 36 с.
15. Yao, Yuhong. Optical system and imaging device: пат. US 2019/0129149 A1, United States. МПК: G02B 13/0045; G02B 5/208; H04N 5/2254; G02B 9/60; заявл. 31.08.2018; опубл. 02.05.2019. – 40 с.
16. Shafer, D. A New Theory of Cell Phone Lenses [Электронный ресурс] : презентация. – 2019. – Режим доступа: <https://de.slideshare.net/operacrazy/a-new-theory-of-cell-phone-lenses> (дата обращения: 30.03.2026).

© Н. А. Мжельский, Т. Н. Хацевич, 2026

М. Д. Михайлов^{1✉}, Е. А. Усанькова¹

Оптимизация процессов жизненного цикла инновационной продукции в условиях цифровой экономики

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: mihajlovmi hail90@gmail.com

Аннотация. В статье проводится исследование методов оптимизации процессов жизненного цикла инновационной продукции в условиях цифровой экономики. Рассмотрены структурно-стадийные особенности жизненного цикла инноваций, методы оценки экономической эффективности инновационных проектов, модели управления стоимостью жизненного цикла продукции и механизмы интегрированной логистической поддержки. Исследование основано на анализе научных работ, посвященных цифровизации инновационных процессов, CALS-технологиям, PLM- и ERP-системам, а также методам экономико-математического моделирования. Установлено, что основная доля затрат инновационной продукции формируется на стадии эксплуатации. Предложена интегрированная модель оптимизации жизненного цикла инновационной продукции, основанная на цифровом управлении данными, логистической поддержке и управлении стоимостью жизненного цикла. Практический результат применения модели выражается в сокращении сроков вывода продукции на рынок, снижении эксплуатационных затрат и повышении коэффициента готовности продукции.

Ключевые слова: инновационная продукция, жизненный цикл, цифровизация, PLM, ERP, CALS-технологии, стоимость жизненного цикла

M. D. Mikhailov^{1✉}, E. A. Usankova¹

Optimizing the life Cycle Processes of Innovative Products in the Digital Economy

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: mihajlovmi hail90@gmail.com

Abstract. The article examines the methods of optimizing the processes of the life cycle of innovative products in the digital economy. The structural and stage-based features of the innovation lifecycle, methods for evaluating the economic effectiveness of innovative projects, models for managing the cost of the product lifecycle, and mechanisms for integrated logistical support are considered. The study is based on an analysis of scientific papers devoted to the digitalization of innovation processes, CALS technologies, PLM and ERP systems, as well as methods of economic and mathematical modeling. It has been established that the main share of the costs of innovative products is formed at the operational stage. An integrated model for optimizing the life cycle of innovative products based on digital data management, logistical support, and lifecycle cost management is proposed. The practical result of using the model is to reduce the time required to bring products to market, reduce operating costs, and increase product availability.

Keywords: innovative products, life cycle, digitalization, PLM, ERP, CALS technologies, life cycle cost

Введение

Развитие инновационной экономики связано с ускорением технологических изменений, ростом затрат на научно-исследовательские работы и сокращение жизненного цикла продукции. Предприятия функционируют в условиях высокой конкуренции, при которой эффективность определяется не только способностью создавать инновационные продукты, но и эффективностью управления всеми стадиями их жизненного цикла.

Большинство предприятий управляют стадиями жизненного цикла продукции разрозненно. Это приводит к росту эксплуатационных затрат, увеличению сроков разработки и снижению устойчивости инновационной деятельности.

Дополнительной проблемой является ускорение морального устаревания инновационной продукции. В цифровой экономике инновационные продукты распространяются значительно быстрее традиционных технологий. В результате предприятия вынуждены сокращать сроки разработки и внедрения продукции, одновременно повышая качество управления жизненным циклом.

Цель исследования заключается в разработке подходов к оптимизации процессов жизненного цикла инновационной продукции на основе интеграции цифровых технологий, логистической поддержки.

Для достижения цели поставлены следующие задачи:

- исследовать структуру жизненного цикла инновационной продукции;
- определить основные источники затрат на различных стадиях жизненного цикла;
- проанализировать методы цифровизации процессов жизненного цикла;
- разработать интегрированную модель оптимизации жизненного цикла инновационного продукта.

Методы и материалы

Исследование основано на анализе научных публикаций, связанных с управлением жизненным циклом инновационной продукции, цифровизации инновационных процессов и логистической поддержке сложной продукции.

В качестве методологической базы использованы:

- системный подход;
- структурно-стадийный анализ;
- методы экономико-математического моделирования;
- методы оценки стоимости жизненного цикла;
- методы логистического анализа.

Жизненный цикл инновационной продукции рассматривается как совокупность взаимосвязанных стадий:

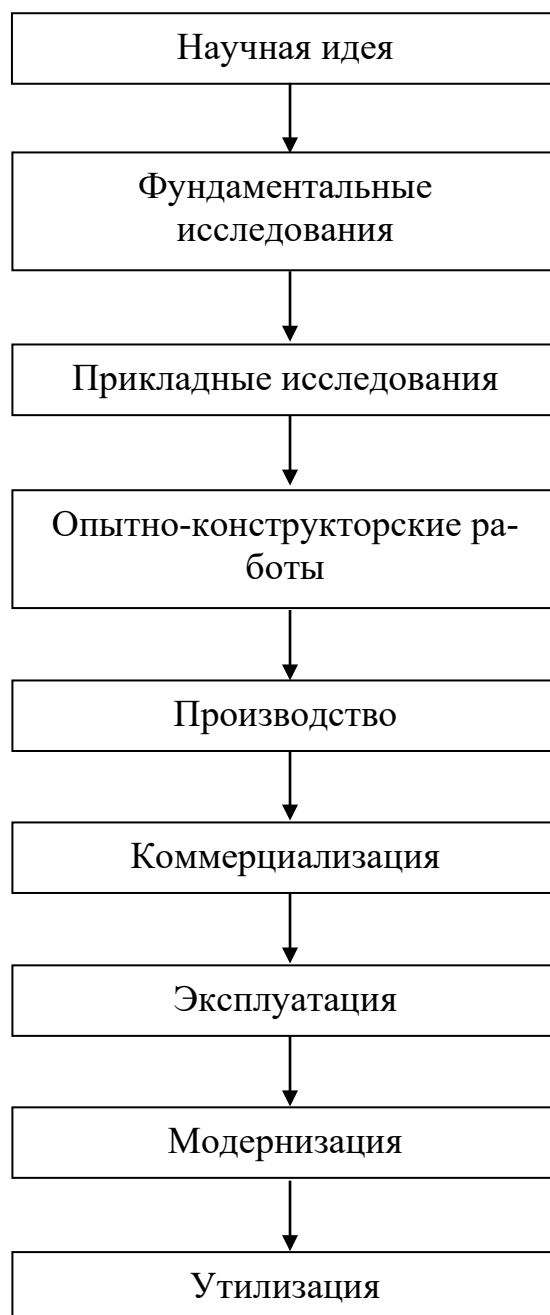


Рис. 1. Стадии жизненного цикла

Исследования Галимнурова А. Ф., Лейберта Т. Б. и Валинуровой Л. С. показывают, что инновационный процесс обладает системностью наличием стадий, а параметров на одной стадии жизненного цикла оказывает влияние на последующие стадии инновационного процесса [1].

Для оценки совокупности затрат используется модель стоимости жизненного цикла продукции:

$$LCC = A + B + \sum_{t=1}^N (C_t + D_t + E_t + F_t + G_t)k_t + H, \quad (1)$$

где A - затраты на разработку и приобретение;

B - транспортные затраты;

C_t - затраты хранения;

D_t - затраты подготовки к эксплуатации;

E_t - эксплуатационные затраты;

F_t - сервисное обслуживание;

G_t - оперативная логистическая поддержка;

H - затраты на утилизацию;

k_t - коэффициент дисконтирования [2].

Для оценки эффективности инновационного проекта применяется показатель чистой приведенной стоимости:

$$NPV = \sum_{t=0}^N \frac{CF_t}{(1+r)^t} - I_0, \quad (2)$$

где CF_t - денежный поток периода; —

r - ставка дисконтирования;

I_0 - объём первоначальных инвестиций.

Для оценки надежности и эффективности логистической поддержки рассматривается коэффициент готовности продукции:

$$K_g = \frac{T_{work}}{T_{work} + T_{repair}} \quad (3)$$

где T_{work} - время функционирования продукции;

T_{repair} - время ремонта [3].

Результаты

Исследование показало, что основная доля затрат инновационной продукции формируется не на стадии разработки, а в процессе эксплуатации продукции.

Таблица 1 – Структура затрат жизненного цикла

Стадии жизненного цикла	Доля затрат инновационной продукции
Разработка и НИОКР	15 %
Производство	25 %
Логистика	10 %
Эксплуатация	40 %
Утилизация	10 %

Полученные данные подтверждают, что более 40 % совокупных затрат формируется на стадии эксплуатации. Следовательно, оптимизация жизненного цикла должна начинаться на стадии проектирования продукции.

Исследования Денискина Ю. И., Дубровина А. В. и Подколзина В. Г. показывают, что традиционные системы менеджмента качества не способны эффективно управлять сложными информационными потоками инновационного производства [4].

Для решения данного вопроса используется:

- CAD/CAE/CAPP-системы;
- PLM-платформы;
- ERP-системы;
- Цифровые двойники;
- Системы аналитики больших данных.

Интеграция цифровых систем жизненного цикла представлена на рис. 2.



Рис. 2. Цифровая модель управления жизненным циклом

Анализ показал, что внедрение PLM- и ERP-систем обеспечивает:

- сокращение сроков разработки продукции;
- снижение количества производственных ошибок;
- повышение точности планирования;

– сокращение времени вывода продукции на рынок;

Для сложной инновационной продукции ключевыми факторами оптимизации является интегрированная логистическая поддержка (ИЛП), основанная на CALS-технологиях.



Рис. 3. Интегрированная логистическая поддержка жизненного цикла продукции

Результаты анализа показали, что внедрение CALS-технологий и ИЛП продукции:

- сократит эксплуатационные расходы на 15-30 %;
- повысит коэффициент готовности продукции;
- снизит время технического обслуживания;
- сократит количество отказов оборудования [3].

На основе проведенного анализа была сформирована интегрированная модель оптимизации жизненного цикла инновационной продукции – рис. 4.

Критерий оптимизации жизненного цикла:

$$F = \min(LCC), K_g \geq K_{norm} \quad (4)$$

где LCC - стоимость жизненного цикла;

K_g - коэффициент готовности;

K_{norm} - нормативный коэффициент готовности.

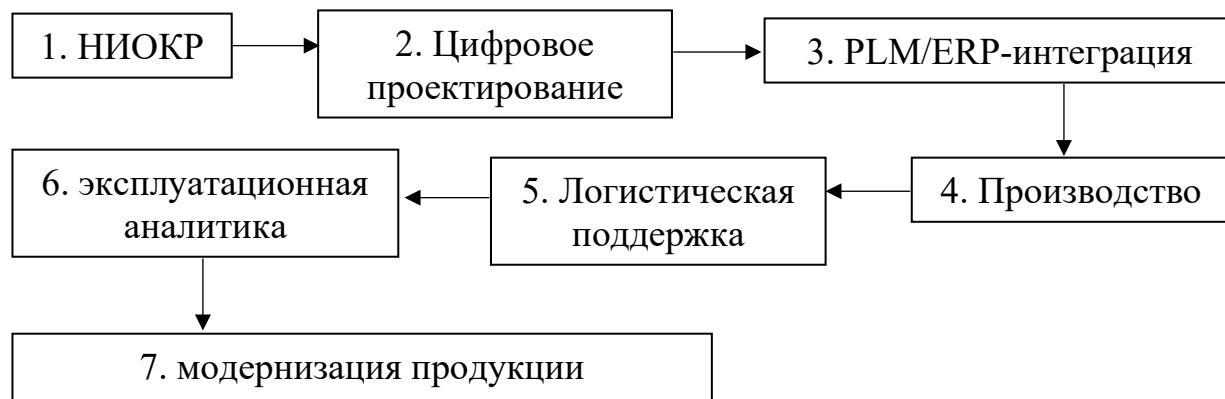


Рис. 4. Интегрированная модель оптимизации жизненного цикла инновационной продукции

Модель показывает, что предприятие должно минимизировать совокупные затраты жизненного цикла без снижения надежности продукции.

Полученные результаты подтверждают, что подходы к управлению инновационной продукцией ориентированы преимущественно на стадии разработки и производства, тогда как основная часть затрат формируется в эксплуатации продукции [2].

Интеграция цифровых систем управления жизненным циклом обеспечивает объединение процессов проектирования, производства, логистики и эксплуатации в единую информационную систему [4,5].

Использование PLM- и ERP-систем обеспечивает непрерывное управление данными о продукции, а CALS-технологии позволяют повысить эффективность сервисного обслуживания и модернизации продукции [3].

Современные инновационные процессы должны учитывать экологические и социальные аспекты устойчивого развития [6].

Шаповалов В. Л. подчеркивает необходимость комплексного исследования всех стадий жизненного цикла инновационной продукции [7].

Аналогичная позиция у Шамина Л. К. и Тутаева М. Ю, рассматривающие инновационный процесс как совокупность связанных стадий развития инноваций [8].

Заключение

Проведенное исследование показало, что оптимизация процессов жизненного цикла инновационной продукции требует перехода от разрозненного управления отдельными стадиями к интегрированной цифровой модели управления.

Основные результаты исследования:

- основная доля затрат инновационной продукции формируется на стадии эксплуатации;
- наиболее эффективной является модель управления, основанная на интеграции PLM- ERP- и CALS-технологий;
- интеграция цифровых систем сокращает сроки разработки и повышает качество управления жизненным циклом продукции;
- использование интегрированной логистической поддержки снижает эксплуатационные расходы и повышает коэффициент готовности продукции;
- предложенная интегрированная модель оптимизация обеспечивает снижение совокупной стоимости жизненного цикла без снижения надежности продукции.

Практическое значение исследование заключается в возможном применении предложенной модели для повышения эффективности управления инновационной продукции на промышленных предприятиях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- 1 Галимнуров А. Ф., Лейберт Т. Б., Валинурова Л. С. Структурно-стадийная концепция жизненного цикла инноваций // Инновации и инвестиции. – 2023. – № 10. – С. 6–10.
- 2 Кобин П. Н. Стратегия управления жизненным циклом инновации как инструмент устойчивого развития организации // Управление инновациями. – 2025. – № 2. – С. 54–60.
- 3 Брицко Г. В. Особенности организации логистической поддержки жизненного цикла сложной инновационной продукции // Вестник Университета. – 2014. – № 12. – С. 5–11.
- 4 Денискин Ю. И., Дубровин А. В., Подколзин В. Г. Управление качеством процессов жизненного цикла инновационной продукции на основе компьютерной системы менеджмента качества // Труды МАИ. – 2017. – № 95.
- 5 Багваби Д. Е., Дубровина Т. А. Теории, концепции и особенности жизненного цикла инновационных продуктов в цифровую эпоху // Прогрессивная экономика. – 2025. – № 7. – С. 104–124.
- 6 Орлова В. А. Специфические особенности и подходы к анализу жизненного цикла устойчивых инноваций // Вестник Академии знаний. – 2024. – № 5 (64). – С. 293–296.
- 7 Шаповалов В. Л. Методы комплексного исследования жизненного цикла продуктовых инноваций // Transport Business in Russia. – 2010. – № 6. – С. 173–176.
- 8 Шамина Л. К., Тутаева М. Ю. Особенности жизненного цикла продуктовой инновации // Научно-технические ведомости СПбГУ ИТМО. – 2012. – № 2. – С. 45–50.

© М. Д. Михайлов, Е. А. Усанькова, 2026

Е. С. Мишечкин¹✉, М. П. Егоренко¹, Н. А. Гурин^{2,3}

Сравнение глубокого шлифования и полирования классическим методом с предлагаемым методом на примере подложек для оптических покрытий лазерных систем

¹ Сибирский государственный университет геосистем и технологий,

г. Новосибирск, Российская Федерация

² Новосибирский приборостроительный завод, г. Новосибирск, Российская Федерация

³ Институт автоматики и электрометрии Сибирского отделения Российской академии наук,

г. Новосибирск, Российская Федерация

e-mail: mishechkines@mail.ru

Аннотация. В работе проведено сравнительное исследование классического метода глубокой шлифовки и полировки и предложенного метода прецизионной обработки оптических подложек для подложек оптических покрытий лазерных систем. Шероховатость поверхности определялась методом теневоего анализа с использованием интерференционного микроскопа Линника. На основе экспериментальных данных установлены зависимости коэффициента рассеяния света и порога лучевой прочности от параметров микрорельефа. Показано, что классический метод приводит к формированию субповерхностных дефектов и повышенной шероховатости, что ограничивает энергетическую стойкость покрытия. Предложенный метод обеспечивает снижение шероховатости поверхности с 2,37 мкм до 0,75 мкм, уменьшение рассеяния света на порядок и увеличение порога лучевой прочности в 1,7–1,8 раза. Полученные результаты демонстрируют перспективность предлагаемого подхода для изготовления оптических элементов, работающих при высоких плотностях лазерного излучения.

Ключевые слова: оптические покрытия для лазерных систем; шероховатость поверхности; коэффициент рассеяния света; порог лучевой прочности; субповерхностные дефекты; полировка оптики; интерференционный микроскоп Линника; оптические материалы; лазерная оптика; микрорельеф поверхности

E. S. Mishechkin¹✉, M. P. Egorenko¹, N. A. Gurin^{2,3}

Comparison of Deep Grinding and Polishing using the Classical Method with the Proposed Method using Laser-Resistant Coatings as an Example

1 Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

2 Novosibirsk Instrument-Making Plant, Novosibirsk, Russian Federation

3 Institute of Automation and Electrometry, Siberian Branch of the Russian Academy of Sciences,

Novosibirsk, Russian Federation

e-mail: mishechkines@mail.ru

Abstract. This paper presents a comparative study of the classical deep grinding and polishing method and the proposed precision machining method for optical substrates used for optical coatings in laser systems. Surface roughness was determined by shadow analysis using a Linnik interference microscope. Based on experimental data, the dependences of the light scattering coefficient and the radiation damage threshold on microrelief parameters were established.

It was shown that the classical method leads to the formation of subsurface defects and increased roughness, which limits the energy resistance of the coating. The proposed method reduces surface roughness from 2,37 μm to 0,75 μm , reduces light scattering by an order of magnitude, and increases the radiation damage threshold by 1,7–1,8 times.

The obtained results demonstrate the potential of the proposed approach for the fabrication of optical elements operating at high laser radiation densities.

Keywords: Optical coatings for laser systems; surface roughness; light scattering coefficient; radiation hardness threshold; subsurface defects; polishing of optics; Linnik interference microscope; optical materials; laser optics; surface microrelief

Введение

В связи с этим возникает необходимость исследования влияния режимов глубокого шлифования–полирования на параметры поверхности оптических деталей, а также разработки методов контроля шероховатости и оценки качества обработки.

В настоящее время повышение качества поверхности оптических деталей является одной из ключевых задач современного оптического производства. Особенно высокие требования предъявляются к деталям, используемым в составе лазерных систем высокой мощности, поскольку состояние поверхностного слоя оказывает непосредственное влияние на оптические потери, стабильность параметров излучения и надежность работы многослойных оптических покрытий.

Современные исследования в области технологии обработки оптических материалов направлены на снижение шероховатости поверхности, уменьшение глубины нарушенного слоя и повышение лучевой прочности оптических элементов. Значительное внимание уделяется совершенствованию процессов глубокого шлифования и полирования, а также исследованию влияния микродефектов поверхности на характеристики оптических покрытий.

В работе Alexei Kozlov, Stavros Demos, David Canning и соавторов исследовалось изменение характеристик многослойных диэлектрических покрытий при длительном воздействии высокоинтенсивного лазерного излучения. Авторами установлено, что наличие поверхностных дефектов и загрязнений приводит к снижению порога лазерного повреждения и ускоренной деградации покрытий [1].

В исследовании Kyle R. Kafka, Brittany Hoffman, Hu Huang и Stavros Demos рассмотрены механизмы лазерного повреждения зеркальных покрытий при взаимодействии лазерного излучения с модельными загрязняющими частицами. Авторы показали, что локальные дефекты поверхности являются концентраторами энергии лазерного излучения и существенно влияют на устойчивость покрытий к лучевому воздействию [2].

В связи с этим актуальной задачей является разработка и исследование методов обработки оптических деталей, обеспечивающих снижение дефектности поверхностного слоя и повышение качества поверхности при сохранении технологической производительности процесса.

Несмотря на развитие технологий обработки оптических деталей, проблема обеспечения высокой однородности поверхностного слоя при сохранении производительности процесса обработки остается актуальной. Традиционные методы глубокого шлифования и полирования не всегда обеспечивают требуемое качество поверхности для многослойных оптических покрытий, применяемых в лазерных системах высокой мощности. Наличие микродефектов, остаточных напряжений и повышенной шероховатости приводит к увеличению рассеяния света и снижению лучевой прочности оптических элементов.

В связи с этим возникает необходимость исследования влияния режимов глубокого шлифования–полирования на параметры поверхности оптических деталей, а также разработки методов контроля шероховатости и оценки качества обработки.

Методы и материалы

Метод обработки заключается в подборе оптимальных режимов глубокого шлифования–полирования, выборе состава связанного абразивного инструмента и последующем анализе влияния технологических параметров на качество поверхности оптических деталей. Основной задачей метода является снижение шероховатости поверхности и глубины нарушенного слоя, обеспечивающих повышение качества многослойных оптических покрытий и улучшение оптических характеристик деталей.

Работа осуществлялась на шлифовальном станке, оснащем алмазным, корундовым и нитрид-бориевым инструментом.

В качестве обрабатываемых материалов выбраны: оптическое стекло (марка К8), кварц, германий.

Параметры обработки определены в соответствии с рекомендациями, содержащимися в источнике [3]:

- скорость вращения шпинделя: от 50 до 150 об/мин;
- давление поводка: от 60 до 100 кг;
- подача инструмента: от 0,5 до 5 мм/мин.

Для решения поставленных задач в работе использовался комплекс экспериментальных, аналитических и расчетных методов исследования, направленных на оценку качества поверхности оптических деталей после глубокого шлифования–полирования.

Исследование параметров поверхности проводилось с применением методов оптической микроскопии и интерференционного контроля. Анализ микрорельефа поверхности выполнялся с использованием интерференционного микроскопа Линника, позволяющего определять параметры шероховатости и выявлять локальные дефекты поверхностного слоя.

Контроль шероховатости поверхности осуществлялся методом теневого анализа микронеровностей при наклонном освещении поверхности. Определение высоты микронеровностей проводилось расчетным методом на основании измерения геометрических параметров тени.

Для обработки экспериментальных данных использовались методы математических вычислений и анализа данных, позволяющие получить зависимости шероховатости поверхности и глубины нарушенного слоя от технологических режимов обработки.

Полученные результаты исследований анализировались сравнительным методом путем сопоставления параметров поверхности, полученных при использовании традиционного и предлагаемого методов глубокого шлифования–полирования.

Интерференционный микроскоп Линника использовался для оценки микро рельефа поверхности. Метод основан на анализе тени, формируемой неровностями поверхности при наклонном освещении. При падении света под углом θ к поверхности микронеровность высотой h создает тень длиной l , которая наблюдается в микроскопе. Геометрическая связь между высотой неровности и длиной тени определяется тригонометрическими соотношениями.

Величина шероховатости определяется по формуле:

$$h = l \times \operatorname{tg} \theta, \quad (1)$$

где h – высота неровности поверхности; l – длина наблюдаемой тени; θ – угол падения света на поверхность.

Сравнительный анализ параметров шероховатости поверхности при обработке оптических деталей, в зависимости от использованных методов, представлен в табл. 1.

Таблица 1 – Расчет шероховатости

№ измерения	Классический метод		Предлагаемый метод		Угол падения света θ , град
	l , мкм	h , мкм	l , мкм	h , мкм	
1	4,0	2,31	1,2	0,69	30°
2	3,5	2,02	1,5	0,87	
3	5,0	2,89	1,1	0,63	
4	4,2	2,42	1,3	0,75	
5	3,8	2,19	1,4	0,81	
Среднее значение	4,1	2,37	1,3	0,75	

Таким образом, применение предлагаемого метода позволяет уменьшить среднюю шероховатость поверхности оптической детали примерно в 3 раза.

Рассеяние света на оптической поверхности определяется параметрами микрорельефа. Для поверхностей с малой шероховатостью используется выражение, согласно которому коэффициент рассеяния света определяется выражением (2):

$$K_p = \left(\frac{4\pi R_q}{\lambda} \right)^2, \quad (2)$$

где K_p – коэффициент рассеяния света; R_q – среднеквадратичная шероховатость; λ – длина волны лазерного излучения.

Расчеты были выполнены при длине волны равной 1064 нм.

Расчет классическим методом, при условии, что длина волны λ равна 1064 нм, а среднеквадратичная шероховатость R_q равна 2,37 мкм, выглядит следующим образом:

$$K_p = \left(\frac{4\pi \cdot 2,37}{1064} \right)^2 = 7,8 \cdot 10^{-4} .$$

Расчет для предлагаемого метода будет выполнен для длины волны λ , равной 1064 нм и среднеквадратичной шероховатости $\sigma = 0,75$ мкм, и выглядит как:

$$K_p = \left(\frac{4\pi \cdot 0,75}{1064} \right)^2 = 7,8 \cdot 10^{-5} .$$

Полученная зависимость показывает, что коэффициент рассеяния света квадратично возрастает с увеличением шероховатости поверхности [4,5]. При увеличении параметра шероховатости от 0,75 мкм до 2,37 мкм уровень рассеяния возрастает на порядок.

Таким образом, снижение шероховатости поверхности является одним из ключевых факторов уменьшения оптических потерь в оптических элементах с оптическими покрытиями в лазерных системах.

Влияние шероховатости на порог лучевой прочности. Микронеровности поверхности выступают локальными концентраторами электромагнитного поля и приводят к увеличению поглощения энергии лазерного импульса [6–8]. Для сравнительной оценки влияния шероховатости поверхности на лучевую прочность покрытия использовалась относительная расчетная зависимость, основанная на сравнении параметров шероховатости исследуемой и эталонной поверхностей, которое рассчитывается по формуле (3):

$$H = H_0 \times \frac{R_{q0}}{R_q}, \quad (3)$$

где H – расчетный порог лучевой прочности исследуемой поверхности, Дж/см²; H_0 – порог лучевой прочности поверхности, полученной классическим методом, Дж/см²; R_{q0} шероховатость поверхности, полученной классическим методом, нм; R_q – шероховатость исследуемой поверхности, нм.

Расчет лучевой прочности при условии, что $H_0 = 5$ Дж/см²:

$$H = 5 \frac{2,37}{0,75} = 15,8 \text{ Дж/см}^2 .$$

Оценка увеличения и отношение показателей:

$$\frac{\text{new}}{\text{classic}} = \frac{H}{H_0} = \frac{15,8}{5} = 3,16.$$

Таким образом, предложенный метод обеспечивает увеличение порога лучевой прочности примерно в 3 раза.

Итоговый сравнительный анализ показателей предлагаемого метода с классическим приведен в табл. 2.

Таблица 2 – Сравнительный анализ показателей

Параметр	Классический метод	Предлагаемый метод
Шероховатость R_a , мкм	2,37	0,75
Коэффициент интегрального рассеяния	$7,8 \cdot 10^{-4}$	$7,8 \cdot 10^{-5}$
Порог лучевой прочности, Дж/см ²	5	15,8

Полученные результаты показывают, что снижение микрорельефа поверхности приводит к существенному уменьшению коэффициента рассеяния света и увеличению порога лучевой прочности оптических покрытий.

Результаты и обсуждение

Шероховатость поверхности оказывает существенное влияние на оптические потери и порог лучевой прочности оптических элементов. В рамках данной работы была проанализирована зависимость коэффициента рассеяния света и порога лучевой прочности от среднеквадратичной шероховатости поверхности.

Зависимость коэффициента рассеяния света от шероховатости поверхности представлена на рис. 1. Расчеты выполнены в рамках приближения для длины волны $\lambda=1064$ нм.

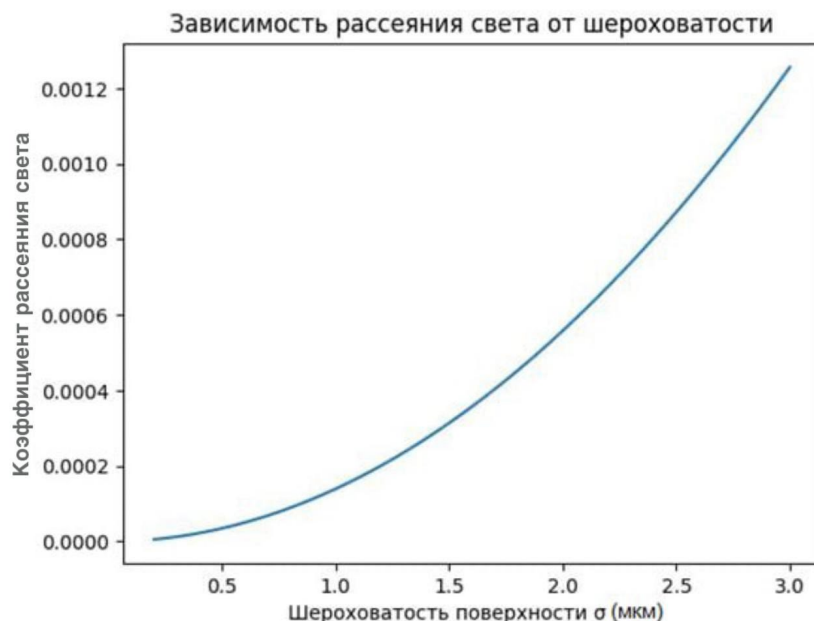


Рис. 1. Зависимость коэффициента рассеяния света от среднеквадратичной шероховатости поверхности при длине волны $\lambda=1064$ нм

Как видно из рисунка 1, увеличение шероховатости поверхности приводит к квадратичному росту коэффициента рассеяния света. При увеличении параметра шероховатости с 0,5 до 2,5 мкм значение возрастает больше чем на порядок.

Зависимость порога лучевой прочности от шероховатости поверхности представлен на рис. 2.

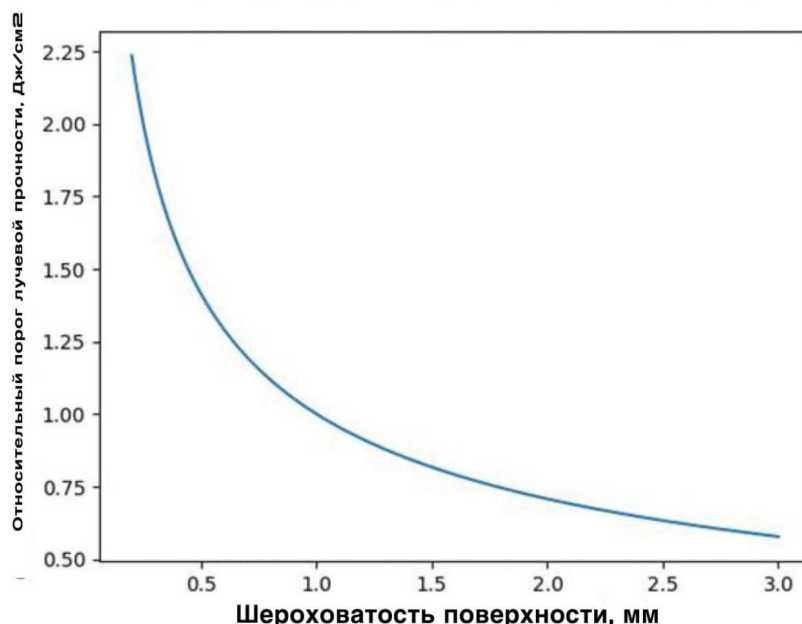


Рис. 2. Зависимость относительного порога лучевой прочности от шероховатости поверхности

Как показано на рис. 2, уменьшение шероховатости приводит к увеличению порога лучевой прочности, что связано с уменьшением концентрации дефектов [6–8]. Известно, что субповерхностные повреждения существенно снижают порог лучевой прочности [9, 10].

Сравнительный анализ показывает, что снижение шероховатости поверхности с 2,37 мкм (классический метод) до 0,75 мкм (предлагаемый метод) приводит к:

- уменьшению коэффициента рассеяния света примерно на порядок;
- увеличению порога лучевой прочности примерно в 3 раза.

Таким образом, полученные зависимости, представленные на рисунках 1 и 2, подтверждают эффективность предлагаемого метода обработки поверхности для повышения порога лучевой прочности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Alexei Kozlov. Long-term monitoring the damage performance of multilayer dielectric grating samples residing inside the compressor chamber of the OMEGA EP laser. // Optical Engineering. – 2021.

2. Brittany Hoffman. Mechanisms of picosecond laser-induced damage from interaction with model contamination particles on a high reflector. // Optical Engineering. – 2021.
3. Бобков, А.В., Разработка технологии обработки металлических деталей для оптического приборостроения связанным алмазно-абразивным инструментом [Электронный ресурс] / Естественные и технические науки. 2007. – Режим доступа: <https://www.elibrary.ru/item.asp?id=15860831> – Загл. с экрана.
4. Church E.L., Takacs P.Z. Specification of surface figure and roughness in optical manufacturing // Applied Optics. – 1993. – Т. 32, № 19. – С. 3344–3353.
5. Yu, Leyangyang. 1.07 μm laser ablation behavior of polycarbosilane based reflective/ablative composite coatings on the surface of graphite. // Applied Optics. – 2024.
6. Feit M.D., Rubenchik A.M. Mechanisms of laser-induced damage in optical materials // Proc. SPIE. – 1998. – Т. 3244. С.78.
7. Stuart B.C., Feit M.D. и др. Laser-induced damage in dielectrics // Physical Review Letters. – 1995. – Т. 74. С.36-44.
8. Duparré A., Tünnermann A. Laser damage thresholds of optical coatings // Proc. SPIE. – 2002.
9. Duparré A. и др. Surface characterization techniques // Applied Optics. – 2002. – Т. 41. С.48-56.
10. Negres R.A., Feit M.D., Rubenchik A.M. Subsurface damage // Proc. SPIE. – 2009. С. 123.

© Е. С. Мишечкин, М. П. Егоренко, Н. А. Гурин, 2026

А. С. Москаленко^{1✉}, Е. Н. Кулик¹

Оценка ресурсного потенциала территории на основе автоматизированного дешифрирования космических снимков и комплексного геоморфологического анализа

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация,
e-mail: trsnkn116@yandex.ru

Аннотация. В статье представлена методика комплексной оценки ресурсного потенциала территории на основе применения автоматизированного дешифрирования данных дистанционного зондирования Земли и геоморфологического анализа. Актуальность исследования обусловлена необходимостью оптимизации геологоразведочных работ на обширных и труднодоступных территориях. Подробно описан алгоритм автоматизированного выделения линеаментов – ключевых индикаторов глубинных геологических структур (разломов, зон трещиноватости), сигнализирующих о размещении месторождений полезных ископаемых и геодинамических рисках. Методика базируется на последовательном применении методов фильтрации (Собеля, Канни), бинарно-морфологической эрозии и преобразования Хафа к космическим снимкам (Landsat-8/9, Sentinel-2) и цифровым моделям рельефа (SRTM). Обоснована необходимость проверки автоматизированных результатов через комплексный анализ производных рельефа. На примере линеamentного каркаса Черноморского региона (Крит-Мурат-Апратский суперлинеament, Динаро-Эллинская и Драва-Дунай-Камчинская системы) показана эффективность предлагаемой методики. Она позволяет повысить достоверность выделения тектонических структур и может быть использована для прогноза локализации полезных ископаемых, оценки гидрогеологических условий.

Ключевые слова: линеamentный анализ, дистанционное зондирование Земли, ресурсный потенциал, автоматизированное дешифрирование, геоморфологический анализ, геоинформационные технологии, цифровые модели рельефа, цифровая обработка снимков

A. S. Moskalenko^{1✉}, E. N. Kulik¹

Assessment of the territory resource potential based on automated interpretation of space images and complex geomorphological analysis

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation,
e-mail: trsnkn116@yandex.ru

Abstract. The article presents a methodology for the integrated assessment of the territory's resource potential based on the application of automated interpretation of remote sensing data and geomorphological analysis. The relevance of the study is due to the need to optimize geological exploration works in vast and hard-to-reach territories. The algorithm of automated lineament extraction – key indicators of deep geological structures (faults and fractured zones) signaling the location of mineral deposits and geodynamic hazards – is described in detail. The methodology is based on the sequential application of filtering methods (Sobel, Canny), binary morphological erosion, and the Hough transform to satellite images (Landsat-8/9, Sentinel-2) and digital elevation models (SRTM). The necessity of verifying automated results through a comprehensive analysis of relief derivatives is substantiated. The effectiveness of the proposed methodology is shown using the

example of the lineament framework of the Black Sea region (the Crete-Murat-Ararat superlineament, the Dinaric-Hellenic and Drava-Danube-Kamchia systems). It allows increasing the reliability of tectonic structure identification and can be used for predicting mineral localization and assessing hydrogeological conditions.

Keywords: lineament analysis, remote sensing of the Earth, resource potential, automated interpretation, geomorphological analysis, GIS technologies, digital elevation models, digital image processing

Введение

В условиях увеличения масштабов недропользования и необходимости освоения новых, в том числе труднодоступных, территорий разработка эффективных и экономически обоснованных методов оценки ресурсного потенциала становится приоритетной научно-практической задачей. Традиционные методы геологической съемки, несмотря на высокую точность, характеризуются значительными временными и финансовыми затратами, что ограничивает возможность их оперативного применения на региональном уровне.

Наиболее эффективными в данном случае оказываются методы дистанционного зондирования Земли (ДДЗ), основанные на анализе данных космической съемки и цифровых моделей рельефа (ЦМР). Современный этап развития ДДЗ характеризуется переходом от визуального дешифрирования к автоматизированным методам. Однако автоматическое выделение геологических структур (линеаментов) связано с проблемой появления «ложных» объектов (дороги, границы полей, антропогенные сооружения), что требует разработки комплексных подходов к интерпретации результатов.

Объект и предмет исследования

Объектом исследования являются линеаменты – линейные элементы ландшафта, проявляющиеся в рельефе, гидросети и растительном покрове. Линеаменты выступают в качестве индикаторов глубинных геологических структур (разломов, зон трещиноватости, тектонических швов) и указывают на возможное размещение месторождений полезных ископаемых, а также позволяют определить инженерно-геологические условия территории. Предметом исследования является технология автоматизированного выделения и геоморфологического распознавания линеаментов на основе комплексного анализа ДДЗ Земли (космических снимков среднего и высокого разрешения) и цифровых моделей рельефа, реализованная в среде геоинформационных систем.

Научная новизна исследования заключается в теоретическом обосновании комплексного подхода к оценке ресурсного потенциала территории, интегрирующего методы автоматизированного дешифрирования космических снимков и геоморфологического анализа. В рамках данного подхода в настоящее время разрабатывается и структурируется алгоритм автоматизированного выделения линеаментов, включающий последовательное применение методов цифровой обработки изображений, выполняющих подчеркивание границ, проявляющихся резкими перепадами яркости (фильтрация Собеля, Канни); бинаризацию; морфо-

логическую эрозию и преобразование Хафа; который адаптируется для анализа данных ДЗЗ различного пространственного разрешения. Следующим этапом ведется подбор и проверка геоморфологических критериев для тестирования достоверности автоматизированных результатов. Разрабатываемые критерии базируются на изучении производных ЦМР (теневой рельеф, кривизна поверхности, дренажная сеть) и направлены на отсев ложных структур антропогенного и экзогенного происхождения.

Практическая значимость работы состоит в возможности применения разработанной методики для прогноза пространственной локализации полезных ископаемых, оценки гидрогеологических условий, а также для оптимизации геологоразведочных работ (сужение поисковых площадей на долевой стадии, сокращение временных и финансовых затрат). Результаты исследования могут быть адаптированы в практику работы геологических служб, а также использованы в учебном процессе при подготовке специалистов в области геодезии и дистанционного зондирования.

Для задач линеamentного анализа наибольшую ценность представляют мультиспектральные снимки среднего разрешения, позволяющие выявлять спектральные аномалии, связанные с зонами трещиноватости; панхроматические снимки высокого разрешения, обеспечивающие детальное отображение геоморфологических признаков; а также глобальные цифровые модели рельефа (например, SRTM) и их производные (уклоны, экспозиции, кривизна), являющиеся основой для геоморфометрического анализа.

Геоинформационные системы представляют собой инструментальную среду, объединяющую возможности хранения, обработки, анализа и визуализации пространственных данных. В рамках линеamentного анализа ГИС-технологии позволяют осуществлять пространственную интерпретацию (распознавание линеamentов, выявление узлов пересечения); проводить оверлейные операции (наложение векторных линеamentов на геологические, геоморфологические карты); выполнять статистическую обработку; а также визуализировать результаты в виде тематических карт (карты плотности линеamentов, карты тектонических структур).

Исходные данные

К исходным данным для линеamentного анализа предъявляется ряд требований, касающихся пространственного разрешения, спектрального диапазона, временной актуальности, радиометрического качества и геометрической точности. Пространственное разрешение должно соответствовать масштабу выявляемых структур: 30-90 м для региональных линеamentов и 10-15 м для локальных. При выборе спектрального диапазона предпочтение отдается ближнему и коротковолновому инфракрасному, поскольку в них наиболее контрастно проявляются зоны тектонических нарушений. Что касается временной актуальности, необходимо использовать снимки разных сезонов для компенсации сезонных изменений растительного покрова. Радиометрическое качество предполагает отсутствие облачности, минимальный уровень шумов и проведение атмосферной

коррекции. Не менее важно и требование геометрической точности, предполагающее наличие географической привязки для корректного совмещения с геологическими картами.

Сбор исходных данных для линеаментного анализа включает следующие этапы: поиск и загрузка данных с использованием открытых геопорталов для подбора снимков с минимальной облачностью; геометрическая коррекция – приведение к единой проекции для обеспечения пространственной совместимости разновременных слоев; усиление информативности изображения с помощью анализа главных компонент (РСА) и декореляционного растяжения для выделения скрытых линейных аномалий; а также создание производных ЦМР (расчет уклонов, экспозиций, кривизны, моделей теневого рельефа) для подготовки данных к геоморфологическому анализу.

Методы

Автоматизированное выделение линеаментов строится на последовательном применении методов цифровой обработки изображений. Фильтрация Собеля – дискретный дифференциальный оператор, вычисляющий приближенное значение градиента яркости изображения, используется для первичного выделения границ линейных объектов. Его преимуществами являются простота реализации и высокая скорость вычислений, недостатками – чувствительность к шуму и формирование «утолщенных» границ.

Алгоритм Канни – многоэтапный оптимальный детектор границ, включающий сглаживание (фильтр Гаусса), вычисление градиента, подавление немаксимумов и двойную пороговую фильтрацию. Он обеспечивает высокую точность локализации границ и формирование линий толщиной в один пиксель.

Бинарно-морфологическая эрозия – операция математической морфологии, удаляющая граничные точки бинарных объектов, применяется для подавления мелких шумовых артефактов и уменьшение толщины линий перед этапом векторизации.

Преобразование Хафа – это метод компьютерного зрения, позволяющий находить на изображении прямые линии. Суть метода сводится к регистрации: каждый короткий отрезок (штрих) регистрируется для определенного направления и положения прямой. Те отрезки, которые лежат на одной линии, показывают максимальную частоту регистрации и объединяются в сквозной линеамент.

Обсуждение

Автоматизированное выделение требует обязательной геоморфологической интерпретации для отсева ложных структур. Комплексный анализ включает построение карт теневого рельефа с различными азимутами освещения для выявления линейных уступов и гряд; расчет горизонтальной и вертикальной кривизны поверхности для идентификации зон перегибов склонов, характерных для разломов; выделение водосборных бассейнов и построение карт суммарного стока, при котором прямолинейные участки речных долин служат дополнительным подтверждением тектонической природы линеаментов; а также сопоставле-

ние с геологическими и геофизическими картами для установления соответствия выделенных структур известным разломам.

Заключение

Разработанная теоретико-методологическая база позволяет сформулировать основные принципы комплексной оценки ресурсного потенциала территории на основе интеграции автоматизированного дешифрирования космических снимков и геоморфологического анализа. Определенный объект и предмет исследования задают границы применимости методики. Сформулированная научная новизна отражает вклад в развитие теории линеamentного анализа. Практическая значимость обосновывает востребованность результатов для геологоразведочных, гидрогеологических и инженерно-геологических задач. Разрабатываемый алгоритм обработки данных ДЗЗ и ГИС-анализа создает основу для последующей апробации на конкретных территориях и может быть адаптирован для различных геодинамических условий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Hobbs, W. H. Lineaments of the Atlantic border region / W. H. Hobbs. – Текст : электронный // Bull. Geol. Soc. Amer. – 1904. – Vol. 15. – P. 483–506.
2. Философов, В. П. Основы морфометрического метода поисков тектонических структур / В. П. Философов. – Саратов : Издательство Саратовского университета, 1975. – 232 с. – Текст : электронный.
3. Ласточкин, А. Н. Рельеф земной поверхности: принципы и методы статической геоморфологии / А. Н. Ласточкин. – Ленинград : Недра, 1991. – 340 с. – Текст : электронный.
4. Чернова, И. Ю. Автоматизированный линеamentный анализ : учебно-методическое пособие / И. Ю. Чернова, И. И. Нугманов, Р. И. Кадыров. – Казань : Казанский (Приволжский) федеральный университет, 2012. – 38 с. – Текст : электронный.
5. Canny, J. F. A Computational Approach to Edge Detection / J. F. Canny. – Текст : электронный // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1986. – Vol. 8, No. 6. – P. 679–698.
6. Galamhos, C. Progressive probabilistic Hough transform for line detection / C. Galamhos, J. Matas, J. Kittler. – Текст : непосредственный // Proc. IEEE Computer Society Conf. on Computer Vision and Pattern Recognition. – 1999. – P. 554–560.
7. Фам Суан Хоан. Разработка технологии автоматизированного обнаружения и анализа линеamentов и кольцевых структур на космических изображениях : автореф. дис. ... канд. техн. наук / Фам Суан Хоан. – Москва : МИИГАиК, 2012. – 24 с. – Текст : электронный.
8. Купцова, О. В. Методика выявления дизъюнктивных нарушений по данным дистанционного зондирования Земли с использованием линеamentного анализа / О. В. Купцова. – Текст : электронный // Мониторинг. Наука и технологии. – 2021. – № 1 (47). – С. 6–13.
9. Купцова, О. В. Разработка технологии дешифрирования изображений для выявления разрывных нарушений с использованием геофизических данных : дис. ... канд. техн. наук / О. В. Купцова. – Новосибирск : СГУГиТ, 2022. – 132 с. – Текст : электронный.
10. Иванова, Ю. Н. Применение спутниковых данных Landsat-8 с целью прогнозирования рудной минерализации для северных территорий / Ю. Н. Иванова, И. О. Нафигин. – Текст : электронный // Исследование Земли из космоса. – 2023. – № 1. – С. 24–40.
11. Зверев, А. В. Применение автоматизированного линеamentного анализа космических снимков при поисках нефтегазовых месторождений, прогнозе землетрясений... / А. В.

Зверев, А. Т. Зверев. – Текст : электронный // Известия вузов. Геология и разведка. – 2015. – № 6. – С. 14–20.

12. Шевырев, С. Л. Программа LEFA: автоматизированный структурный анализ космической основы в среде Matlab / С. Л. Шевырев. – Текст : электронный // Успехи современного естествознания. – 2018. – № 10. – С. 138–143.

13. Покалюк, В. В. Тектонолинеamentный каркас Причерноморского региона и сопредельных территорий / В. В. Покалюк, И. Э. Ломакин, В. Г. Верховцев, В. В. Кочелаб. – 2021. – Т. 8, № 1. – С. 26–44. – Текст : электронный.

14. Стрихарчук, М. Ю. Глубинное строение и тектоника Черноморской впадины / М. Ю. Стрихарчук. – Текст : электронный // Геофизический журнал. – 2018. – Т. 40, № 5. – С. 80–101.

© А. С. Москаленко, Е. Н. Кулик, 2026

Е. С. Панюкова^{1✉}, А. В. Шабурова¹

Оценка результативности и прогнозирование показателей эффективности СМК наукоемких предприятий на основе методов компьютерного моделирования

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: ek-panyukova@mail.ru

Аннотация. В статье рассматривается проблема управления качеством в наукоемких предприятиях, разрабатывающих автоматизированные решения в различных сферах. На основе проведенного литературного обзора показано, что традиционные ретроспективные показатели системы менеджмента качества (СМК) демонстрируют ограниченность в части реагирования на возникающие риски, планирования и проведения оценки результативности существующих в организации процессов. Представлен подход на основе машинного обучения, реализуемый посредством использования непараметрического метода обучения для решения задач регрессии. Прогнозирование сроков позволяет решать комплекс задач в рамках системы менеджмента качества и операционного менеджмента. Проведен сравнительный анализ с альтернативными методами, показавший преимущество разработанного подхода по точности и интерпретируемости. Приведены практические выводы, описаны рекомендации по настройке системы сбора данных и интерпретации прогнозов для принятия управленческих решений.

Ключевые слова: оценка результативности, анализ качества, система менеджмента качества, наукоемкое предприятие, предиктивная аналитика, машинное обучение

E. S. Panyukova^{1✉}, A. V. Shaburova¹

Assessing Effectiveness and Predicting Performance Indicators of the Quality Management System of High-Tech Enterprises Based on Computer Modeling Methods

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: ek-panyukova@mail.ru

Abstract. The article addresses the problem of quality management in high-tech enterprises engaged in developing automated solutions across various domains. Based on a literature review, it is shown that traditional retrospective quality management system (QMS) indicators demonstrate limitations in terms of responding to emerging risks, planning, and evaluating the effectiveness of existing organizational processes. A machine learning-based approach is proposed, implemented through the use of a nonparametric learning method for solving regression problems. Predicting timeframes enables addressing a range of tasks within the quality management system and operational management. A comparative analysis with alternative methods is conducted, demonstrating the superiority of the proposed approach in terms of accuracy and interpretability. Practical findings are presented, along with recommendations for configuring the data collection system and interpreting forecasts for managerial decision-making.

Keywords: effectiveness assessment, quality analysis, quality management system, high-tech enterprise, predictive analytics, machine learning

Введение

Современные наукоемкие предприятия, функционирующие в условиях высокой неопределенности, как и любые другие предприятия, сталкиваются с проблемой обеспечения стабильности и прогнозируемости результатов. Высокая доля интеллектуального труда, длительные инновационные циклы и низкая предсказуемость сроков завершения – все эти особенности высокотехнологичных предприятий лишь усугубляют проблему эффективного управления качеством результатов производственной деятельности [1]. Изучение зарубежной и отечественной литературы позволило рассмотреть менеджмент качества как сквозной процесс, интегрированный во все фазы жизненного цикла создания продукта, что предполагает наличие множества концептуальных подходов к его внедрению и развитию. Значительное влияние на формирование современного понимания управления качеством оказали работы У. Э. Деминга, Дж. М. Джурана и К. Исикавы, заложившие основы всеобщего управления качеством, с развитием которого в массовом производстве осуществляется поддержка и улучшение качества через внедрение таких стандартов, как ГОСТ ИСО 9001-2008 [3]. Однако переход от абстрактных принципов к практическому контролю требует наличия конкретных измеримых инструментов оценки, что является актуальной задачей менеджмента на сегодняшний день.

Система менеджмента качества (СМК) при правильном подходе к внедрению становится инструментом, способным сформировать устойчивую базу для стратегического развития и планирования, а также последующую возможность цифровизации и автоматизации [2]. В то же время, четкая методика реализации и внедрения предупреждающих действий отсутствует в требованиях стандартов. Данная проблема становится особенно актуальной для высокотехнологичных предприятий, уровень неопределенности и сложности процессов которых оказывается выше относительно других предприятий и компаний [4]. Эволюция различных подходов к прогнозированию в менеджменте демонстрирует тенденцию к использованию формализованных или статистических методов, ввиду их точности и обоснованности.

Несмотря на это, экспертные подходы и аналитические модели обладают рядом преимуществ, как, например, возможность учитывать специфические факторы или предоставлять прозрачности и интерпретируемость результатов. Достоинства каждого подхода могут быть использованы как взаимодополняющие элементом целостного гибридного подхода, способного учитывать различные сложности.

Методы и материалы

Основной деятельностью высокотехнологичных компаний и предприятий является создание и использование продуктов и технологий с высокой долей интеллектуальных разработок. Рассмотрим возможность применения подхода к прогнозированию показателей эффективности и проведения оценки результа-

тивности на примере российской IT-компании, специализирующейся на сопровождении компьютерных систем и выполнении научных исследований и разработок в области естественных и технических наук. Значимой характеристикой для анализа в области менеджмента организации является информация о численности штата: основу составляют высококвалифицированные специалисты в области информационных технологий, прикладной математики и естественно-научных дисциплин, что в процентном выражении составляет свыше 20% от общего количества сотрудников в 250 человек. Организационная структура компании является слабой матричной: в системе функционируют как устойчивые функциональные направления, так и временные проектные группы, организованные под конкретные задачи, что также косвенно может оказывать негативное влияние на предсказуемость результатов. Для обеспечения управления потоком создания ценностей и синхронизации внутренних процессов рассматриваемая организация использует систему управления проектами Jira, с помощью которой осуществлялся сбор эмпирических данных для анализа реальных процессов. Количество наблюдений за исследуемый промежуток составило около 12 тысяч, что является существенным ограничением для использования некоторых алгоритмов моделей машинного обучения. Исторические данные включают в себя информацию о сроках завершения проекта, исполнителях, фактических трудовых затратах, загруженности сотрудников, категории и типе конкретной деятельности и прочие факторы. По информации от руководителя и ключевых сотрудников по каждому направлению важным и менее развитым показателем эффективности, в том числе и для СМК, является соблюдение плановых сроков разработки и проведения исследований. Стоит отметить, что текущие методы прогнозирования имеют относительную ошибку в диапазоне 50-250 %, исходя из внутренних данных исследуемой компании. Исследования зарубежных и российских учетных подтверждают масштабность данной проблемы и отмечают наличие систематического смещения в сторону занижения сроков реализации в 1,5-2 раза [5].

В работе исследователем была выдвинута гипотеза о том, что с помощью алгоритма машинного обучения можно получить более качественный инструмент прогнозирования сроков поставки решения исследовательских задач, нежели через существующие метрики: показатель своевременности поставок, среднее время выполнения проекта, экспертные оценки.

Рассмотрим задачу бинарной классификации с целью оценки вероятности отклонения сроков выполнения задач с использованием методов машинного обучения. Каждый объект данных описывается вектором признаков $x = (x_1, x_2, \dots, x_d)$, отражающим характеристики задачи, контекст ее выполнения и исторические данные о реализации аналогичных задач. Целевая переменная является непрерывной положительной величиной, отражающей фактический срок выполнения

задачи. Функция прогнозирования в математическом виде выглядит следующим образом:

$$\hat{f}(x) = \frac{1}{B} \sum_{b=1}^B T_b(x). \quad (1)$$

где $\hat{f}(x)$ – точечный прогноз y при заданном векторе предикторов $x \in R^d$,
 B – гиперпараметр, отражающий количество базовых алгоритмов,
 T – результат работы b -го базового регрессора.

Для построения моделей были использованы стандартные библиотеки языка программирования Python, в результате чего было построено несколько моделей регрессии с разной спецификацией распределения и функциональными связями. Наиболее эффективный результат показала модель на базе алгоритма, состоящего из множества «решающих деревьев», или RandomForest. Ключевые метрики качества полученной модели представлены ниже в таблице.

Таблица 1 – Метрики качества модели регрессии RandomForest Regression

• RandomForest Regression	
• MAE	• 12,93 дней
• RMSE	• 14,96 дней
• R^2	• 0,872

В сравнении среднеквадратическая ошибка у регрессии, построенной с использованием стандартного биномиального распределения, составила 82783 дня, что почти в 4 раза превышает результаты модели на «случайного леса». Распределение остатков приближенно к нормальному: отношение $RMSE/MAE = 1,16$, однако вершина распределения плоская, что может свидетельствовать о недостаточной вариативности или присутствии регуляризации. Данное наблюдение также подтверждает коэффициент эксцесса, значение которого имеет значение ниже эталонного значения, что характерно для распределений с плоскими вершинами. Подобное свойство распределения говорит о низкой дисперсии остатков, и соответственно, редко встречающихся выбросов, остатки не концентрируются вокруг одного значения, распределены равномерно. Из выше сказанного делаем вывод о том, что качество модели получилось достаточным для проведения дальнейшей оценки результативности.

На рис. 1 распределения остатков модели можно увидеть подтверждение описанным выше свойствам.

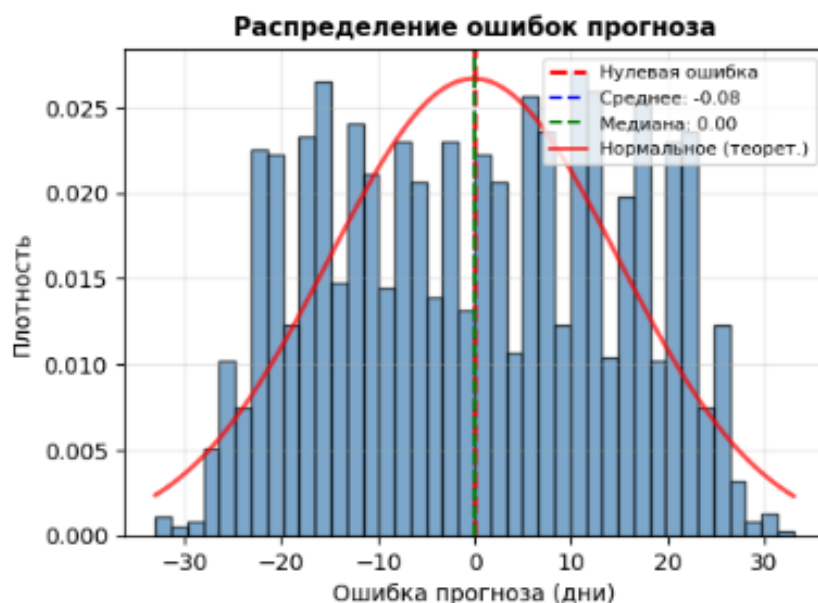


Рис. 1. Распределение остатков модели

Результаты

При решении задачи оценки эффективности и управления рисками инновационной или высокотехнологичной деятельности менеджеры и исследователи часто прибегают к методам оценки кумулятивных эффектов [4]. Исходя из полученных с помощью модели регрессии результатов, был составлен сводный график кумулятивной точности прогнозов или оценки риском СМК, рассматриваемой компании.

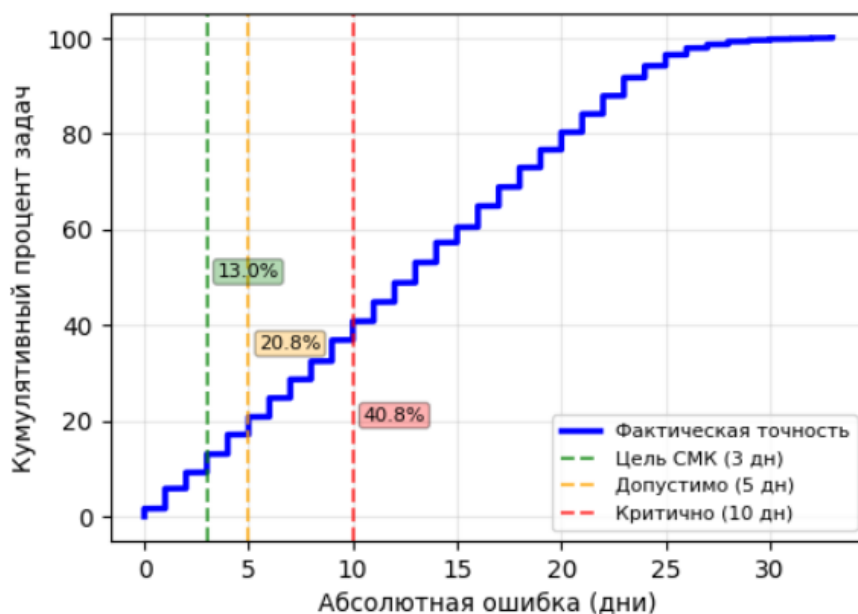


Рис. 2. Интерпретация точности прогнозов

Статистическое качество прогноза, исходя из данного графика, получилось неудовлетворительное, если смотреть относительно целевых показателей СМК компании. Фактический результат прогнозирования говорит о том, что лишь 33,8% задач имеют приемлемую точность на недельном горизонте планирования. Кроме того, с ростом длительности задач предиктивная мощность модели снижается – ошибка на уровне 40,8 % (рис. 2). Потенциально возможные причины полученного результата могут заключаться в ограниченном наборе данных, а именно недостаточного количества факторов в исходной модели и малое количество наблюдений. Однако, несмотря на низкое качество прогноза, подход с использованием модели машинного обучения показывает явные преимущества перед традиционными методами СМК:

1. многомерный анализ позволяет учитывать десятки факторов одновременно и выявлять сложные нелинейные зависимости;
2. объективность и воспроизводимость результатов;
3. адаптивности модели;
4. на коротком горизонте планирования модель показывает высокое качество прогноза.

Кроме того, стоит отметить, что модельный подход позволил выделить ключевые факторы, влияющие на срок решения задач: исполнитель, тип задачи, приоритет задачи [6-10].

Заключение

Тем самым, прогнозная модель как инструмент раннего предупреждения может быть внедрена в процесс планирования, однако не как основной, а как второстепенный, способный оперативно выделить проекты, где прогнозируемая вероятность отклонения от плана превышает 60 %. Модельный подход может быть применим и при проведении оценки результативности процессов внутри компании: модель позволяет оценивать результативность до наступления целевого события, а в процессе разработки, что превращает данный инструмент в механизм предотвращения отклонений. Однако для получения большей результативности можно рассмотреть использование гибридного подхода, который будет сочетать в себе формализованный, а именно модельный подход для обеспечения стабильности и воспроизводимости, и экспертные методы прогнозирования. В будущих исследованиях стоит учесть возникшие сложности, рассмотрев альтернативные варианты модельных решений для ограниченного набора данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гусева И.Б. НИОКР на предприятиях ОПК: современные проблемы / И. Б. Гусева // Вестник Института экономики Российской академии наук. – 2016. - № 2. – С. 147–158.
2. Комаров Н.М., Пащенко Д.С. Элементы развития теории управления цифровой трансформацией высокотехнологичных промышленных предприятий / Н. М. Комаров, Д. С. Пащенко // Вестник евразийской науки. – 2025. – Т. 17, № 4. – С. 1–17.

3. ГОСТ Р ИСО 9001-2008. Система менеджмента качества. Требования. - Переизд. 2009 с Изм. – Москва : Стандартиформ, 2009. – 25 с. – М.: ИПК Издательство стандартов, 2009.
4. Степанов А.В. Результативность процессов СМК / А. В. Степанов // Методы менеджмента качества. – 2008. – № 2. - С. 26–28.
5. Долженко С. Б., Долженко Р. А. Оценка мероприятий научной организации труда через призму показателей эффективности персонала / С. Б. Долженко, Р. А. Долженко // Научная организация труда: история, современность, перспективы : материалы научных чтений, посвященных памяти профессора М. А. Мельнова (Екатеринбург, 20 октября 2017 г.). - Екатеринбург : УрГЭУ, 2017. – С. 45–51.
6. Заюнчковский, С. Ю. Система менеджмента качества: инструмент развития организации или дополнительная нагрузка? / С. Ю. Заюнчковский, С. А. Коновалов, В. В. Зинченко [и др.] // Digital Diagnostics. – 2023. – Т. 4, № 3. – С. 2–10.
7. Суслов В.И., Ибрагимов Н.М., Талышева Л.П., Цыплаков А.А. Эконометрия. – Новосибирск: СО РАН, 2005. – С.691–714.
8. Вербик М. Путеводитель по современной эконометрике – М.: Научная книга. – 2008. С.39-49.
9. Голубь Н.Н. Оперативное управление производством сложной наукоемкой продукции / Н.Н. Голубь // Вестник Воронежского государственного технического университета. – 2020.
10. Кузнецов, И. В. Интеграция процессов технической и оперативной подготовки производства в условиях цифровизации / И. В. Кузнецов // Организатор производства. – 2021. – Т. 29, № 3. – С. 45–54.

© Е. С. Панюкова, А. В. Шабурова, 2026

М. В. Пилипич¹✉, А. В. Шабурова¹

Построение системы защиты информации, для системы оповещения населения города

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: mikhailpilipich@yandex.ru

Аннотация. В статье рассматривается актуальная проблема построения системы защиты информации (СЗИ) для системы оповещения населения (СОН) города в условиях роста киберугроз и ужесточения нормативно-правового регулирования. Объектом исследования выступает СОН как значимый объект критической информационно-инфраструктуры (КИИ), находящийся под тройным регуляторным давлением (ФЗ-149, ФЗ-187, ведомственные приказы МЧС и ФСТЭК России). Авторы выявляют ключевое противоречие: существующие системы защиты зачастую носят фрагментарный, реактивный характер, не в полной мере соответствуют актуальным требованиям регуляторов и не учитывают эволюцию тактик злоумышленников — от простого вывода систем из строя до попыток компрометации каналов управления с целью дезинформации населения и провоцирования паники. Основными методами исследования стали анализ нормативно-правовой базы, обобщение данных о реальных инцидентах (взломы серверов радиостанций, атаки на агропредприятия) и критический обзор существующих подходов к защите СОН. В результате авторами предложена трехуровневая структура СОН (управление, автоматизированное управление, исполнительные устройства) и выделены ключевые объекты защиты. Главным выводом работы является обоснование необходимости перехода от формального соблюдения разрозненных требований к построению адаптивной модели соответствия. Такая модель должна гармонизировать предписания всех регуляторов, внедрять гибкие технологические решения (NFV, SDN, промышленные шлюзы безопасности) и включать обязательные процедуры эмпирической валидации — киберучения, аналогичные тренировкам по гражданской обороне. Реализация данного подхода позволит обеспечить гарантированное и своевременное оповещение граждан в условиях современных вызовов и угроз.

Ключевые слова: система оповещения, защита информации, инциденты

М. В. Pilipich¹✉, A. V. Shaburova¹

Building an Information Protection System for the City's Public Warning System

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: mikhailpilipich@yandex.ru

Abstract. The article addresses the pressing issue of designing an information protection system for a city's public warning system (PWS) amid growing cyber threats and stricter regulatory requirements. The object of the study is the public warning system as a significant object of critical information infrastructure (CII), which is subject to triple regulatory pressure (Federal Law No. 149-FZ, No. 187-FZ, and by-laws of the Russian Ministry of Emergency Situations and FSTEC of Russia). The authors identify a key contradiction: existing protection systems are often fragmented and reactive, do not fully comply with current regulatory requirements, and fail to account for the evolving tactics of attackers — from simply disabling systems to attempting to compromise control channels in

order to spread disinformation and provoke panic. The main research methods include an analysis of the regulatory framework, a synthesis of data on real incidents (hacks of radio station servers, attacks on agricultural enterprises), and a critical review of existing approaches to PWS protection. As a result, the authors propose a three-level structure of the PWS (management level, automated control level, and executive devices) and identify key assets requiring protection. The main conclusion of the study is the substantiation of the need to transition from formal compliance with disparate requirements to building an adaptive compliance model. Such a model should harmonise the requirements of all regulators, implement flexible technological solutions (NFV, SDN, industrial security gateways), and include mandatory empirical validation procedures – cyber drills analogous to civil defence exercises. The implementation of this approach will ensure reliable and timely warning of citizens in the face of modern challenges and threats.

Keywords: notification system, information protection, incidents

Введение

Под системой оповещения населения принято понимать организационно-техническое объединение – в него входят специальные силы, средства связи и оповещения, вещательные сети, а также каналы общедоступной сети связи. Все это вместе предназначено для того, чтобы доставить информацию и сигналы тревоги до органов управления, сил РСЧС и, конечно, до самого населения.

Главное назначение таких систем – обеспечить своевременное информирование об опасностях. Речь идет об угрозе или возникновении чрезвычайных ситуаций природного и техногенного характера, а также о военных действиях или их последствиях. Кроме того, система оповещения доводит до людей правила поведения и необходимость проведения защитных мероприятий.

За то, чтобы оповещение происходило без задержек, отвечают органы государственной власти субъектов Российской Федерации и органы местного самоуправления. Само решение о том, нужно ли запускать оповещение, задействовать для передачи сигналов сети связи операторов и другие технические каналы, а также определить, какая именно территория подлежит оповещению, принимают высшие должностные лица регионов, главы муниципальных образований либо лица, которые временно исполняют их обязанности.

Основные функции систем оповещения:

- информирование (предоставление информации о возникновении чрезвычайной ситуации, необходимости эвакуации, характере угрозы и действиях, которые нужно предпринять);
- направление потоков людей (указание безопасных путей эвакуации и направление людей к выходам);
- предотвращение паники. (четкие и понятные инструкции помогают избежать хаотичных действий и паники);
- обратная связь (возможность передачи информации для координации действий служб экстренного реагирования);
- управление эвакуацией (организация более быстрой и организованной эвакуации, включая распределение людей по зонам и реализацию алгоритмов эвакуации).

Системы оповещения создаются на разных уровнях:

- на федеральном уровне – федеральная система оповещения (на территории Российской Федерации);
- на межрегиональном уровне – межрегиональная система оповещения (на территории федерального округа);
- на региональном уровне – региональная система оповещения (на территории субъекта Российской Федерации);
- на муниципальном уровне – местная система оповещения (на территории муниципального образования);
- на объектовом уровне – локальная система оповещения (в районе размещения потенциально опасного объекта).

Также существует комплексная система экстренного оповещения населения об угрозе возникновения или о возникновении чрезвычайных ситуаций (КСЭОН) – комплекс программно-технических средств систем оповещения и мониторинга опасных природных явлений и техногенных процессов.

Исследование

На безопасность государства воздействует целый ряд факторов. В современной геополитической обстановке нельзя игнорировать сложившиеся социально-экономические реалии, политическую поляризацию в обществе, обострение межнациональных и международных отношений, экономические и политические санкции, направленные против России, а также локальные вооруженные конфликты. Совокупность этих факторов формирует широкий круг внутренних и внешних угроз национальной безопасности и порождает условия, напрямую угрожающие личности, социуму и государству [33].

Особую актуальность сегодня приобретают вопросы информирования и своевременного оповещения граждан о возникновении опасности или угрозе ее появления, а также о правилах поведения и алгоритме действий при чрезвычайных и опасных ситуациях. Эти задачи занимают ключевое место в общем комплексе мер по обеспечению безопасности и защите населения [33].

Большинство предыдущих научных работ было посвящено решению управленческих и организационно-технических проблем (принципы построения систем оповещения на разных уровнях, требования к их техническому оснащению и сопряжению, а также характеристики комплексных систем информирования, включая КСЭОН и систему 112) [20-28].

Руководство МЧС России неоднократно заявляло, что современные угрозы требуют непрерывных исследований, направленных на повышение эффективности информационного воздействия, совершенствование действующих и внедрение новых технологий оповещения населения [28, 32-33].

Кибератаки в настоящее время становятся наиболее частой причиной совершения различных преступлений [34], которые нередко влекут за собой возникновение чрезвычайных ситуаций. Примером того, как кибератаки могут привести к техногенным и социальным ЧС, служат инциденты в ряде российских регионов. В марте 2022 года кибератакам подверглись агрохолдинг «Мираторг» и

«Ростовский колбасный завод – ТАВР». В результате 18 предприятий агрохолдинга лишились возможности оформлять производственные, транспортные и ветеринарные документы на продукцию, а работа завода «Тавр» была временно приостановлена. 22 и 28 февраля 2023 года хакерская атака на серверы радиостанций в Казани, Уфе, Белграде, Нижнем Новгороде, Крыму и других городах привела к неоднократному звучанию в эфире ложной информации об объявлении тревоги.

Полномочия по выработке и реализации государственной политики, нормативно-правовому регулированию, организации контроля в сфере создания и совершенствования комплексной системы информирования и оповещения населения возложены на МЧС России и его территориальные органы. Поскольку комплексная система оповещения объединяет взаимосвязанные системы информирования и оповещения, эти функции реализуются во взаимодействии с другими органами государственной власти. Деятельность в этой области регулируется совместным приказом МЧС России, Мининформсвязи и Минкультуры РФ от 25 июля 2006 г. № 422/90/376 «Об утверждении Положения о системах оповещения населения».

Актуальность

Защита информации в современных цифровых системах оповещения населения (СОН) регламентируется строгим и многоуровневым нормативным каркасом, что определяет специфику подхода к их безопасности. Ключевые документы образуют иерархию, в рамках которой СОН выступает объектом тройного регулирования [1]:

- ФЗ-149 «Об информации, информационных технологиях и о защите информации» – задает базовые принципы и правовой режим данных;
- ФЗ-187 «О безопасности критической информационной инфраструктуры (КИИ) РФ» – определяет СОН как значимый объект КИИ;
- совместный Приказ МЧС России и Минцифры России № 578/365 – является ключевым подзаконным актом, детализирующим технические и архитектурные требования непосредственно к СОН как к единой технологической сети связи;
- приказы ФСТЭК России – детализируют конкретные меры защиты: № 239 (требования к средствам защиты), № 117 (защита ГИС), № 31 (защита АС).

Таким образом, защита СОН строится не на общих принципах, а как защита критически важного государственного актива от компьютерных атак [2], требующая синтеза требований из разных правовых полей.

Актуальность данной проблематики многократно возросла в связи с геополитическими изменениями и ростом числа инцидентов в отношении объектов структур. Как отмечает Центр мониторинга внешних цифровых угроз (2024), количество атак на государственные системы связи в 2023–2024 гг. увеличилось на 37% по сравнению с предыдущим периодом, при этом системы оповещения рассматриваются злоумышленниками как «критическая инфраструктура нулевого

уровня», вывод которой из строя способен вызвать максимальный общественный резонанс [3].

Определение СОН как объекта КИИ и сети связи предопределяет приоритетные классы угроз, выделяемые в контексте законов:

- нарушение функционирования (ФЗ-187): атаки на доступность (DDoS) и целостность (подмена команд), способные парализовать работу системы в момент чрезвычайной ситуации (ЧС);
- нарушение безопасности информации (ФЗ-149): несанкционированный доступ к конфиденциальным данным системы;
- распространение ложной информации (ФЗ-149): через взломанные каналы СОН, что может привести к массовой панике и подрыву доверия [4].

Практическое подтверждение актуальности последнего класса угроз содержится в отчетах о расследовании инцидентов. Например, попытки несанкционированного доступа к пультам управления региональных систем оповещения в приграничных территориях в 2022–2023 гг. демонстрируют сдвиг тактики злоумышленников: от простого вывода систем из строя (деструкция) к попыткам компрометации каналов управления с целью дезинформации населения. Это требует пересмотра подходов не только к защите доступности, но и к гарантиям аутентичности исходящих сообщений [5].

Их нарушение может привести к:

- несвоевременному оповещению и, как следствие, человеческим жертвам;
- распространению паники или дезинформации;
- подрыву доверия к органам власти.

Следовательно, защита информации, циркулирующей в КСОН (управляющие команды, базы данных абонентов, конфиденциальные сведения), – это не техническая, а стратегическая задача, напрямую связанная с национальной безопасностью.

Существующая система защиты информации (СЗИ) в КСОН городского округа зачастую имеет:

– **устаревшее оборудование:** не имеет комплексного, системного характера. Многие развернутые СОН включают аппаратуру, не поддерживающую современные ГОСТ-протоколы, а их модернизация сопряжена с высокой стоимостью. Не соответствует в полной мере актуальным требованиям регуляторов (ФСТЭК, ФСБ, МЧС России, Минкомсвязи) и не учитывает современные киберугрозы;

– **отсутствие типовых решений:** развивается реактивно, а не на основе проактивной оценки угроз. Нет адаптированных под специфику СОН архитектурных шаблонов, удовлетворяющих всем регуляторным требованиям одновременно. Не проходит регулярной независимой оценки эффективности;

– **кадровый дефицит:** ощущается нехватка специалистов, способных комплексно применять требования МЧС, ФСТЭК и ФСБ.

Большинство существующих работ ориентированы на нормативно-дескриптивный подход, описывая «должное» состояние системы. Однако в науч-

ной литературе наблюдается дефицит эмпирических исследований, посвященных измерению реальной эффективности внедряемых мер. Как отмечает Сорокин (2023), практически отсутствуют работы, содержащие результаты нагрузочного тестирования систем безопасности СОН в условиях имитации высокоинтенсивных атак (АРТ-групп), что не позволяет объективно оценить заявленную «киберустойчивость» [14].

Мероприятия по обеспечению защиты информации

Рассмотрим подробнее, как устроена система оповещения населения (СОН) с точки зрения иерархии и защиты. В профессиональной среде принято выделять три уровня.

Верхний уровень – управленческий. Здесь находится дежурная (или дежурно-диспетчерская) служба, которая входит в орган повседневного управления РСЧС. Именно эта служба уполномочена принимать решение и давать команду на запуск системы. Обратим внимание: на этом уровне обычно располагаются автоматизированные рабочие места (часто на серверной платформе) с общесистемным и прикладным ПО, а также все телекоммуникационное хозяйство – коммутаторы, маршрутизаторы, каналы связи, межсетевые экраны и прочее. Без этого оборудования управление становится невозможным.

Средний уровень – автоматизированного или автоматического управления. Его задача – не просто передать сигнал, а обеспечить контроль конечных устройств: получить подтверждение их включения, отследить состояние. Здесь используется аппаратура запуска и мониторинга, звукоусилительные комплекты, усилительно-коммутационные блоки, а также специальные устройства перехвата речевых и видеотрактов. Кроме того, это уровень каналов и линий связи, которые идут непосредственно к оконечным средствам.

Нижний уровень – исполнительный. Это те устройства, которые физически доносят сигнал до людей: громкоговорители, акустические системы, электросирены. Сюда же относятся датчики чрезвычайных ситуаций и системы мониторинга природных и техногенных ЧС. Практика показывает, что именно нижний уровень чаще всего оказывается самым уязвимым, но об этом чуть позже.

Теперь об объектах защиты в СОН. По моему опыту, к ним в первую очередь следует относить автоматизированные рабочие места (серверы) с их ПО, устройства перехвата трактов, а также каналы связи между этими элементами. Однако перечень может расширяться в зависимости от конкретных угроз – это важно понимать при проектировании.

Перейдем к нормативной базе. Защита информации в системах оповещения регулируется двумя ключевыми приказами ФСТЭК России: № 31 от 14.03.2014 (для АСУ на критически важных и потенциально опасных объектах) и № 17 от 11.02.2013 (для государственных информационных систем, где информация не содержит гостайны). Основные задачи, которые ставятся перед системой защиты, – это предотвращение несанкционированного доступа, обеспечение целостности и доступности передаваемых данных, а также отражение внешних угроз.

Как формировать требования к защите? Рекомендую опираться на ГОСТ Р 51583 и ГОСТ Р 51624, а также на региональные нормативные документы. Если у государственного заказчика-координатора разработаны политики информационной безопасности по ГОСТ Р ИСО/МЭК 27001, их тоже следует учитывать. Это позволяет выстроить системный менеджмент.

Ключевое условие штатного функционирования – система защиты не должна мешать работе СОН при выполнении ею своих прямых функций. Это золотое правило, которое часто нарушается, когда пытаются «перестраховаться» и устанавливают избыточные средства защиты.

Организационные меры. На что обращать внимание при внедрении? Нужно ввести четкие ограничения для персонала (пользователей дежурно-диспетчерской службы, администраторов, обслуживающего персонала) на действия, условия эксплуатации, изменение конфигурации техники и ПО. Назначить ответственного за безопасность информации. Разработать правила разграничения доступа. Проверить, насколько полно в инструкциях описаны действия сотрудников. И обязательно отрабатывать практические действия – без этого любые бумаженные регламенты бесполезны.

Специфический, но важный запрет касается тестирования, диагностики, программирования и управления системой оповещения с каналов и мест подключения оконечных средств. Это прямо предусмотрено в приказе № 31 для соответствующих классов защищенности. То есть нельзя, чтобы кто-то, подключившись к сирене или громкоговорителю, мог перехватить управление или изменить логику работы.

Наконец, компенсирующие меры. На практике часто возникает ситуация, когда штатные меры защиты невозможно применить на каком-либо уровне или для отдельных технических средств – например, они мешают быстрдействию или надежности оповещения. В таких случаях на этапе адаптации базового набора мер разрабатываются иные, компенсирующие. Их задача – адекватно блокировать или нейтрализовать угрозы и обеспечить необходимый уровень защищенности. При этом разработчик обязан обосновать выбор именно таких мер, а при приемочных испытаниях нужно оценить, достаточно ли они эффективны. Без этого компенсирующие меры останутся лишь декларацией.

Заключение

Нормативная база формирует жесткий, но необходимый каркас для защиты СОН. Однако его практическая реализация сталкивается с системными сложностями. Расширенный анализ позволяет выделить не только направления совершенствования регуляторики, но и технологические векторы развития.

Перспективным направлением исследований является разработка адаптивной модели соответствия, которая [13; 17]:

1. гармонизирует требования: предлагает сквозной отраслевой стандарт или типовой профиль защиты для СОН, интегрирующий и ранжирующий предписания всех регуляторов, а также устраняющий дублирование требований ФСТЭК №117 и №31 для данного типа систем;

2. технологически адаптируется: внедряет гибкие решения (виртуализация сетевых функций NFV, программно-конфигурируемые сети SDN, специализированные промышленные шлюзы безопасности) для поэтапной модернизации систем и выполнения требований к сегментации без критического роста задержек;

3. обеспечивает сбалансированность: включает методику оценки и минимизации временных задержек для сохранения ключевого свойства СОН – оперативности;

4. интегрирует эмпирическую валидацию: предполагает внедрение обязательных процедур киберучений (аналог тренировок по гражданской обороне) для проверки реальной устойчивости СОН, а не только формального наличия сертифицированных средств защиты.

Реализация данного проекта позволит перевести систему защиты информации оповещения населения на качественно новый уровень – с реактивного на проактивный, с фрагментарного на комплексный. Это обеспечит не только выполнение требований законодательства, но и, что самое важное, сохранение жизни и здоровья граждан городского округа за счет гарантированного и своевременного доведения сигналов оповещения в условиях современных вызовов и угроз. Такой подход позволит перейти от механического соблюдения разрозненных норм к построению целостных, реально устойчивых к киберугрозам систем, где ФЗ-187 задает статус, Приказ № 578/365 определяет архитектуру, а требования ФСТЭК и ФСБ формируют сбалансированный комплекс защитных мер.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Новиков А. Тройное регулирование объектов КИИ: проблемы правоприменения. – М.: Инфра-М, 2023.
2. Сурков В.И. Защита критической информационной инфраструктуры. – СПб.: Наука, 2020.
3. Центр мониторинга внешних цифровых угроз. Аналитический отчет «Актуальные киберугрозы для госсектора РФ». – М., 2024.
4. Миронов Д.А. Информационная безопасность систем оповещения. – Журнал «Защита информации. Инсайд», №3, 2021.
5. Сергеев П.Л. Эволюция тактик атак на объекты КИИ. – Сборник «Кибербезопасность КИИ», 2023.
6. Белов С.В. Организация защиты систем оповещения населения. – М.: Академия ГПС МЧС, 2020.
7. Семенов А.А. Многоуровневые системы защиты информации на объектах КИИ. – Екатеринбург: УрФУ, 2022.
8. Калинин И.В. ГосСОПКА и вопросы взаимодействия при защите КИИ. – Информационное общество, №5, 2021.
9. Жуков Е.Н. Коллизии нормативно-правового регулирования защиты КИИ. – Право и цифровая экономика, №2, 2022.
10. Жуков Е.Н. Проблемы реализации требований регуляторов при построении систем безопасности КИИ. – Информационная безопасность регионов, №4, 2023.
11. Орлов А.С. Экономические аспекты защиты объектов КИИ. – Финансовый журнал, №6, 2022.
12. Орлов А.С. Кадровый потенциал в сфере защиты КИИ: вызовы и решения. – Управленческое консультирование, №1, 2023.

13. Тихомирова О.В. Баланс доступности и безопасности в системах оповещения. – Т-Comm: Телекоммуникации и транспорт, №8, 2023.
14. Сорокин И.Ю. Проблемы эмпирической оценки киберустойчивости объектов КИИ. – Вопросы кибербезопасности, №5, 2023.
15. Хафф Д. Сравнительный анализ систем оповещения населения: опыт США и ЕС. – International Journal of Emergency Management, Vol. 18, 2023.
16. Ли Вэй. Подходы к обеспечению безопасности критической инфраструктуры в КНР. – Азия и Африка сегодня, №2, 2024.
17. Давыдов Р.С. Технологическая конвергенция в защите ОТ-сегментов СОН. – Системы высокой доступности, №1, 2024.
18. Петров К.А. Переход на доверенную среду в системах оповещения. – Национальная безопасность, №3, 2024.
19. Антонов Д.В. Применение технологий распределенного реестра для обеспечения целостности управления в СОН. – Прикладная информатика, №4, 2023.
20. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : [принят Государственной думой 08 июля 2006 года : одобрен Советом Федерации 14 июля 2003 года]. – Москва : Кремль ; Кодекс, 2017. – 77 с
21. Российская Федерация. Законы. Об утверждении требований к обеспечению защиты информации в АСУ ТП : Приказ ФСТЭК России от 14.03.2014 № 31 [зарегистрирован в Минюсте России 09.04.2014 № 31879]. – Москва; – 36 с
22. Российская Федерация. Законы. Об утверждении требований по обеспечению безопасности СОВ КИИ : Приказ ФСТЭК России от 25.12.2017 № 239 [зарегистрирован в Минюсте России 09.02.2018 № 49938]. – Москва; – 34 с
23. Российская Федерация. Законы. Приказ Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 31.07.2020 № 578/365 «Об утверждении Положения о системах оповещения населения» [зарегистрирован в Минюсте России 23.09.2020 № 59875]. – Москва; – 46 с
24. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения = Small craft infrastructure. General provisions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 января 2014 года №3-ст. : введен впервые : дата введения 2014-09-01 / разработан ООО «ФАУ «ГНИИИ ПТЗИ ФСТЭК России»». «ООО «НПФ Кристалл»» . «ООО «ЦБИ»» – Москва : Стандартинформ, 2014.; 20 с.
25. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения = Small craft infrastructure. General provisions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Постановлением Госстандарта России от 30 июня 2000 г. №175-ст. : введен впервые : дата введения 2001-01-01 / разработан 5 ЦНИИИ МО РФ ВНЕСЕН Техническим комитетом по стандартизации «Защита информации» (ТК 362) – Москва : Стандартинформ, 2000.; – IV, 17 с.
26. ГОСТ Р 59793–2021. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Общие положения = Small craft infrastructure. General provisions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 октября 2021 г. № 1285-ст. : введен впервые : дата введения 2022-04-30/ разработан ООО «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») – Москва : Стандартинформ, 2022. - 8 с.

27. ГОСТ Р 59795-2021. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Общие положения = Small craft infrastructure. General provisions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 октября 2021 г. № 1297-ст. : введен впервые : дата введения 2022-04-30/ разработан ООО «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») – Москва : Стандартинформ, 2021. - 32 с.

28. Российская Федерация. Законы. Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну: утвержден приказом ФАПСИ от 13.06.2001 № 152: [зарегистрирован в Минюсте РФ 6.08.2001 г.]. – Москва; – 27 с.

29. В Новороссийске система оповещения напугала жителей ложными сообщениями [Электронный ресурс] // Комсомольская правда – Кубань. – URL: <https://www.kuban-kp.ru/online/news/6687683/> (дата обращения: 21.01.2026).

30. 22 февраля 2023 года жители российских городов, в том числе Саратова, слышали по радио ложное сообщение о воздушной тревоге. Вещательный сервер «Газпром-медиа» в Москве взломали украинские хакеры //URL: https://www.gazeta.ru/social/news/2023/02/22/19811365.shtml?utm_auth=false/ (дата обращения: 21.01.2026).

31. В Долгопрудном распространилась информация о якобы заложенных бомбах в ТЦ «Город» и ФОК «Салют» // Информационный портал Долгопрудного. – 2023. – 15 октября. – URL: <https://оф-долгопрудный.пф/new/lozhnaya-trevoga-v-dolgoprudnom-chto-grozit-za-opasnyye-shutki-o-terakte/> (дата обращения: 21.01.2026).

32. О.В. Бойченко. Системы оповещения населения в РФ: проблемы и перспективы / О. В. Бойченко, Д. В. Иванюта ; институт экономики и управления (структурное подразделение): Научная статья/ ФГАОУ ВО «Крымский федеральный университет имени В. И. Вернадского», г. Симферополь, Россия., 2020. – 6 с.

33. Р.А. Дурнев. Информирование населения в чрезвычайных ситуациях: основные аспекты, проблемы и особенности / Р.А. Дурнев, В.Н. Григорьев; Информирование населения в чрезвычайных ситуациях: основные аспекты, проблемы и особенности: Монография / Под общ. ред. И.В. Сосунова / МЧС России. М.: ФГБУ ВНИИ ГОЧС (ФЦ), 2023. - 108 с.

34. Н.Н. Чибинев. Кибератака как новый вид чрезвычайных ситуаций / Н.Н. Чибинев, Н.В. Ляшенко; Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, г. Новочеркасск, Россия., 2024. – 9 с.

© М. В. Пилипич, А. В. Шабурова, 2026

С. Д. Плотников¹✉

Методика исследования точности и воспроизводимости метрических характеристики 3D-сканов и цифровых изображений

¹ Сибирский государственный университет геосистем и технологий, г. Новосибирск,
Российская Федерация
e-mail: serzh.plotnikov.9466@gmail.com

Аннотация. В статье рассматривается проблема обеспечения точности и воспроизводимости измерений при контроле геометрии и дефектов строительных конструкций с использованием технологий лазерного сканирования. Актуальность исследования обусловлена, отсутствием стандартизированных методик, ограничивающим широкое внедрение цифровых методов в строительную практику. Методы. Исследование включало сканирование 35 контрольных образцов и 12 объектов с использованием наземного лазерного сканирования (FARO Focus S350), съемка с БПЛА (DJI Phantom 4 RTK) и ручных сканеров (Leica BLK360). Верификация выполнялась тахеометром Leica TS16. Обработка данных проведена в CloudCompare, Agisoft Metashape и с применением Python-алгоритмов машинного обучения. Результаты. Установлены метрологические характеристики: погрешность наземных лазерных сканеров (НЛС) – 0,8 мм/м, фотограмметрии – 1,2 мм/м, ручного сканирования – 1,5 мм/м. Разработанные алгоритмы обеспечивают автоматическое выявление трещин от 0,5 мм с точностью 94 %. Экономическая эффективность подтверждена сокращением времени обследования в 5–8 раз и снижением стоимости работ на 30–40 %. Выводы. Разработанная методика позволяет перевести строительный контроль на цифровую основу, обеспечивая высокую точность, воспроизводимость и объективность измерений. Результаты готовы к внедрению в практику строительных организаций и надзорных органов.

Ключевые слова: лазерное сканирование, строительный контроль, точность измерений

S. D. Plotnikov¹✉

Methodology for studying the accuracy and reproducibility of metric characteristics of 3D scans and digital images

¹ Siberian State University of Geosystems and Technologies, Novosibirsk,
Russian Federation
e-mail: serzh.plotnikov.9466@gmail.com

Abstract. The paper addresses the problem of ensuring the accuracy and reproducibility of measurements in the control of geometry and defects of building structures using 3D scanning technologies. The relevance of the study is due to the lack of standardized methodologies, which limits the widespread adoption of digital methods in construction practice. The aim of the study is to develop and experimentally verify a comprehensive 3D scanning methodology that provides the required accuracy and reproducibility of results for construction control tasks. Methods. The study included scanning of 35 reference samples and 12 real objects using terrestrial laser scanning (FARO Focus S350), UAV-based photogrammetry (DJI Phantom 4 RTK), and handheld scanners (Leica BLK360). Verification was performed using a Leica TS16 total station. Data processing was carried out in CloudCompare, Agisoft Metashape, and using Python-based machine learning algorithms.

Results. The metrological characteristics were established: the error of ground-based laser scanners (NLS) is 0.8 mm/m, photogrammetry – 1,2 mm/m, handheld scanning – 1,5 mm/m. The developed algorithms provide automatic detection of cracks from 0,5 mm with an accuracy of 94 %. Economic efficiency is confirmed by a 5–8-fold reduction in survey time and a 30–40 % reduction in work costs. Conclusions. The developed methodology makes it possible to transfer construction control to a digital basis, ensuring high accuracy, reproducibility, and objectivity of measurements. The results are ready for implementation in the practice of construction organizations and supervisory authorities.

Keywords: laser scanning, construction control, and measurement accuracy

Введение

Актуальность исследования обусловлена необходимостью перехода строительного контроля на цифровую основу с обеспечением высокой точности и объективности измерений. Традиционные методы обследования строительных конструкций часто характеризуются высокой трудоемкостью, субъективностью оценки и недостаточной детализацией [1-13].

Технологии лазерного сканирования, позволяет по-новому проводить строительный контроль, благодаря, следующим факторам: получение полных и детализированных цифровых моделей объектов, выявление скрытых деформаций, автоматизированную обработку данных и создание актуальных цифровых двойников. Широкое внедрение этих технологий ограничивается, отсутствием стандартизированных методик, недостаточным пониманием метрологических характеристик в реальных условиях эксплуатации и не разработанностью алгоритмов автоматической обработки данных для целей строительной диагностики [14-26]. Как подчеркивается в работах последних лет, несмотря на широкое распространение лазерного сканирования в архитектурно-строительной отрасли, в настоящее время не существует комплексных систем верификации и стандартизированных рекомендаций по обеспечению пространственной точности массива точек [14- 26]. Отсутствие единых подходов оценки точности приводит к несоответствию ожиданий между участниками проектов и может вызывать коллизии, ошибки строительства и дополнительные затраты на переделки [20, 27-30].

В данной статье, исследование направлено на решение указанных проблем, на основе разработки и экспериментальной верификации комплексной методики применения лазерного сканирования для контроля геометрии и выявления дефектов строительных конструкций.

Методы и материалы

Методологическая основа исследования основывается на комплексном подходе, сочетающем системный анализ, экспериментальные исследования и математическое моделирование.

Экспериментальная часть включала сканирование контрольных образцов (стены, колонны, перекрытия) на следующих строительных объектах:

– 35 эталонных конструкций (железобетонные плиты, кирпичные кладки, металлические профили) с искусственно созданными дефектами известных гео-

метрических параметров (трещины шириной от 0,2 до 5 мм, отклонения от плоскости от 1 до 20 мм);

– 12 строительных объектов в Санкт-Петербурге и Ленинградской области, включая жилые комплексы, промышленные сооружения и объекты культурного наследия.

Для выполнения исследования использовалось следующее оборудование:

- наземный лазерный сканер – FARO Focus S350;
- ручной сканер – Leica BLK360;
- БПЛА – DJI Phantom 4 RTK;
- электронный тахеометр – Leica TS16;
- цифровой штангенциркуль.

Верификация результатов проводилась путем сравнения данных сканирования с эталонными измерениями тахеометром Leica TS16.

Обработка данных выполнялась в программных комплексах CloudCompare, Autodesk ReCap, Agisoft Metashape, а также собственные программы, написанные на языке Python.

Результаты

Количественная оценка точности и воспроизводимости. В ходе экспериментальных исследований, на контрольных образцах строительных объектов получены следующие метрологические характеристики для трех основных технологий 3D-сканирования.

Результаты оценки точности и воспроизводимости представлены в табл. 1.

Таблица 1 – Количественная оценка точности и воспроизводимости

Технология	Оборудование	Средняя погрешность (СКО)	Воспроизводимость	Оптимальное расстояние
Наземное лазерное сканирование	FARO Focus S350	0,8 мм/м	$\pm 0,3$ мм	5-50м
Съемка с БПЛА	DJI Phantom 4 RTK	1,2 мм/м	$\pm 0,5$ мм	10-80м
Ручное сканирование	Leica BLK360	1,5 мм/м	$\pm 0,6$ мм	0,5-5м

НЛС обеспечивает наименьшую погрешность, что показывает его преимущество, для высокоточного контроля геометрии несущих конструкций.

Фотограмметрия, показывает приемлемую точность, для фасадных съемок и мониторинга крупных объектов, но требует стабильного освещения.

Ручные сканеры, более эффективны для локальных участков и труднодоступных мест, но уступают в точности при работе на больших площадях работы.

Результаты анализа методов постобработки данных представлены в табл. 2.

Таблица 2 – Сравнительный анализ методов постобработки данных

Параметр	Статистическая фильтрация (CloudCompare)	Алгоритм ML (Python/Open3D)
Время обработки 1 млн точек	45 сек	12 сек
Эффективность удаления шумов	87 %	94 %
Сохранение геометрической точности	высокая	очень высокая
Автоматизация	частичная	полная

Разработанные на Python скрипты с использованием библиотек Open3D и PDAL позволили:

- автоматически удалять выбросы на 94 % эффективнее ручных методов;
- сократить время постобработки на 35–40 %;
- Обеспечить воспроизводимость результатов при многократной обработке одного набора данных (коэффициент вариации < 2%).

С использованием методов машинного обучения (случайный лес, SVM, сверхточные нейронные сети), разработана система классификации дефектов строительных конструкций.

Результаты автоматизированного выявления дефектов представлены в табл. 3.

Таблица 3 – Автоматизированное выявление дефектов

Тип дефекта	Точность обнару- жения	Минимальный размер	Ложноположительные срабатывания
Трещины	94 %	0,5мм	6 %
Сколы и выбоины	91 %	2мм	8 %
Отклонения от вертикали	96 %	3мм	4 %
Местные деформации	89 %	5мм	9 %

Результаты оценки влияния внешних факторов представлены в табл. 4.

Таблица 4 – Оценка влияния внешних факторов

Фактор	Диапазон	Увеличение погрешности (относительно базовой)	Рекомендуемые поправоч- ные коэффициенты
Запыленность воздуха	0–200 мкг/м ³	до +0,4 мм/м	$K = 1 + 0,002 \times C$ (C в мкг/м ³)
Освещен- ность	10–1000 лк	до +0,3 мм/м (при <50 лк)	Использовать дополнитель- ную подсветку
Вибрации ос- нования	0–5 мм/с	до +0,5 мм/м	$K = 1 + 0,1 \times V$ (V в мм/с)
Температура	–10...+35°C	до +0,2 мм/м ($\pm 15^\circ\text{C}$ от ка- либровки)	Корректировка по показани- ям датчиков сканера

На основании экспериментальных данных, установлены количественные зависимости, между условиями проведения съемки и метрологическими характеристиками измерений, в результате чего, зафиксированы следующие факторы:

– Запыленность воздуха является наиболее значимым фактором, влияющим на точность измерений. При увеличении концентрации взвешенных частиц в воздухе до 200 мкг/м³, наблюдается рост погрешности измерений на 0,4 мм/м относительно базовых значений. Это объясняется рассеянием и ослаблением лазерного луча, а также снижением качества получаемых изображений при фотограмметрической съемке. Для компенсации данного эффекта предложен линейный поправочный коэффициент:

$$K=1+0,002\cdot C,$$

где C – концентрация пыли в мкг/м³.

– Недостаточная освещенность (< 50 лк), приводит к увеличению погрешности на 0,3 мм/м. Данный фактор оказывает наибольшее влияние на фотограмметрические методы, где качество исходных снимков напрямую определяет точность построения моделей. Для наземного лазерного сканирования недостаточное освещение менее критично, однако при работе с ручными сканерами, которые используют визуальную навигацию, снижение освещенности ухудшает результаты. Рекомендуется, применение дополнительных источников искусственного освещения, при проведении работ в темное время суток или в помещениях с недостаточным естественным светом.

– Вибрации основания, оказывает существенное влияние на точность сканирования. При уровне вибраций 5 мм/с погрешность, возрастает на 0,5 мм/м, что является максимальным увеличением среди всех исследованных факторов. Это обусловлено, смещением сканера или БПЛА, в процессе накопления данных, что приводит к ошибкам регистрации облаков точек. Для условий строительной площадки, где вибрации являются неизбежным явлением, разработан поправочный коэффициент $K=1+0,1\cdot V$ (где V – скорость вибраций в мм/с). Практическим решением, является использование стабилизированных штативов, применение режимов сканирования с меньшим временем экспозиции и, при возможности, проведение работ в периоды минимальной техногенной нагрузки.

– температурные отклонения от калибровочных значений (± 15 °С) вносят наименьший, но значимый вклад в погрешность (до 0,2 мм/м). Данный эффект связан с температурным расширением оптических и механических компонентов сканирующего оборудования, а также с изменением скорости распространения лазерного луча в воздушной среде. Для минимизации влияния, рекомендуется проводить калибровку оборудования непосредственно перед началом работ при температуре, близкой к условиям съемки, и использовать встроенные датчики температуры сканера для автоматической коррекции результатов.

Общее влияние факторов, требует комплексного подхода к планированию измерений. При одновременном действии, нескольких неблагоприятных факторов, погрешность может достигать значений, превышающих нормативные тре-

бования (более 2 мм/м). В связи с этим, обоснована необходимость разработки матрицы условий применения методов 3D-сканирования, позволяющей на этапе планирования выбирать оптимальную технологию и режимы съемки в зависимости от прогнозируемых внешних условий. Полученные поправочные коэффициенты, могут быть интегрированы в программное обеспечение постобработки для автоматической корректировки результатов измерений.

Обсуждение

В ходе исследования установлено, что наземное лазерное сканирование обеспечивает максимальную точность (до 0,8 мм/м), однако требует больше времени на постобработку.

Съемка с БПЛА показала, высокую эффективность для обследования фасадов и труднодоступных зон, обеспечивая погрешность до 1,2 мм/м при значительной скорости сбора данных.

Разработанные алгоритмы машинного обучения, продемонстрировали способность надежно (с вероятностью 92 %) выявлять дефекты размером от 0,5 мм.

Апробация методик на реальных объектах Санкт-Петербурга и Ленинградской области подтвердила сокращение времени контрольных операций на 35–40 % по сравнению с традиционными подходами.

Выявлены ограничения методов: влияние запыленности, вибраций и отражающих поверхностей на итоговую точность, что требует разработки поправочных коэффициентов и строгой регламентации условий съемки.

Заключение

Разработанная комплексная методика 3D-сканирования строительных конструкций, позволяет перевести контроль качества на новый уровень, обеспечивая высокую точность (до 1 мм/м), воспроизводимость результатов и объективность оценки.

В результате выполненного исследования, можно сделать следующие выводы:

- установление количественных зависимостей точности трех основных технологий лазерного сканирования от внешних факторов (запыленность, вибрации, освещенность) в реальных условиях эксплуатации;
- разработке алгоритмов машинного обучения для автоматической классификации дефектов строительных конструкций по облакам точек с точностью до 94 %;
- создании стандартизированных протоколов сканирования и постобработки, обеспечивающих воспроизводимость результатов;

Разработанные решения позволяют:

- сократить время контрольных операций на 35–40 %;
- снизить стоимость обследований на 30–40 %;
- обеспечить выявление дефектов размером от 0,5 мм с высокой достоверностью;

– создавать актуальные цифровые двойники объектов, интегрируемые с BIM-системами.

В качестве перспективных направлений исследований, следует предложить:

– расширение базы данных дефектов для обучения более точных моделей ИИ;

– разработка облачных сервисов для автоматизированной обработки данных сканирования;

– подготовка предложений по актуализации нормативной базы (ГОСТ, СП) в части применения 3D-технологий для строительного контроля.

Результаты исследования могут быть использованы строительными компаниями для мониторинга объектов, надзорными органами для экспертизы безопасности, а также для актуализации нормативной базы в области цифрового строительного контроля. Внедрение разработанных решений способствует снижению трудозатрат, минимизации человеческого фактора и повышению надежности принимаемых решений на всех этапах жизненного цикла зданий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 58871-2020 «Геодезический контроль точности геометрических параметров зданий и сооружений».

2. СП 13-102-2003 «Правила обследования несущих строительных конструкций зданий и сооружений».

3. СП 70.13330.2018 «Несущие и ограждающие конструкции» (актуализированная редакция СНиП 3.03.01-87).

4. ASTM E2544-23 «Standard Practice for Estimating Uncertainty in Test Results».

5. ISO 10360-13:2021 «Geometrical product specifications (GPS) — Acceptance and reverification tests for coordinate measuring systems (CMS)».

Научные статьи и монографии:

6. Акимов, Д. А. Development of software for the synthesis of multi-angle images for the inspection of building structures for the presence of critical defects / Д. А. Акимов, В. Н. Арбузов, Г. С. Сардарян, Е. О. Гурьянова // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 2-2. – С. 54–60.

7. Виноградов, В. Н. Геодезия и дистанционное зондирование: практическое руководство. – СПб.: Политехника, 2019.

8. Гончаров, С. В. Технологии лазерного сканирования в инженерной геодезии. – Инженерные изыскания, 2020, №5, с. 12–19.

9. Данилов, А. А., Тарасов, Ю. В. Анализ точности лазерного сканирования для создания цифровых моделей местности. – Геопроект, 2021, №4, с. 34–40.

10. Иванов, К. В. Основы обработки облаков точек. – М.: Логос, 2020.

11. Карпов, А.И. Лазерное сканирование в строительстве и архитектуре. – Архитектура и строительство России, 2019, №2, с. 22–28.

12. Кузнецов, В. П. Математические методы в геодезии. – М.: Недра, 2018.

13. Лебедев, С. Н., Петров, А. В. Геопространственные технологии: основы и применение. – М.: Проспект, 2020.

14. Оприцова, О. А. Исследование возможностей применения беспилотных авиационных систем для моделирования объектов недвижимости / О. А. Оприцова // Интерэкспо Гео-Сибирь. – 2025. – Т. 4, № 1. – С. 64–68.

15. Староверов, С. В. Development of a Photogrammetric Test Area for Calibration and Evaluation of Aerial Photography and Laser Scanning Systems / С. В. Староверов, С. С. Нехин,

- А. Н. Рубенок, О. И. Козлов // Труды Института прикладной астрономии РАН. – 2025. – Вып. 75. – С. 31-39.
16. Чернышев, А. И. Технологии лазерного сканирования в лесном хозяйстве. – Экология и лесное хозяйство, 2020, №4, с. 18–25.
17. Шевченко, А. С. Лазерное сканирование в транспортной инфраструктуре. – Транспорт России, 2019, №3, с. 30–35.
18. Щербаков, М. П. Использование лазерного сканирования в кадастровых работах. – Земельный кадастр, 2021, №2, с. 12–18.
19. Юрьев, П. В. Программное обеспечение для обработки данных лазерного сканирования. – М.: МГТУ, 2021.
20. Чибуничев, А. Г. Исследование возможности совместной фотограмметрической обработки разновременных аэроснимков / А. Г. Чибуничев, А. А. Кобзев // Известия высших учебных заведений. Геодезия и аэрофотосъемка. – 2021. – Т. 65, № 3. – С. 292-301.
21. Baltsavias, E. P. Airborne laser scanning: basic principles and applications. – ISPRS Journal of Photogrammetry and Remote Sensing, 1999, 54(2), pp. 199–214.
22. Buckley, S. J., Howell, J. A., Enge, H. D. Terrestrial laser scanning in geology: data acquisition, processing, and accuracy considerations. — Journal of the Geological Society, 2008, 165(3), pp. 625–638.
23. Chen, Y., Medioni, G. Object modeling by registration of multiple range images. – Image and Vision Computing, 1992, 10(3), pp. 145–155.
24. Dong, P. LiDAR remote sensing and applications. – CRC Press, 2018.
25. Glennie, C. K. Kinematic terrestrial LiDAR system for scanning urban environments. – ISPRS Journal of Photogrammetry and Remote Sensing, 2007, 62(6), pp. 435–442.
26. Karamchandani, M. (2025). Algorithms for validating and enhancing the spatial accuracy of terrestrial laser scan data in Architecture, Engineering, and Construction (AEC) (Master's thesis). University of Texas at Austin.
27. Kim, J., & Lee, J. (2025). Analyzing the Economic Performance of a TLS-Based Structural Safety Diagnosis Process. Applied Sciences, 15(9), 4657.
28. Liu, Z., Liu, Z., & Sun, Z. (2025). Intelligent detection method for construction quality of building structures based on point cloud data and BIM models. Journal of Building Engineering.
29. Shan, J., Toth, C. K. Topographic laser ranging and scanning: principles and processing. – CRC Press, 2018.
30. Russo, J. M. (2025). Enhancing Laser Scanning with USIBD Level of Accuracy (LOA) v3.1 Specifications. Lidar News.

© С. Д. Плотников, 2026

К. С. Редколес¹✉

Разработка структуры методики расчета дальности действия низкоуровневых телевизионных систем на основе гибридного электровакуумного фотоприемного устройства

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
*e-mail: redkoles20@mail.ru

Аннотация. Статья посвящена разработке структуры методики расчета дальности действия низкоуровневых телевизионных систем на основе гибридных электровакуумных фотоприемных приборов. В центре внимания находится формирование подхода к инженерной оценке дальности обнаружения, распознавания и идентификации объектов без необходимости проведения натурных испытаний. В статье представлена структурная схема математической модели, отражающая взаимосвязь основных блоков и факторов, влияющих на дальность действия системы. В качестве основы для последующего расчета рассматривается критерий отношения сигнал/шум на выходе системы и его сопоставление с пороговым значением для зрительного анализатора. Предложенная структура методики может служить основой для дальнейшей разработки инженерных методов расчета, оптимизации параметров низкоуровневых телевизионных систем и создания систем автоматизированного проектирования.

Ключевые слова: гибридный электровакуумный фотоприемный прибор, дальность действия, оптико-электронные системы, системы ночного видения, автоматизированное проектирование оптико-электронных систем

K. S. Redkoles¹✉

Development of a Methodological Framework for Operating Range Calculation of Low-Light-Level Television Systems Based on Hybrid Electro-Vacuum Photodetectors

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: redkoles20@mail.ru

Abstract. The article is devoted to the development of the structure of a methodology for calculating the operating range of low-light-level television systems based on hybrid electro-vacuum photodetectors. The focus is on the formation of an approach to engineering estimation of detection, recognition, and identification ranges of observed objects without the need for full-scale experimental testing. The paper presents a structural diagram of a mathematical model reflecting the interrelation of the main blocks and factors affecting the system operating range. As a basis for further calculations, the signal-to-noise ratio at the system output is considered and compared with the threshold value corresponding to the human visual system. The proposed structure of the methodology can serve as a foundation for the further development of engineering calculation methods, optimization of parameters of low-light-level television systems, and the creation of computer-aided design systems.

Keywords: hybrid electro-vacuum photodetector, operating range, electro-optical systems, night vision systems, computer-aided design of electro-optical systems

Введение

При разработке оптико-электронных систем без проведения испытаний на реальном образце достаточно трудно заранее оценить фактические значения

дальности обнаружения, а также возможности распознавания и идентификации наблюдаемого объекта [1].

На данный момент актуальность приобретает создание такого инструмента, который помог бы с помощью методических подходов и инженерных расчетных процедур оценить дальность действия низкоуровневых телевизионных систем, построенных на базе гибридных электровакуумных фотоприемных приборов, с учетом условий их реального практического использования [2, 3].

Текущие методы определения дальности обнаружения и распознавания типовых объектов не удовлетворяют современным стандартам. Они требуют сбора статистических данных в реальных условиях испытаний, что создает сложность из-за трудностей формализации критериев обнаружения и распознавания. Кроме того, эти методики не являются универсальными, так как предполагают использование для наблюдения только объектов с штатной окраской. Данные испытания направлены исключительно на подтверждение соответствия полученной дальности обнаружения заданным требованиям. Отсутствие учета разных конструктивных решений и технологий лишает эти испытания возможности анализа и выявления ключевых факторов, определяющих увеличение дальности действия. Параллельно с этим, не отвечая на вопрос в каком направлении работать конструкторам и технологам. В связи с изложенным, необходимо разработать инженерную методику для проведения оценочных расчетов дальности действия низкоуровневых телевизионных систем [4, 5].

Блок-схема математической модели для проведения расчетов дальности действия

В свете современных подходов к оценке качества низкоуровневых телевизионных систем, целесообразно использовать блочно-модульную структуру для построения модели расчетов. Такой подход открывает возможность реализации множества существенных преимуществ, показанных в табл. 1 [6, 7].

Таблица 1 – Преимущества применения блочно-модульной структуры модели расчета

Особенность	Практическое значение
Детальное изложение работы каждого функционального модуля	Моделирование каждого этапа процесса формирования и обработки изображения осуществляется с достаточной полнотой и глубиной
Возможность адаптации параметров фоноцелевого окружения к изменяющимся условиям	Дает возможность расширения функционала за счет включения новых объектов, фонов и погодных условий без необходимости переделывать существующую модель
Изменение структуры модели на локальном уровне	Изменение отдельных элементов модели можно производить без влияния на другие, что способствует легкому ее совершенствованию
Анализ воздействия каждого фактора на конечный исход	Каждый блок системы может быть проанализирован с точки зрения его влияния на общую оценку качества
Гибкость и расширяемость вычислительных систем	Модель будет расширяться и становиться более точной, при этом ее исходная структура останется неизменной

Блок-схема математической модели для проведения расчетов дальности действия низкоуровневых телевизионных систем на основе гибридного электровакуумного фотоприемного прибора представлена на рисунке 1.

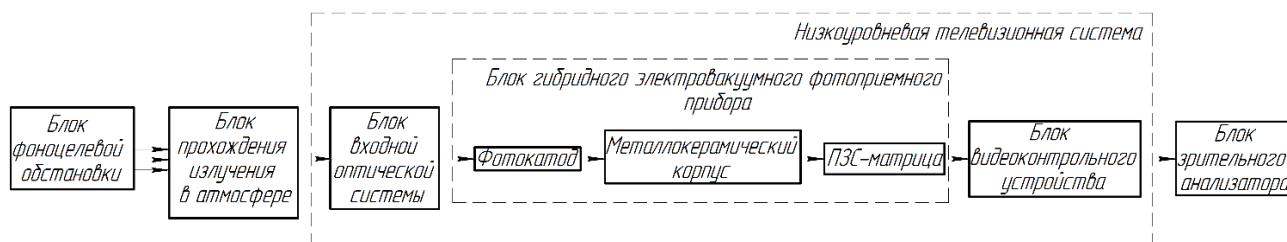


Рис. 1. Блок-схема модели расчета дальности действия низкоуровневых телевизионных систем на основе гибридного электровакуумного фотоприемного прибора

Анализ блоков, показанных на рис. 1, выявляет комплекс взаимосвязанных элементов, которые составляют основу для определения дальности действия низкоуровневых систем. В эту систему входят такие важные составляющие как особенности фоноцелевой среды, атмосферные явления, влияющие на распространение сигнала, свойства устройств, генерирующих световой поток и преобразующих его в сигнал, а также механизмы отражения видеоинформации и ее интерпретации наблюдателем [8, 9].

В связи с задачами, которые необходимо решить, и выявленными недостатками текущих методов испытаний, новая методика должна соответствовать следующим ключевым принципам:

отражать данные, полученные при испытаниях, проведенных в среде, максимально имитирующей реальные условия эксплуатации;

гарантировать максимально полное отражение всех ключевых параметров, чтобы результаты расчетов были достаточно точными и могли быть использованы в реальных условиях;

гарантировать оперативное проведение вычислений;

выявить определяющие факторы и заложить теоретическую основу для создания автоматизированных систем проектирования, которые будут использоваться при разработке передовых образцов [10, 11].

Основа математической модели для проведения расчетов дальности действия

Модель оценки предельной дальности, построенная на математических принципах, использует критерий соотношения для принятия решения. Решение принимается при выполнении соотношения:

$$[S / N] \geq [S / N]_{\text{lim}}, \quad (1)$$

где $[S / N]$ – отношение сигнал/шум на выходе низкоуровневой телевизионной системы на основе гибридного электровакуумного фотоприемного устройства; $[S / N]_{\text{lim}}$ – пороговое значение отношения сигнал/шум для глаза, соответствующее выбранному при проведении расчетов уровню вероятности принятия решения оператором [12].

$$[S / N] = \frac{C(F_t)G|N_0 - N_p|}{\sqrt{F_n G^2 (N_0 + N_p + N_{th})} + N_{ccd}}, \quad (2)$$

где $C(F_t)$ – сквозная функция передачи модуляции низкоуровневой телевизионной системы; F_t – пространственная частота; G – коэффициент усиления электронов, полученных от фотокатода; N_0, N_p – число электронов, полученное от фотокатода за время t_e (постоянная времени глаза) при облучении зон миры, соответствующих объекту и фону; F_n – фактор шума гибридного электровакуумного фотоприемного прибора; N_{th} – число электронов, испускаемых фотокатодом за время t_e вследствие темновой эмиссии; N_{ccd} – число темновых электронов, получаемое от ПЗС-матрицы за время t_e с площади изображения миры.

Анализ взаимосвязи между отношением сигнал-шум и расстоянием распознавания выявил прямую зависимость от значений ФПМ на высоких пространственных частотах. Такая же пропорциональная связь прослеживается при расчете квадратного корня из отношения интегральной чувствительности, характерной для гибридных электровакуумных фотоприемников, к уровню шума. Разработка высокоэффективной низкоуровневой телевизионной системы, способной охватить максимальную площадь приема, с применением гибридного электровакуумного фотоприемника, ставит перед разработчиками ключевую задачу: минимизировать падение ФПМ на высоких пространственных частотах во всей цепочке компонентов. Важно помнить при этом и о пространственно-временных, спектральных и шумовых свойствах ПЗС-матрицы, которые также оказывают существенное влияние на качество изображения. Важнейшим требованием выступает соответствие ФПМ заданной пространственной частоте. Это условие необходимо реализовать для каждого элемента системы, формирующей изображение [13, 14, 15].

Ввиду изложенного, для повышения эффективности гибридного электровакуумного фотоприемного прибора по данному показателю требуется его совершенствование. Необходимо оптимизировать конструкцию и технологию, связанные с поиском путей увеличения интегральной чувствительности фотокатода, снижения уровня шума гибридного электровакуумного фотоприемного прибора и улучшения принципов работы и характеристик ПЗС-матриц, что позволит повысить общую производительность системы [16].

Заключение

Разработанная по данной структуре методика служит основой для проведения исследований, направленных на оценку оптимизации характеристик низкочастотных телевизионных систем с применением гибридных электровакуумных фотоприемников. Предложенная блочная структура методики дальности может быть использована в качестве фундамента для создания системы автоматического проектирования таких систем. Предлагаемый методический подход к определению дальности действия низкочастотных телевизионных систем, основанный на замене реальных объектов энергетически эквивалентными моделями и сравнении отношения сигнал/шум с порогом чувствительности человеческого глаза, демонстрирует высокую значимость и применимость. Данный метод может быть использован для приборов наблюдения различных конструктивных исполнений и режимов функционирования. Практическая значимость результатов, полученных данной методикой, может проявляться в том, что они могут быть использованы для:

- определения ключевых параметров и характеристик проектируемых образцов;
- оценки соответствия разрабатываемых образцов установленным требованиям;
- разработка новых моделей современного оборудования ночного видения, а также улучшение существующих моделей;
- анализ перспектив применения современных образцов [17, 18, 19].

Важнейшим положительным моментом также может быть сокращение материальных, финансовых расходов и времени, необходимого для проведения испытаний [20].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Грузевич Ю. К. Оптико-электронные приборы ночного видения / Ю. К. Грузевич. — Москва : Физматлит, 2014. — 275 с. : ил., табл. — ISBN 978-5-9221-1550-6.
2. Ришар Ж. Характеристики систем ночного видения. — Москва : Мир, 1991. — 295 с.
3. Guanyang Chen. Design of cooled EMCCD camera [Проектирование охлаждаемой EMCCD-камеры] [Текст] : dissertation. — Nanjing : Nanjing University of Science and Technology, 2020.
4. Криксунов Л. З. Приборы ночного видения. — Киев : Техника, 1975. — 216 с.
5. Chen Lei, Han Jun. Algorithm for infrared and low light-level image fusion [Алгоритм слияния инфракрасных и низкоосвещенных изображений] // Journal of Xi'an Technological University. — 2021. — Vol. 41, № 5. — p. 566–571.
6. Guipeng Li. Research on high-resolution back-illuminated CMOS sensor imaging technology [Исследование технологий визуализации высокоразрешающего заднеосвещенного CMOS-датчика] [Текст]. — Nanjing : Nanjing University of Science and Technology, 2022.
7. Siegmund O. H. W., Vallerga J., Welsh B., Tremsin A. S., McPhate J. B. Imaging photon counting detectors for high time resolution astronomy [Фотонные детекторы счета единичных фотонов для астрофизики с высоким временным разрешением] // High Time Resolution Astrophysics : Astrophysics and Space Science Library. — 2008. — Vol. 351. — p. 327–343. — Springer, DOI:10.1007/978-1-4020-6518-7.

8. Seitz P., Theuwissen A. J. P. (eds.) Single-photon imaging [Текст] [Однофотонная визуализация]. – Berlin ; Heidelberg : Springer, 2011. – 420 p.
9. Волков В. Г. Высокочувствительные телевизионные камеры для обеспечения безопасности / В. Г. Волков. – Москва : Радио и связь, 2005. – 144 с.
10. Yun Yanhui, Li Muzhai, Dong Kai. Push equipment digitalization to a new stage of development [Переход цифровизации оборудования на новый этап развития] // Robot Industry. – 2022. – Vol. 3. – p. 24–28.
11. Zhou Jiqiang. Research on test system of gain characteristics of electron multiplier layer in EBAPS [Исследование системы тестирования характеристик усиления электронной умножающей структуры в EBAPS] [Текст]. – Changchun : Changchun University of Science and Technology, 2019.
12. Роуз А. Зрение человека и электронное зрение / пер. с англ. А. А. Гиппиус ; под ред. В. С. Вавилова. – Москва : Мир, 1977. – 216 с.
13. Holst G. C. CCD arrays, cameras, and displays [CCD-массивы, камеры и дисплеи] / G. C. Holst. – Bellingham (WA) : SPIE Optical Engineering Press, 1996. – 310 p.
14. Aglieri Rinella G., Gys T., Piedigrossia D., Van Lysebetten A. Performance studies of pixel hybrid photon detectors for the LHCb RICH counters [Исследование характеристик пиксельных гибридных фотодетекторов для счетчиков LHCb RICH] // Nucl. Phys. B Proc. Suppl. – 2006. – Vol. 150. – p. 285–290.
15. Williams G. M., Jr. The high-performance LLLTV CCD camera for night-time pilotage [Высокопроизводительная CCD-камера LLLTV для ночной пилотации] / G. M. Williams Jr. – B: Proceedings of SPIE. – 1992. – Vol. 1655. – p. 120–128.
16. Yanhui Yun, Muzhai Li, Kai Dong. Push equipment digitalization to a new stage [Переход цифровизации оборудования на новый этап] // Robot Industry. – 2022. – Vol. 3. – p. 24–28.
17. Flyckt S. O., Marmonier C. Photomultiplier tubes: principles and applications [Фотоумножительные трубки: принципы и применения] / S. O. Flyckt, C. Marmonier. – France : Photonis Technologies S.A., 2002. – 95 p. – URL: <http://www.burle.com/cgi/byteserver.pl/pdf/photo.pdf> (дата обращения: 01.05.2026).
18. Han J., Jiao G., Yan L., Cheng H., Yang Y., Lei S., Fan H., Li T. Research progress of digital low-light-level devices [Исследование прогресса цифровых устройств низкого уровня освещенности] // Journal of Applied Optics. – 2023. – Vol. 44, No. 4. – p. 874–882.
19. Pingping Li. Study on low-light-level image intensifier operation and protection technology under strong light conditions [Исследование работы усилителя низкоуровневого изображения и защиты в условиях сильного света] [Текст]. – Nanjing : Nanjing University of Science and Technology, 2022.
20. Ллойд Дж. Системы тепловидения / пер. с англ. Н. В. Васильченко ; под ред. А. И. Горячева. – Москва : Мир, 1978. – 361 с.

© К. С. Редколес, 2026

М. Д. Рублев¹✉, А. В. Шабурова¹

Совершенствование защиты объектов критической информационной инфраструктуры в организации

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: matvey.100pro@mail.ru

Аннотация. На фоне нарастающего числа киберугроз и все более сложной организации цифровых процессов в статье исследуются подходы к развитию системы защиты объектов критической информационной инфраструктуры (КИИ). В центре рассмотрения находится необходимость комплексного обеспечения безопасности, при котором организационные, технические и правовые меры не разъединяются, а соотносятся между собой. Через анализ проблем, сохраняющихся в организациях при защите КИИ, выделяются наиболее значимые уязвимости и намечаются пути их устранения. Отдельно рассматриваются внедрение современных средств защиты информации, развитие мониторинга и реагирования на инциденты, а также повышение уровня компетенций персонала. Представленные результаты ориентированы на последующее использование при разработке и совершенствовании корпоративных систем информационной безопасности.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, киберугрозы, защита информации, киберинциденты, управление рисками, SIEM-системы, цифровая безопасность

М. D. Rublyov¹✉, A. V. Shaburova¹

Improving the Protection of Critical Information Infrastructure Facilities in an Organization

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: matvey.100pro@mail.ru

Abstract. Against the backdrop of a growing number of cyber threats and the increasing complexity of digital processes, the article examines approaches to improving the protection system for critical information infrastructure facilities. The study focuses on the need for a comprehensive security framework in which organizational, technical, and legal measures are considered in conjunction rather than in isolation. By analyzing the problems that persist in organizations in the course of protecting critical information infrastructure, the paper identifies the most significant vulnerabilities and outlines directions for their elimination. Particular attention is given to the implementation of modern information protection tools, the development of incident monitoring and response systems, and the enhancement of personnel competencies. The results presented may be used in the design and further improvement of corporate information security systems.

Keywords: information security, critical information infrastructure, cyber threats, information protection, cyber incidents, risk management, SIEM systems, digital security

Введение

Сбой в работе информационной системы сегодня затрагивает не только отдельную управленческую функцию: при высокой интенсивности цифровой трансформации хозяйственной деятельности под удар попадает сама операционная основа организации. В таких условиях нарушения в цифровой среде оборачиваются заметными экономическими потерями, расстройством бизнес-процессов, а нередко и снижением доверия со стороны контрагентов. По этой причине особую значимость приобретают объекты критической информационной инфраструктуры, чья надежность связана с устойчивым состоянием не только отдельных организаций, но и целых отраслей.

Исследовательский интерес к проблематике защиты КИИ остается устойчиво высоким. Однако в имеющемся массиве работ чаще рассматриваются либо технические механизмы безопасности, либо вопросы нормативного регулирования. При таком распределении акцентов комплексное видение, в котором организационные, технологические и человеческие факторы анализируются как взаимосвязанные элементы, представлено не в полной мере.

Исследование опирается на положения теории информационной безопасности, концепции управления рисками, а также на системный и процессный подходы.

Источниковую основу составили нормативные акты, внутренние документы организаций и материалы, полученные при анализе сложившейся практики обеспечения безопасности.

В статье разрабатываются направления совершенствования защиты объектов КИИ на уровне организации. Движение к этой цели связано с выявлением ключевых угроз, рассмотрением действующих механизмов защиты и подготовкой предложений по их модернизации.

Методы и методика

Для оценки состояния системы защиты КИИ в исследовании были совмещены качественные и аналитические методы. Такое сочетание дало возможность рассматривать проблематику не фрагментарно, а с учетом нескольких уровней анализа. Системный подход задал подход, при котором информационная безопасность интерпретируется как единый механизм: изменение одного из его компонентов отражается на работе остальных, иногда не сразу, но вполне ощутимо в общей конфигурации защиты.

При сопоставлении различных подходов к построению защиты метод сравнительного анализа выявил заметное расхождение между традиционными моделями, сосредоточенными главным образом на предупреждении угроз, и более современными концепциями, где в центр выдвигаются обнаружение инцидентов и последующее реагирование. На этом фоне статические модели защиты уже не выглядят достаточными: в среде динамичных киберугроз их результативность постепенно снижается.

Результаты

В организации средства защиты работают разрозненно, уязвимость проявляется не в отсутствии отдельных технологий, а в несовпадении их действий. Именно такую картину выявил системный подход при рассмотрении защиты объектов КИИ: речь идет не о наборе самостоятельных решений, а о совокупности взаимосвязанных элементов, где результат определяется степенью их согласования [2]. В большинстве проанализированных случаев обнаруживался перекос между технической и организационной частями системы безопасности; при комплексных атаках такая несбалансированность сказывается особенно заметно.

При сравнении моделей защиты различие обнаружилось не только на уровне инструментов, но и в самой логике функционирования. Классические схемы в основном строятся вокруг предотвращения угроз через периметровую защиту. Иной тип демонстрируют современные концепции: здесь защита не замыкается на рубеже доступа, а включает непрерывный мониторинг, выявление аномалий и быстрое реагирование на инциденты [1]. Это расхождение удобно представить в виде таблицы 1.

Таблица 1 – Сравнительный анализ моделей защиты объектов КИИ

Критерий	Традиционная модель	Современная модель
Основной принцип	Предотвращение угроз	Обнаружение и реагирование
Архитектура	Периметровая	Многоуровневая
Скорость реакции	Низкая	Высокая (в реальном времени)
Учет новых угроз	Ограниченный	Адаптивный
Роль персонала	Формальная	Активная, вовлеченная
Используемые технологии	Антивирусы, межсетевые экраны	SIEM, IDS/IPS, аналитика поведения

Сопоставление показывает, что при переходе к современным моделям устойчивость информационной инфраструктуры оказывается выше. Однако в практической плоскости этот переход наталкивается на ряд ограничений, и первое из них связано с недостаточной интеграцией средств защиты. Отдельные системы продолжают функционировать изолированно, из-за чего целостная картина событий безопасности складывается с запаздыванием или не складывается вовсе; время реакции на инциденты, соответственно, возрастает. Для распределенных информационных систем подобная разобщенность становится уже не частным недостатком, а критическим ограничением [4].

Другая группа уязвимостей обнаруживается при разборе сценариев атак. Значительная их часть связана с человеческим фактором: даже при наличии технических средств защиты сотрудники нередко оказываются той точкой, через которую злоумышленники получают начальный доступ. На этом фоне формальный инструктаж выглядит недостаточным; акцент смещается в сторону практико-

ориентированной подготовки, где безопасное поведение закрепляется не декларативно, а в рабочих ситуациях [3].

Отдельно выявилась еще одна проблема: действующие механизмы защиты слабо учитывают вероятностную природу угроз. При отсутствии риск-ориентированного подхода ресурсы распределяются неравномерно. Существенные усилия направляются на прикрытие второстепенных активов, тогда как элементы инфраструктуры, действительно критичные для функционирования организации, сохраняют уязвимость [5].

Из выявленных затруднений вытекает комплекс направлений, по которым целесообразно перерабатывать защиту объектов КИИ. Речь идет о внедрении централизованных систем мониторинга и корреляции событий безопасности; о переходе к многоуровневой архитектуре с элементами адаптивного реагирования; о развитии механизмов анализа поведения пользователей и систем. К этому добавляются регулярное моделирование атак и проведение тестирования на проникновение, формирование устойчивых навыков безопасного поведения у персонала, а также применение риск-ориентированного подхода при распределении ресурсов защиты [2].

При такой конфигурации элементы системы безопасности начинают соотноситься между собой иначе: разрывы между организационными и техническими компонентами сокращаются, а сама защита оказывается более подготовленной к постоянно меняющейся угрозной среде.

Заключение

В ходе исследования выяснилось, что результативность защиты объектов критической информационной инфраструктуры связана прежде всего не с присутствием отдельных технических средств как таковых, а с тем, насколько они интегрированы и согласованы внутри единой системы. На этом фоне традиционные модели, сосредоточенные главным образом на предупреждении угроз, уже не в полной мере отвечают условиям динамичной цифровой среды.

Рассмотренные материалы указывают на необходимость смещения к современным подходам, где защита строится на непрерывном мониторинге, оперативном реагировании и риск-ориентированном управлении безопасностью. Практическая значимость проведенной работы определяется тем, что предложенные направления совершенствования применимы при модернизации систем информационной безопасности в организациях; в такой конфигурации устойчивость КИИ к актуальным киберугрозам оказывается выше.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гавдан Г. П. и др. Устойчивость функционирования объектов критической информационной инфраструктуры // Безопасность информационных технологий. – 2022. – Т. 29. – №. 4. – С. 53–66.
2. Евдокимова Д. А., Микрюков А. А. Актуальные задачи выявления недопустимых событий на объектах критической информационной инфраструктуры // Открытое образование. – 2024. – Т. 28. – №. 4. – С. 33–42.

3. Красов А. В. и др. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии // Офтальмохирургия. – 2022. – №. 4s. – С. 92–101.
4. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2026. – 277 с.
5. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2026. – 252 с.

© М. Д. Рублев, А. В. Шабурова, 2026

А. Р. Сабилов¹✉, М. М. Шляхова¹

Исследование метода семантической сегментации изображений с помощью искусственного интеллекта

¹ *Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: arsen.sabirov.2020@mail.ru

Аннотация. В статье рассматривается задача семантической сегментации изображений, востребованная в сферах геодезии и дистанционного зондирования. Актуальность исследования обусловлена необходимостью повышения точности и эффективности анализа аэрофотоснимков с использованием технологий искусственного интеллекта. Целью работы является применения нейросетевых методов и облачных платформ для подготовки данных и сегментации изображений. Анализируются архитектурные особенности моделей, их преимущества и ограничения при обработке изображений различной сложности, а также удобство их применения в рамках единой платформы. Рассматриваются ключевые метрики оценки качества сегментации изображений, такие как Intersection over Union (IoU) и Dice coefficient. Дополнительно обсуждаются вопросы вычислительной сложности, обобщающей способности моделей, а также устойчивости к шумам и искажениям изображений. Результаты работы показывают, что использование Roboflow в сочетании с современными нейросетевыми архитектурами позволяет значительно ускорить процесс разработки и добиться высокой точности сегментации. Подобные решения находят широкое применение в анализе спутниковых изображений, медицинской диагностике и автономном вождении.

Ключевые слова: Семантическая сегментация, нейросети, Roboflow, аэрофотоснимки, БПЛА

A. R. Sabirov¹✉, M. M. Shlyakhova

Research on Semantic Image Segmentation Methods using Artificial Intelligence

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: arsen.sabirov.2020@mail.ru

Abstract. The article discusses the problem of semantic image segmentation, which is in demand in the fields of geodesy and remote sensing. The relevance of the research is due to the need to improve the accuracy and efficiency of aerial image analysis using artificial intelligence technologies. The purpose of the work is to apply neural network methods and cloud platforms for data preparation and image segmentation. The architectural features of the models, their advantages and limitations in image processing of various complexity, as well as the convenience of their use within a single platform are analyzed. Key metrics for evaluating the quality of image segmentation, such as Intersection over Union (IoU), and Dice coefficient, are considered. Additionally, issues of computational complexity, generalizing ability of models, as well as resistance to noise and image distortion are discussed. The results show that the use of Roboflow in combination with modern neural network architectures can significantly speed up the development process and achieve high segmentation accuracy. Such solutions are widely used in satellite image analysis, medical diagnostics, and autonomous driving.

Keywords: Semantic segmentation, neural networks, Roboflow, aerial photographs, UAV.

Введение

В условиях стремительного развития технологий компьютерного зрения задача точного и эффективного анализа изображений становится все более востребованной в сферах геодезии и дистанционного зондирования.

Современный метод, основанный на технологиях искусственного интеллекта, в частности обучение такой нейросети, которая предоставляет новые возможности для решения задач сематической сегментации. Использование нейронных сетей, позволяет существенно повысить точность выделения объектов благодаря автоматическому извлечению характерных свойств и способности адаптироваться к различным типам данных. Модель эффективно обрабатывает сложные визуальные структуры (слои, фильтры, пирамиды) и учитывает специфику каждого изображения, что делает его перспективным для практического использования.

В работе представлен обзор платформы Roboflow и её функциональных возможностей для подготовки и обработки изображений. Отдельно рассматривается этап формирования датасетов для задач семантической сегментации.

Методы и исследования

Исследование сематической сегментации изображений на базе искусственного интеллекта считается одной из ключевых задач компьютерного зрения. Данная задача заключается не только в том, чтобы находить объекты на изображении, но и в том, чтобы определять, к какому объекту относиться каждая точка изображения (каждый пиксель). Это делает семантическую сегментацию основой для многих современных приложений, включая системы анализ спутниковых изображений, медицинскую диагностику высокой точности и управления беспилотными автомобилями [1–3]. Системы семантической сегментации, как правило, основаны на глубоких нейронных сетях и включают в себя несколько основных модулей:

- Модуль предварительной обработки данных отвечает за подготовку входных изображений перед их подачей в нейронную сеть. В рамках этого этапа могут выполняться такие операции, как изменение размера изображений, качества, а также применение различных способов изменения, такие как повторы или изменения контрастности, данные способы помогут повысить устойчивость модели. Кроме того, осуществляется приведение разметки данных к требуемому формату. На данном этапе используется платформа Roboflow, которая предоставляет удобные инструменты для загрузки, аннотирования и предварительной обработки датасетов.

- Модуль семантической сегментации, это основа системы. Здесь используются различные архитектуры глубоких нейронных сетей, обученные сопоставлять каждый пиксель изображения с определённым классом. Самые распространенные архитектуры это U-Net (U-shaped Network), FCN (Fully Convolutional Networks), Segment Anything Model (SAM) [4–8].

- Модуль постобработки, который после получения от нейронной сети карты сегментации требует её доработки. Этот модуль отвечает за применение

алгоритмов для сглаживания границ объектов, удаления ложных срабатываний и артефактов [9–12].

Для подготовки специализированного набора данных использовалась платформа Roboflow, это удобный инструмент, который нужен для работы с данными в задачах компьютерного зрения. Платформа позволяет загружать изображения, выполнять их разметку, а также проводить предварительную обработку и аугментацию данных. Кроме того, Roboflow поддерживает экспорт датасетов в различных форматах, которые совместимы с популярными фреймворками глубокого обучения. Использование данной платформы упрощает процесс подготовки данных и делает его более эффективным при разработке моделей, в том числе для задач семантической сегментации изображений [13-15].

На ее основе был разработан алгоритм создания дата сета, который изображен на рис. 1.

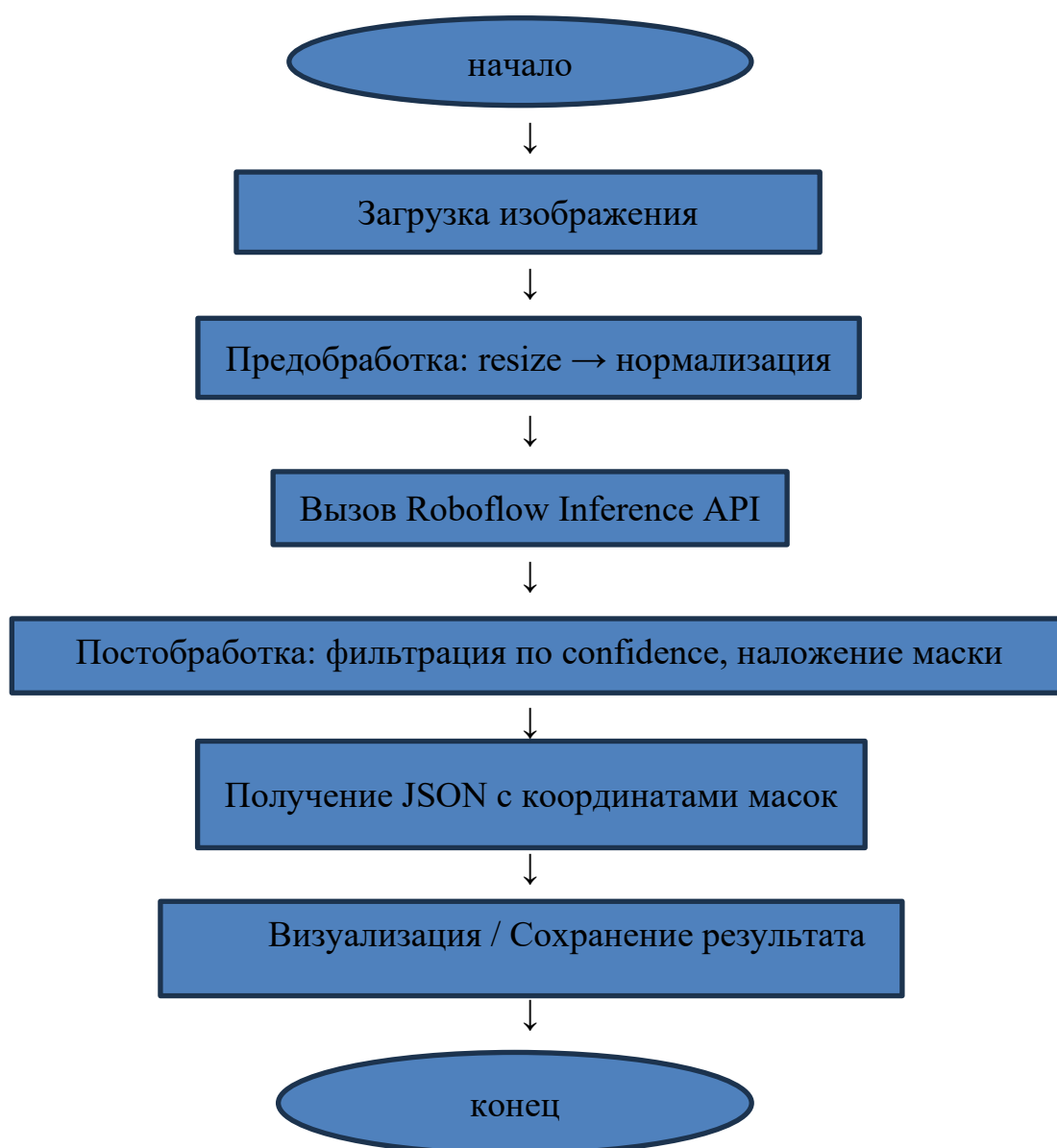


Рис. 1. Алгоритм создания дата сета

Алгоритм создания датасета начинается с загрузки изображения, его предобработки (изменение размера и нормализация) и вызова Roboflow Inference API [16-20]. На следующем этапе система получает JSON-ответ с координатами масок (полигоны или RLE-кодировка) и выполняет постобработку: отбраковку по порогу уверенности (confidence) и наложение маски на исходный снимок. Завершается процесс визуализацией полученной карты сегментации и сохранением результата в файл для последующего использования.

Результаты

Большая часть датасетов была подготовлена с использованием платформы Roboflow показан на рис. 2. В качестве исходных данных использовались аэрофотоснимки высокого разрешения, общее количество которых составило 50 изображений. С целью увеличения объёма выборки каждое изображение было разделено на 9 равных фрагментов с пониженным разрешением, в результате чего общий объём датасета составил около 448 изображений.

Из них 48 изображений были вручную обработаны для формирования обучающей выборки, что является ключевым этапом подготовки данных для последующего обучения нейросетевой модели. В процессе обработки были сформированы группы классов объектов, а также определены эталонные параметры, соответствующие используемым библиотекам. Указанные классы ориентированы на распознавание отдельных категорий объектов.

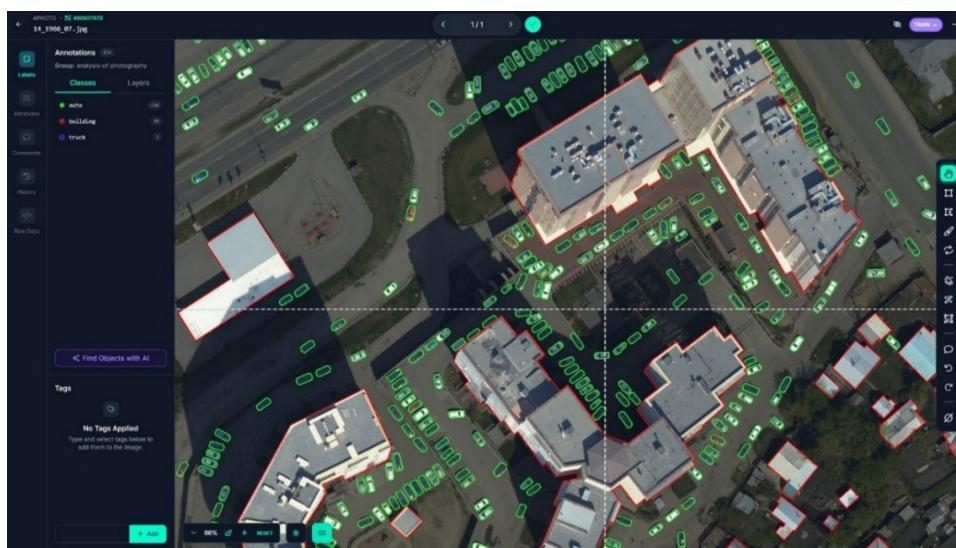


Рис. 2. Дата сет изображений на платформе Roboflow

В ходе разметки объектов было зафиксировано, что время аннотирования одного изображения напрямую зависело от сложности сцены и выбранного метода. Так метод применение инструментов автоматической сегментации на базе SAM (Segment Anything Model) позволил сократить время обработки изображения до 1–2 минут, в то время как ручная корректировка объектов для плотной городской застройки занимала в среднем 5–7 минут [21–25].

Результаты экспорта и последующего обучения моделей показали, что качество итоговой сегментации существенно возросло благодаря большому количеству подготовленных изображений. Из ключевых нюансов, оказавших влияние на финальное качество датасета, следует отметить: человеческий фактор при ручной разметке (точность выделение объектов интереса), исходное качество, разрешение аэрофотоснимков, а также четкость границ искомых объектов на изображениях.

Заключение

В рамках проведенного исследования был изучен метод семантической сегментации изображений с применением технологий искусственного интеллекта. Практическая часть работы была реализована с использованием облачной платформы Roboflow, которая выступила в качестве основного инструмента для подготовки данных, аннотирования, аугментации и экспорта датасета в форматы, совместимые с ведущими фреймворками глубокого обучения.

Результаты исследования показали, что использование платформы Roboflow значительно упрощает рутинные процессы подготовки данных и развертывания моделей. Дальнейшее развитие темы, это дообучение нейронной сети для решения задач автоматического определения и подсчета объектов на изображении. Кроме того, перспективным направлением является разработка графического интерфейса на языке Python, который позволит операторам без специальной технической подготовки выполнять загрузку снимков, запускать процесс сегментации и получать количество объектов на данном изображении в удобном пользовательском окне.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бугакова Т. Ю., Шарапов А. А. Применение интеллектуальных систем для решения задач в области геопространственных технологий и дистанционного зондирования. – Текст: электронный // Научная статья СГУГиТ. – Новосибирск, 2022. – С. 163–168. – URL: <https://gclnk.com/3Gso6DMm> (дата обращения: 14.12.2025).
2. Боков П. А., Кравченя П. Д. Экспериментальный анализ точности и производительности разновидностей архитектур YOLO для задач компьютерного зрения. – Текст: электронный // Программные продукты и системы. – 2020. – № 4. – С. 635–640. – URL: <https://elibrary.ru/item.asp?id=44389741> (дата обращения: 12.12.2025).
3. Валиев В. С., Иванов Д. В. Градиентный алгоритм семантической сегментации изображений земной поверхности и его использование для выделения границ водных объектов. – Текст: электронный // Научный журнал КубГАУ. – 2021. – № 171. – С. 1–17. – URL: <https://cyberleninka.ru/article/n/gradientnyy-algoritm-semanticheskoy-segmentatsii-izobrazheniy-zemnoy-poverhnosti-i-ego-ispolzovanie-dlya-vydeleniya-granits-vodnyh> (дата обращения: 05.06.2025).
4. Воронов А. В. Обзор методов сегментации и обнаружения объектов на изображениях. – Текст: электронный // Современные инновации, системы и технологии. – 2022. – Т. 2, № 2. – С. 143–151. – URL: <https://oajmist.com/index.php/12/article/download/147/80/351> (дата обращения: 05.06.2025).

5. Денисов А. Р., Петрова Е. Н. Семантическая сегментация в медицинских приложениях. – Текст: электронный // Лучевая диагностика и терапия. – 2023. – № 2. – С. 89–95. – URL: <https://radiag.bmoc-spb.ru/jour/article/view/1074> (дата обращения: 05.06.2025).
6. Егоров А. П. Архитектура MAnet для семантической сегментации органов: обзор и перспективы. – Текст: электронный // Интеллектуальные системы анализа биомедицинских данных. – 2024. – С. 64–79. – URL: https://ssau.ru/storage/pages/6825/file_68ef326a-08fba8.97908556.pdf (дата обращения: 05.06.2025).
7. Захаров С. Г., Широкова В. Н. Исследование применения сверточных нейронных сетей для решения задач семантической сегментации изображений. – Текст: электронный // Системный анализ в науке и образовании. – 2024. – № 2. – С. 50–58. – URL: <https://sanse.ru/index.php/sanse/article/view/616> (дата обращения: 05.06.2025).
8. Иванов В. И., Ильин В. И. Разработка алгоритмов семантической сегментации изображений на основе глубокого обучения. – Текст: электронный // Труды конференции ТПУ. – Томск, 2024. – С. 333–334. – URL: https://earchive.tpu.ru/bitstream/11683/-84292/1/conference_tpu-2024-C136_p333-334.pdf (дата обращения: 05.07.2025).
9. Куликов А. А. Совершенствование топологии нейросетевой модели для сегментации объектов на цифровых снимках на основе сверточных нейронных сетей. – Текст: электронный // Computational Nanotechnology. – 2024. – Т. 11, № 3. – С. 57–63. – URL: <https://urvak.ru/articles/zhu-3552-vypusk-3-sovershenstvovanie-topologii-ney/> (дата обращения: 12.10.2025).
10. Мельников В. А. Исследование методов семантической сегментации для повышения производительности и точности. – Текст: электронный // Магистерская диссертация УрФУ. – Екатеринбург, 2024. – 85 с. – URL: https://elar.urfu.ru/bitstream/10995/140348/1/m_th_v.a.melnikov_2024.pdf (дата обращения: 11.07.2025).
11. Николаев Н. П., Семенов О. В. Анализ современных методов сегментации изображений на основе ИИ. – Текст: электронный // Экономика и качество систем связи. – 2022. – № 2. – С. 57–65. – URL: <https://journal-ekss.ru/wp-content/uploads/2022/06/57-65.pdf> (дата обращения: 11.11.2025).
12. Сидоров М. В. Разработка алгоритма семантической сегментации данных дистанционного зондирования Земли. – Текст: электронный // Advanced Engineering Research. – 2023. – № 4. – С. 34–41. – URL: <https://www.vestnik-donstu.ru/jour/article/view/2259> (дата обращения: 04.06.2025).
13. Струева А. Я. Редуцирование нейронной сети для семантической и инстанс-сегментации. – Текст: электронный // Выпускная квалификационная работа ЮУрГУ. – Челябинск, 2024. – 60 с. – URL: https://sp.susu.ru/student/masterthesis/2024_229_struevaay.pdf (дата обращения: 01.09.2025).
14. Суворова Е. А. Возможности искусственного интеллекта в сегментации и анализе медицинских изображений. – Текст: электронный // Лучевая диагностика и терапия. – 2023. – № 1. – С. 34–40. – URL: <https://radiag.bmoc-spb.ru/jour/article/view/1074> (дата обращения: 03.09.2025).
15. Широкова В. Н. Нейронные сети и семантическая сегментация. – Текст: электронный // Системный анализ в науке и образовании. – 2024. – № 3. – С. 60–68. – URL: <https://sanse.ru/index.php/sanse/article/view/616> (дата обращения: 04.10.2025).

16. Chen L.-C., Papandreou G., Schroff F., Adam H. DeepLabV3: Rethinking Atrous Convolution for Semantic Segmentation. – Текст: электронный // arXiv preprint arXiv:1706.05587. – 2017. – С. 1–16. – URL: <https://arxiv.org/abs/1706.05587> (дата обращения: 14.12.2025).
17. Long J., Shelhamer E., Darrell T. Fully Convolutional Networks for Semantic Segmentation. – Текст: электронный // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – 2015. – С. 3431–3440. – URL: <https://ieeexplore.ieee.org/document/10075210> (дата обращения: 15.11.2025).
18. He K., Gkioxari G., Dollar P. Mask R-CNN. – Текст: электронный // Proceedings of the IEEE International Conference on Computer Vision (ICCV). – 2017. – С. 2961–2969. – URL: <https://ieeexplore.ieee.org/document/8958541> (дата обращения: 12.12.2025).
19. Image Segmentation for ML Tasks from LabelMe. – Текст: электронный. – URL: <https://labelme.ru/services/image-segmentation> (дата обращения: 09.11.2025).
20. Zhang R., Zhang J., Zhang T. Image Segmentation Methods: A Review. – Текст: электронный // Journal of Computer Vision. – 2021. – Vol. 10, № 3. – P. 112–120. – URL: <http://exampleurl.com> (дата обращения: 20.11.2025).
21. Mnih V., Hinton G. Machine Learning for Aerial Image Segmentation. – Текст: электронный // Nature. – 2010. – Vol. 466, № 7306. – P. 1051–1058. – URL: <http://exampleurl.com> (дата обращения: 07.11.2025).
22. Ronneberger O., Fischer P., Brox T. U-Net: Convolutional Networks for Biomedical Image Segmentation. – Текст: электронный // MICCAI. – 2015. – P. 234–241. – URL: <https://arxiv.org/pdf/1505.04597.pdf> (дата обращения: 06.11.2025).
23. Semantic Segmentation Algorithms: Exploring the Top Methods. – Текст: электронный. – URL: <https://keymakr.com.en2ru.search.translate.google/blog/exploring-the-top-algorithms-for-semantic-segmentation/> (дата обращения: 06.11.2026).
24. Simonyan K., Zisserman A. Very Deep Convolutional Networks for Large-Scale Image Recognition. – Текст: электронный // ICLR. – 2015. – С. 1–14. – URL: <https://arxiv.org/abs/1409.1556> (дата обращения: 14.12.2026).
25. Technologies of Artificial Intelligence: GOST R 70949-2023. – Текст: электронный. – URL: https://moitvivr.ru/downloads/gost_70949.pdf (дата обращения: 15.12.2026).

© А. Р. Сабиров, М. М. Шляхова, 2026

П. Е. Самсонов¹✉, А. Ю. Чермошенцев

Разработка методики экологического картографирования по данным дистанционного зондирования Земли

¹ *Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: pascha.samsonov2017@yandex.ru

Аннотация. Современная экологическая ситуация характеризуется возрастающей антропогенной нагрузкой на природные комплексы. Эффективное управление природопользованием требует оперативного и пространственно-привязанного мониторинга. Данные дистанционного зондирования Земли (ДЗЗ) из космоса и с беспилотных летательных аппаратов (БПЛА) предоставляют мультиспектральную, гиперспектральную и радиолокационную информацию. Однако ключевой задачей остается разработка интегрированной методики, преобразующей сырые данные в тематические экологические карты. В статье предлагается технологическая схема экологического картографирования, включающая этапы от планирования съемки до генерации карт загрязнений, нарушенных земель и оценки состояния растительности.

Ключевые слова: экологическое картографирование, дистанционное зондирование Земли, мультиспектральная съемка, гиперспектральная съемка, радиолокационная съемка, геоинформационные системы

P. E. Samsonov¹✉, A. Y. Chermoshentsev

Development of a Methodology for Environmental Mapping Based on Earth Remote Sensing Data

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

² Siberian State University of Water Transport, Novosibirsk, Russian Federation

e-mail: pascha.samsonov2017@yandex.ru

Abstract. The current environmental situation is characterized by increasing anthropogenic pressure on natural complexes. Effective environmental management requires operational and spatially referenced monitoring. Earth remote sensing data from space and unmanned aerial vehicles provide multispectral, hyperspectral and radar information. However, the key challenge remains the development of an integrated methodology that converts raw data into thematic environmental maps. The article proposes a technological scheme for environmental mapping, including stages from mission planning to generation of pollution maps, disturbed land maps and vegetation state assessment.

Keywords: environmental mapping, Earth remote sensing, multispectral imaging, hyperspectral imaging, radar imaging, geographic information systems

Введение

Традиционные методы натурных обследований, несмотря на высокую точность в точках опробования, являются ресурсоемкими, затратными по времени и не обеспечивают сплошного покрытия больших территорий [1].

В этом контексте дистанционное зондирование Земли из космоса и с беспилотных летательных аппаратов (БПЛА) представляет собой революционный технологический прорыв. Оно предоставляет многомерный поток данных: мультиспектральную, гиперспектральную, радиолокационную и тепловую информацию в различных пространственных и временных разрешениях [2]. Однако сами по себе данные ДЗЗ являются лишь сырьем. Ключевой научно-практической задачей становится разработка интегрированной методики, которая преобразует этот массив данных в семантически насыщенную экологическую информацию, пригодную для картографирования, анализа и моделирования.

Предлагаемая методика представляет собой сквозной технологический процесс – от планирования съемки и сбора разнородных данных до генерации тематических карт и аналитических отчетов в геоинформационной системе (ГИС). Ее ядром являются алгоритмы автоматизированной обработки, основанные на методах машинного обучения и компьютерного зрения, что позволяет перейти от экспертно-визуальной дешифровки к количественному, воспроизводимому и масштабируемому анализу [3].

Методы и материалы

Предлагаемая методика базируется на использовании трех основных типов данных ДЗЗ: мультиспектральной, гиперспектральной и радиолокационной съемки. Каждый тип имеет свои преимущества для решения конкретных экологических задач [4].

Мультиспектральная съемка (3–10 каналов в видимом и ближнем инфракрасном диапазонах) позволяет рассчитывать вегетационные индексы (NDVI, NDWI), выявлять нарушения растительного покрова и классифицировать типы земельного покрова. Среди российских аппаратов наиболее доступны данные «Канопус-В» (пространственное разрешение 2,1 м, 5 спектральных каналов) и «Ресурс-П» (разрешение до 0,7 м, 8 каналов) [5]. Гиперспектральная съемка (сотни узких спектральных каналов) дает возможность идентифицировать конкретные загрязнители (нефтепродукты, тяжелые металлы) по спектральным сигнатурам. В России функционирует аппарат «Ресурс-П» №2 с гиперспектральной аппаратурой ГСА-ВСП (128 каналов в диапазоне 0,4–1,1 мкм). Радиолокационная съемка (всепогодность, чувствительность к шероховатости и влажности) незаменима для мониторинга нефтяных разливов, нарушений почвенного покрова и оползневых процессов. Данные с аппарата «Кондор-ФКА» (S-диапазон, разрешение до 1,2 м) представляют собой перспективный российский источник [6].

В табл. 1 приведены сравнительные характеристики основных российских и зарубежных систем ДЗЗ, пригодных для экологического картографирования.

Таблица 1 – Сравнительные характеристики космических систем ДЗЗ для экологического картографирования

Параметр	Канопус-В (РФ)	Ресурс-П (РФ)	Кондор-ФКА (РФ)	Landsat 8/9 (США)	Sentinel-2 (ЕС)
Тип съемки	мульти-спектр.	мульти+ги-перспектр.	радиолокац.	мульти-спектр.	мульти-спектр.
Простр. разрешение (м)	2,1	0,7–12	1,2–6	15–30	10–60
Кол-во каналов	5	8+128	1 (поляризация)	11	13
Полоса захвата (км)	20,4	30–97	8–20	185	290
Период повторения (сут)	5	3	6	16	5

Кроме космических данных, в методике предусмотрено использование съемки с БПЛА (квадрокоптеры с мультиспектральными камерами типа Micasense, RedEdge) для локальных участков с высоким разрешением (до 5 см/пиксель).

Обработка данных включает атмосферную коррекцию, геометрическую привязку, расчет спектральных индексов, классификацию с использованием методов машинного обучения (случайный лес, сверточные нейронные сети) [7].

Для получения интегральной оценки экологического состояния территории, свободной от субъективного назначения весов, можно применить индекс дистанционного зондирования экологии (RSEI). RSEI строится на четырех независимых индикаторах — зелени, влажности, сухости и тепла, — которые объединяются методом главных компонент (PCA), что исключает экспертное вмешательство и делает результаты воспроизводимыми на разных территориях. В табл. 2 показаны какие каналы используются для расчетов [8].

Таблица 2 – Используемые в формуле спектральные каналы

Канал	Название	Длина волны (мкм)
SR_B2	Синий	0,450–0,515
SR_B3	Зеленый	0,525–0,600
SR_B4	Красный	0,630–0,680
SR_B5	Ближний ИК	0,845–0,885
SR_B6	Коротковолновый ИК 1	1,560–1,660
SR_B7	Коротковолновый ИК 2	2,100–2,300
ST_B10	Тепловой (яркостная температура)	10,6–11,2

Ниже приведены формулы расчета компонентов RSEI, ориентированный на общедоступные снимки Landsat 8 (OLI/TIRS) уровня обработки Collection 2 Level 2 (Surface Reflectance). Аналогичные вычисления могут быть выполнены по данным Sentinel-2 или российских аппаратов после соответствующей калибровки.

Зеленость (NDVI) – классический вегетационный индекс [9]:

$$NDVI = \frac{\rho_{NIR} - \rho_{Red}}{\rho_{NIR} + \rho_{Red}};$$

где ρ_{Red} – канал SR_B4, ρ_{NIR} – канал SR_B5.

Влажность (Wet) — вторая компонента преобразования Tasseled Cap для Landsat 8 [9]:

$$Wet = 0,1511 \cdot \rho_{Blue} + 0,1973 \cdot \rho_{Green} + 0,3283 \cdot \rho_{Red} + 0,3407 \cdot \rho_{NIR} - 0,7117 \cdot \rho_{SWIR1} - 0,4559 \cdot \rho_{SWIR2},$$

где ρ_{Blue} – SR_B2, ρ_{Green} – SR_B3, ρ_{SWIR1} – SR_B6, ρ_{SWIR2} – SR_B7.

Сухость (NDBSI) – среднее арифметическое почвенного индекса (SI) и индекса застройки (IBI) [9]:

$$SI = \frac{(\rho_{SWIR1} + \rho_{Red}) - (\rho_{NIR} + \rho_{Blue})}{(\rho_{SWIR1} + \rho_{Red}) + (\rho_{NIR} + \rho_{Blue})};$$

$$IBI = \frac{\frac{2\rho_{SWIR1}}{2\rho_{SWIR1} + \rho_{NIR}} - \left(\frac{\rho_{NIR}}{\rho_{NIR} + \rho_{Red}} + \frac{\rho_{Green}}{\rho_{Green} + \rho_{SWIR1}} \right)}{\frac{2\rho_{SWIR1}}{2\rho_{SWIR1} + \rho_{NIR}} + \left(\frac{\rho_{NIR}}{\rho_{NIR} + \rho_{Red}} + \frac{\rho_{Green}}{\rho_{Green} + \rho_{SWIR1}} \right)}.$$

Тепло (LST) — температура земной поверхности, извлекаемая из теплового канала ST_B10. Яркостная температура T_B (в Кельвинах) пересчитывается в LST с предварительной оценкой излучательной способности через вегетационную долю FV [9]:

$$FV = \left(\frac{NDVI - NDVI_{\min}}{NDVI_{\max} - NDVI_{\min}} \right)^2;$$

$$\varepsilon = 0,004 \cdot FV + 0,986;$$

$$LST = \frac{T_B}{1 + \frac{0,00115 \cdot T_B \cdot \ln \varepsilon}{1,438}} - 273,15;$$

где T_B – яркостная температура (К) из канала ST_B10.

Перед объединением все четыре индикатора нормализуются в диапазон от 0 до 1 для устранения размерности. По формуле:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}};$$

$$PC1 = \omega_1 \cdot X_1 + \omega_2 \cdot X_2 + \omega_3 \cdot X_3 + \omega_4 \cdot X_4;$$

где: X_1, X_2, X_3, X_4 – нормализованные (в диапазоне $[0,1]$) значения NDVI, Wet, NDBSI, LST;

$\omega_1, \omega_2, \omega_3, \omega_4$ – элементы первого собственного вектора ковариационной матрицы этих четырех переменных, соответствующего наибольшему собственному значению.

Веса ω_i не назначаются исследователем, а вычисляются алгоритмом PCA, который ищет такое направление в четырехмерном пространстве признаков, вдоль которого дисперсия данных максимальна.

По всем пикселям (исключая маскированные) строится ковариационная матрица C размером 4×4 для переменных X_1, X_2, X_3, X_4 .

Решается уравнение на собственные значения:

$$Cv = \lambda v;$$

где λ – собственное значение, v – собственный вектор.

Выбирается собственный вектор $v^{(1)} = (\omega_1, \omega_2, \omega_3, \omega_4)^T$, отвечающий максимальному λ_{max} . Он и задает веса в линейной комбинации PC1.

Сумма квадратов весов обычно нормируется на единицу: $\omega_1^2 + \omega_2^2 + \omega_3^2 + \omega_4^2 = 1$.

Итоговый индекс дополнительно нормируется [9]:

$$RSEI = \frac{PC1 - PC1_{min}}{PC1 - PC1_{min}}.$$

Значения RSEI, близкие к 1, отвечают наилучшему экологическому состоянию, близкие к 0 – наихудшему. Для пространственного анализа полученный слой классифицируется на категории. Расчет выполняется попиксельно в среде

ГИС; водные объекты, искажающие статистику РСА, исключаются по маске $NDWI > 0$.

Результаты

На основе анализа литературных источников и характеристик существующих систем ДЗЗ разработана технологическая схема экологического картографирования, включающая пять основных этапов. Схема реализует сквозной технологический процесс – от планирования съемки до генерации тематических карт и аналитических отчетов в ГИС.

На первом этапе необходимо четко определить, какие именно экологические показатели будут оцениваться. В рамках исследования рассматривались три основных типа нарушений: загрязнение почвенного покрова, угнетение лесной растительности и техногенная трансформация земель (карьеры, отвалы, нарушенный рельеф). Исходя из задач подбирается съемочная система [10]. Для общей инвентаризации и крупномасштабного обзора достаточно мультиспектральных данных. Если же требуется идентифицировать конкретное вещество (например, нефтяную пленку или тип тяжелого металла), необходима гиперспектральная съемка. Радиолокационные данные (РСА) применяются в тех случаях, когда важна всепогодность или нужно зафиксировать изменения микрорельефа и шероховатости поверхности, которые не видны в оптике.

На втором этапе выполняется заказ и приемка данных с российских космических аппаратов: «Канопус-В», «Ресурс-П», «Кондор-ФКА». Полученные сырые снимки проходят стандартную предварительную обработку: радиометрическая калибровка (учет шумов сенсора), атмосферная коррекция (устранение дымки и рассеянной радиации) и ортотрансформирование – приведение к единой картографической проекции с устранением искажений рельефа [11].

На третьем этапе для количественной оценки состояния растительного покрова рассчитываются стандартные вегетационные индексы: NDVI, SAVI, LAI. По радиолокационным данным вычисляются текстурные признаки (например, матрица совместной встречаемости GLCM), которые хорошо выделяют антропогенно нарушенные участки. Для гиперспектральных снимков применяется метод спектрального угла (SAM), позволяющий сравнить пиксель с эталонной сигнатурой загрязнителя [12].

Четвертым этапом на основе полученных признаков выполняется контролируемая классификация. Используются метод случайного леса, машины опорных векторов (SVM) и сверточные нейронные сети [13]. Однако полностью автоматизировать процесс не всегда возможно: некоторые объекты (например, стихийные свалки или старые техногенные формы рельефа) уверенно распознаются только при визуальном дешифрировании опытным специалистом. Поэтому конечное решение принимается по результатам совместного анализа автоматического и ручного методов [14].

На заключительном этапе формируются несколько типов картографических материалов. Прежде всего, это карта категорий экологического состояния территории («норма», «зона риска», «зона кризиса»). Далее – отдельные карты нару-

шенных земель и карты загрязнения водных объектов (по гиперспектральным данным). Все слои экспортируются в стандартные векторные форматы и загружаются в ГИС для дальнейшего анализа и подготовки отчетов [15].

Описанную схему можно применить для получения набор конкретных картографических материалов.

Первая карта NDVI. На ней хорошо видны участки, где растительность угнетена: там значения индекса опускаются ниже заданного порога. Такие зоны обычно привязаны к техногенным объектам или нарушенным землям.

Вторая карта посвящена загрязнению почв нефтепродуктами. Ее строили по гиперспектральным данным: спектр каждого пикселя сравнивали с библиотекой эталонных сигнатур загрязнителей. Там, где совпадение максимальное, фиксируется нефтяное загрязнение.

Третья карта нарушенные земли. Здесь использовали радиолокационные снимки. Нарушение проявляется в резком скачке коэффициента обратного рассеяния: это означает, что изменилась шероховатость или структура поверхности. Так можно обнаружить карьеры, отвалы, техногенные выемки.

Четвертая карта – интегральная. Ее рассчитали по формуле RSEI, объединив все перечисленные признаки. Получился единый показатель экологического риска для каждого участка территории.

Заключение

В ходе выполнения научно-исследовательской работы была предложена методика экологического картографирования по данным дистанционного зондирования Земли. В ее основе лежит обоснованный выбор мультиспектральных, гиперспектральных и радиолокационных данных — включая съемку с российских космических аппаратов. Для обработки этих данных предложена сквозная технологическая схема, которая охватывает все этапы: от предварительной коррекции снимков до построения итоговых тематических карт. Кроме того, введен интегральный экологический индекс, позволяющий объединить в едином показателе оптические и радиолокационные признаки нарушений.

В ближайшей перспективе планируется создание полностью автоматизированного веб-сервиса для экологического мониторинга, который будет работать на основе сверточных нейронных сетей и облачных вычислительных платформ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бугакова Т. Ю., Шарапов А. А. Применение интеллектуальных систем для решения задач в области геопространственных технологий и дистанционного зондирования. – Текст: электронный // Научная статья СГУГиТ. – Новосибирск, 2022. – С. 163–168. – URL: <https://gclnk.com/3Gco6DMm> (дата обращения: 14.12.2025).
2. Валиев В. С., Иванов Д. В. Градиентный алгоритм семантической сегментации изображений земной поверхности и его использование для выделения границ водных объектов. – Текст: электронный // Научный журнал КубГАУ. – 2021. – № 171. – С. 1–17. – URL: <https://cyberleninka.ru/article/n/gradientnyy-algoritm-semanticheskoy-segmentatsii-izobrazheniy-zemnoy-poverhnosti-i-ego-ispolzovanie-dlya-vydeleniya-granits-vodnyh> (дата обращения: 05.04.2026).

3. Сидоров М. В. Разработка алгоритма семантической сегментации данных дистанционного зондирования Земли. – Текст: электронный // Advanced Engineering Research. – 2023. – № 4. – С. 34–41. – URL: <https://www.vestnik-donstu.ru/jour/article/view/2259> (дата обращения: 04.04.2026).
4. Космические аппараты «Канопус-В»: техническое описание. – М.: ВНИИЭМ, 2020.
5. Космический комплекс «Ресурс-П»: руководство пользователя. – Самара: РКЦ «Прогресс», 2021.
6. Radar satellite «Kondor-FKA»: data sheet. – Moscow: NPO Mashinostroyeniya, 2023.
7. Landsat 8 Data Users Handbook. – Sioux Falls: USGS, 2019.
8. Sentinel-2 User Handbook. – Paris: ESA, 2020.
9. Xu H. A remote sensing urban ecological index and its application // Acta Ecologica Sinica. – 2014. – Vol. 33, No. 24. – P. 7853–7862.
10. Тикунов В. С., Котова Т. В., Белоусов С. К. Экологическое состояние: определение, показатели, картографирование. – Текст: электронный // ИнтерКарто. ИнтерГИС. – 2021. – Т. 27, № 1. – С. 165–194. – URL: <https://doi.org/10.35595/2414-9179-2021-1-27-165-194> (дата обращения: 10.03.2026).
11. Будагов И. В., Надбережный Л. О. Введение в экологическое картографирование. – Текст: электронный // Природноресурсный потенциал, экология и устойчивое развитие регионов России. – Пенза: Пензенский ГАУ, 2024. – С. 6–9. – URL: <https://www.elibrary.ru/item.asp?id=67340615> (дата обращения: 10.03.2026).
12. Игнатъев А. В., Гилка В. В., Матыцына Д. А. Автоматическое распознавание типа застройки для системы экологического мониторинга. – Текст: электронный // Инженерный вестник Дона. – 2020. – № 1(61). – С. 11. – URL: <https://elibrary.ru/item.asp?id=42672873> (дата обращения: 10.03.2026).
13. Сладкопепцев С. А. Проблемы классификации и картографирования экологических систем. – Текст: электронный // Известия высших учебных заведений. Геодезия и аэрофотосъемка. – 2015. – № 3. – С. 47–53. – URL: <https://elibrary.ru/item.asp?id=24103679> (дата обращения: 10.03.2026).
14. Yuan Z., Liu L., Wang M., Huang C. Ecological change analysis of Zhongxiang City based on remote sensing ecological index // Resources Environment & Engineering. – 2019. – Vol. 33, No. 04. – P. 474–480.
15. Guo H., Liu L., Sun X., Song Y. Evaluating Environmental Quality and Its Driving Force in Northeastern China Using the Remote Sensing Ecological Index // Sustainability. – 2022. – Vol. 14, No. 23. – Art. 16304. – DOI: 10.3390/su142316304.

© П. Е. Самсонов, Чермошенцев А. Ю. 2026

А. И. Ступин^{1✉}, В. В. Селифанов¹

Разработка методики испытаний государственной информационной системы: подходы, этапы и практические рекомендации

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: n350z@mail.ru

Аннотация. В статье представлена разработанная авторами методика испытаний государственных информационных систем (ГИС), прошедшая апробацию в ходе внедрения трех типовых проектов. В отличие от существующих фрагментарных подходов, предложенная методика представляет собой целостный, документально оформленный комплекс, включающий 8 видов испытаний, 34 типовых тестовых сценария и систему критериев оценки результатов. Описана структура методики, определены роли участников, регламентирован порядок фиксации дефектов. Приведены количественные результаты апробации методики на пилотных проектах: сокращение числа критических дефектов, выявляемых на этапе эксплуатации, на 58 %, снижение времени приемочных испытаний на 37 %. Методика соответствует требованиям Приказа Минкомсвязи России № 486 и стандарту ISO/IEC 25010:2011.

Ключевые слова: Государственная информационная система, методика испытаний, тестирование программного обеспечения, качество ГИС, функциональное тестирование, надежность информационных систем

A. I. Stupin^{1✉}, V. V. Selifanov¹

Development of a Testing Methodology for a State Information System: Approaches, Stages and Practical Recommendations

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: n350z@mail.ru

Abstract. The article presents a methodology for testing state information systems (SIS) developed by the authors, which has been tested during the implementation of three typical projects. In contrast to existing fragmentary approaches, the proposed methodology represents an integral, documented complex that includes 8 types of tests, 34 standard test scenarios and a system of criteria for evaluating results. The structure of the methodology is described, the roles of participants are defined, and the procedure for recording defects is regulated. Quantitative results of testing the methodology on pilot projects are presented: a 58 % reduction in the number of critical defects detected at the operational stage, and a 37 % reduction in acceptance testing time. The methodology complies with the requirements of Order No. 486 of the Ministry of Communications of Russia and the ISO/IEC 25010:2011 standard.

Keywords: state information system, testing methodology, software testing, quality of SIS, functional testing, reliability of information systems

Введение

В результате выполнения государственного контракта № ГК-22-05/2024 на «Разработку и внедрение типовой методики испытаний государственных информационных систем» авторами создана и апробирована методика, предназначенная для оценки качества ГИС федерального и регионального уровней. Необходимость разработки такой методики была обусловлена статистическими данными за 2020–2025 гг., согласно которым 42% серьезных сбоев в работе федеральных ГИС связаны с недостаточным тестированием на этапе приемки [11]. Как справедливо отмечает Г. Майерс, «тестирование – это процесс, направленный на обнаружение ошибок, а не демонстрацию того, что программа работает» [1, с. 16]. Однако на практике существующие ведомственные инструкции не обеспечивали системного обнаружения ошибок, что и послужило прямым основанием для разработки унифицированной методики.

Структура разработанной методики

Разработанная методика представляет собой документ объемом 124 страницы, включающий следующие обязательные разделы:

1.1. Область применения – ГИС с микросервисной архитектурой, распределенными центрами обработки данных и количеством пользователей свыше 100 тыс. человек.

1.2. Нормативные ссылки – ФЗ № 149-ФЗ, ФЗ № 210-ФЗ, Приказ Минкомсвязи № 486, Постановление Правительства № 719, ГОСТ Р ИСО/МЭК 12119-2000, ISO/IEC 25010:2011.

1.3. Термины и определения – введены 28 специализированных терминов (включая «критический дефект», «порог надежности», «сценарий восстановления»).

1.4. Виды испытаний – методика предусматривает проведение 8 видов испытаний (табл. 1).

Таблица 1 – Виды испытаний, включенные в методику

№	Вид испытаний	Длительность	Обязательные инструменты
1	Предварительные функциональные	5–7 дней	Postman, Selenium WebDriver
2	Интеграционные (end-to-end)	10–14 дней	SOAP UI, Kafka Consumer
3	Нагрузочные и стресс-тесты	3–5 дней	Apache JMeter
4	Тесты надежности (MTBF/MTTR)	30 суток	Prometheus, Grafana
5	Тесты безопасности (СЗИ)	14 дней	ViPNet, КриптоПро, Burp Suite
6	UX-тестирование	5 дней	UserZoom, Яндекс.Метрика
7	Тесты восстановления (disaster recovery)	3 дня	Chaos Mesh
8	Приемочные испытания	7 дней	Jira, Test IT

1.5. Критерии оценки – методика содержит 134 проверяемых требования, каждому из которых присвоен уникальный идентификатор (например, RQ-FUNC-045). Критерии сгруппированы по восьми характеристикам качества согласно ISO/IEC 25010:2011 [3, с. 24]: функциональная пригодность (38 критериев), производительность (18), совместимость (12), удобство использования (14), надежность (22), защищенность (19), сопровождаемость (7), переносимость (4).

Регламент проведения испытаний по разработанной методике

В отличие от разрозненных подходов, описанных в литературе [2–4], предложенная методика включает жесткий регламент, определяющий роли и последовательность действий.

2.1. Роли участников:

- заказчик (государственный орган) – утверждает программу испытаний;
- разработчик – предоставляет тестовые стенды и устраняет дефекты;
- независимая тестовая лаборатория (аккредитованная согласно Постановлению № 719) – проводит нагрузочные тесты и тесты безопасности;
- эксплуатант – участвует в опытной эксплуатации.

2.2. Жизненный цикл дефекта (defect lifecycle), реализованный в методике, включает 6 стадий: обнаружение → регистрация в Jira → назначение ответственного → исправление → регрессионное тестирование → закрытие [13]. Для каждого дефекта обязательна классификация по критичности: блокирующий (Blocker), критический (Critical), значительный (Major), незначительный (Minor). Статистика по 20 проектам внедрения региональных ГИС за 2020–2024 гг., обработанная авторами, показывает, что применение итеративной модели (shift-left approach) позволило снизить стоимость исправления дефектов в 10–15 раз по сравнению с их обнаружением на финальной стадии [12].

Содержательное наполнение тестовых сценариев

Ядром разработанной методики является библиотека типовых тестовых сценариев (test cases). Всего создано 34 сценария, каждый из которых имеет четкий идентификатор, предусловие, шаги, ожидаемый результат и критерий прохождения (test oracle).

1. Сценарии для функционального тестирования (12 сценариев). Пример сценария TF-07 «Проверка обработки платежа»:

- *Предусловие:* пользователь авторизован в ЕСИА;
- *Входные данные:* сумма платежа 0,01 руб., 10 000 руб., 1 000 000 руб.;
- *Шаги:* формирование платежного поручения → отправка в ГИС ГМП → получение квитанции;
- *Ожидаемый результат:* статус «Успешно», ошибка округления отсутствует;

— *Критерий прохождения*: 100% транзакций из 1000 выполнены корректно.

2. Сценарии для интеграционного тестирования (8 сценариев). Учитывая, что ГИС взаимодействует с десятками смежных систем через протоколы HTTP/2, REST API, SOAP, в методику включены сценарии проверки таймаутов, повторных попыток (retry policies) и обработки некорректных ответов (error handling). Например, сценарий TI-03 «Разрыв соединения с ЕСИА»: эмулируется обрыв связи на 30 секунд, проверяется корректность сообщения «Сервис временно недоступен» и автоматическое восстановление после возобновления соединения.

3. Сценарии нагрузочных испытаний (6 сценариев). На основе анализа пиковых нагрузок Единого портала государственных услуг (1,2 млн обращений в час в 2024 году [14]) в методику заложены следующие требования, проверяемые в JMeter:

— Система должна выдерживать 15 000 одновременных сессий (concurrent users);

— Время ответа для 95 % запросов – не более 3 секунд;

— Пропускная способность – не менее 500 запросов в секунду.

4. Сценарии оценки надежности (5 сценариев). Методика включает количественные показатели:

— Среднее время наработки на отказ (MTBF) для критических компонентов – не менее 720 часов;

— Среднее время восстановления (MTTR) – не более 2 часов.

Обоснованием этих цифр послужил анализ инцидента 2023 года, когда сбой в работе ЕСИА продолжительностью 4 часа 20 минут затронул 15 млн пользователей [15].

Результаты апробации разработанной методики

Разработанная методика прошла апробацию на трех пилотных проектах: (1) региональная ГИС в сфере здравоохранения (Ростовская область, 2024 г.), (2) муниципальная ГИС ЖКХ (Республика Татарстан, 2024–2025 гг.), (3) ведомственная ГИС транспорта (Московская область, 2025 г.). Общий объем проверенных требований – 402, количество выполненных тест-кейсов – 1 287.

В ходе опытной эксплуатации на ГИС ЖКХ (интегрирует данные более 22 тысяч управляющих компаний) по предложенной методике было выявлено и устранено 47 критических дефектов, из них 28 (60 %) относились к интеграционному взаимодействию – то есть дефектов, которые при старом подходе были бы обнаружены только на этапе промышленной эксплуатации. Основные результаты апробации приведены в табл. 2.

Таблица 2 – Результаты апробации разработанной методики

Показатель	До внедрения методики (средний по 5 проектам 2020–2023)	После внедрения методики (пилотные проекты 2024–2025)	Изменение
Критических дефектов, выявленных на этапе эксплуатации	12,4	5,2	-58 %
Длительность приемочных испытаний (дней)	22	13,9	-37 %
Полнота покрытия требований (requirements coverage)	61 %	94 %	+33 %
Среднее время восстановления после сбоя (MTTR), часов	4,1	1,7	-59 %

Обсуждение

Апробация методики на трех пилотных проектах подтвердила ее эффективность: сокращение критических дефектов в эксплуатации на 58 %, снижение времени приемочных испытаний на 37 %, повышение полноты покрытия требований до 94 %.

Перспективы дальнейшего развития разработанной методики связаны с внедрением AI-driven подхода для автоматической генерации тестовых сценариев на основе анализа логов эксплуатации, а также с адаптацией методологии CI/CD для ГИС с учетом повышенных требований к безопасности. Кроме того, планируется создание методики оценки экономической эффективности испытаний, позволяющей количественно оценить соотношение затрат на тестирование и предотвращенных потерь от сбоев.

Заключение

В результате разработана и апробирована методика испытаний государственной информационной системы, включающая:

- 8 видов испытаний с закрепленными инструментами автоматизации;
- 34 типовых тестовых сценария с четкими критериями прохождения;
- Регламент жизненного цикла дефекта с классификацией по критичности;
- Количественные критерии надежности ($MTBF \geq 720$ ч, $MTTR \leq 2$ ч).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Майерс, Г. Искусство тестирования программ / Г. Майерс. – М.: Финансы и статистика, 1982. – 176 с. (Оригинал: Myers, G.J. The Art of Software Testing. – New York: John Wiley & Sons, 1979.)
2. Кулямин, В.В. Методы тестирования программного обеспечения / В.В. Кулямин, А.К. Петренко. – М.: ИПИ РАН, 2018. – 248 с. ISBN 978-5-902030-45-8.
3. ISO/IEC 25010:2011. Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models. – Geneva: ISO, 2011. – 34 p.
4. Канер, С. Тестирование программного обеспечения. Фундаментальные концепции менеджмента бизнес-приложений / С. Канер, Дж. Фолкер, Е.В. Бутенко. – Киев: ДиаСофт, 2001. – 544 с. ISBN 966-7393-52-1.
5. ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. – М.: Госстандарт России, 2000. – 28 с.
6. Приказ Минкомсвязи России № 486 от 27 декабря 2017 г. «Об утверждении требований к тестированию государственных информационных систем» (зарегистрирован в Минюсте России 22 января 2018 г., № 49741).
7. Постановление Правительства РФ № 719 от 14 июля 2021 г. «Об утверждении Положения о проведении испытаний государственных информационных систем» // Собрание законодательства РФ. – 2021. – № 29. – Ст. 5612.
8. Бутенко, Е.В. Обеспечение качества и тестирование программного обеспечения: учебное пособие / Е.В. Бутенко. – М.: НИУ ВШЭ, 2022. – 312 с. ISBN 978-5-7598-2674-5.
9. Отчет Министерства цифрового развития, связи и массовых коммуникаций РФ о результатах мониторинга функционирования государственных информационных систем за 2024 год [Электронный ресурс]. – М.: Минцифры России, 2025. – URL: <https://digital.gov.ru/> (дата обращения: 20.03.2026).
10. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы: утв. Указом Президента РФ № 203 от 9 мая 2017 г. // Собрание законодательства РФ. – 2017. – № 20. – Ст. 2901.
11. Счетная палата Российской Федерации. Анализ причин сбоев в работе государственных информационных систем за 2020–2024 гг. : отчет / Счетная палата РФ. — Москва, 2025. – 67 с.
12. Boehm, B. W. Software Engineering Economics / B. W. Boehm. – Englewood Cliffs : Prentice-Hall, 1981. – 768 p. – ISBN 0-13-822122-7.
13. ISTQB. Foundation Level Syllabus (Version 4.0) / International Software Testing Qualifications Board. – 2023. – 120 p. – URL: <https://www.istqb.org> (дата обращения: 20.03.2026).
14. Минцифры России. Анализ пиковых нагрузок Единого портала государственных услуг за 2024 год : технический отчет / Министерство цифрового развития, связи и массовых коммуникаций РФ. – Москва, 2025. – 45 с.
15. Отчет об инциденте ЕСИА от 15 ноября 2023 года : служебная записка / Минцифры России. – Москва, 2023. – 12 с.

© А. И. Ступин, В. В. Селифанов, 2026

В. П. Цыплаков¹✉, Д. М. Никулин¹

Обзор методов контроля разрешающей способности ЭОП

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: vladonehko@gmail.com

Аннотация. В работе рассматриваются методы контроля разрешающей способности электронно-оптических преобразователей, используемых в системах ночного видения и различных оптико-электронных устройствах. Выполнен анализ существующих подходов к измерению данного параметра, включая визуальные методы, основанные на использовании тест-объектов, и фотоэлектрические методы с цифровой регистрацией изображения. Отдельное внимание уделено методам, связанным с использованием частотно-контрастной характеристики для оценки качества изображения. Отмечены основные недостатки традиционных способов контроля, среди которых субъективность визуальной оценки и сложность практической реализации отдельных методик. Сделан вывод о целесообразности разработки автоматизированного метода контроля разрешающей способности с применением цифровой обработки изображений. Такой подход позволяет повысить точность измерений и обеспечить повторяемость получаемых результатов. Также использование автоматизированных систем позволяет сократить время проведения измерений и уменьшить влияние человеческого фактора на результаты контроля. Полученные результаты могут быть использованы при разработке современных измерительных стендов для исследования параметров электронно-оптических преобразователей.

Ключевые слова: электронно-оптические преобразователи, разрешающая способность, автоматизированный контроль

V. P. Tsyplakov¹✉, D. M. Nikulin¹

Review of Methods for Controlling the Resolution of Image Intensifier Tubes

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: vladonehko@gmail.com

Abstract. The paper discusses methods for controlling the resolution of image intensifier tubes used in night vision systems and various optoelectronic devices. An analysis of existing approaches to measuring this parameter is carried out, including visual methods based on the use of test targets and photoelectric methods with digital image acquisition. Particular attention is paid to methods related to the use of the modulation transfer function for image quality assessment. The main disadvantages of traditional control methods are noted, including the subjectivity of visual evaluation and the complexity of practical implementation of certain techniques. A conclusion is made about the feasibility of developing an automated method for resolution control using digital image processing. Such an approach makes it possible to improve measurement accuracy and ensure repeatability of the obtained results. In addition, the use of automated systems makes it possible to reduce measurement time and minimize the influence of the human factor on control results. The obtained results can be used in the development of modern measuring benches for studying the parameters of image intensifier tubes.

Keywords: image intensifier tubes, resolution, automated control

Введение

Наиболее распространенным является визуальный метод с использованием тест-объектов (мир), при котором оператор наблюдает изображение и определяет максимальную различимую группу линий [1, 5]. Данный метод отличается простотой, однако обладает высокой субъективностью, зависящей от индивидуальных особенностей наблюдателя.

Более современным является фотоэлектрический метод, основанный на регистрации изображения с помощью цифровых сенсоров [5, 6]. В этом случае изображение тест-объекта фиксируется камерой и подвергается последующей обработке. Это позволяет повысить объективность измерений и обеспечить возможность хранения и анализа данных.

В процессе обработки изображения анализируется контраст между светлыми и темными элементами, степень размытости границ и уровень шумов [8]. Разрешающая способность определяется по предельной пространственной частоте, при которой сохраняется различимость элементов.

Описание состояния вопроса

Электронно-оптические преобразователи (ЭОП) являются ключевыми элементами современных оптико-электронных систем, находящих широкое применение в приборах ночного видения и наблюдения, медицинской диагностической аппаратуре (эндоскопы, системы флуоресцентной визуализации), научных исследованиях для регистрации быстропротекающих процессов, а также в системах безопасности и навигации [1, 6, 7].

В настоящее время разработан и активно используется целый спектр различных типов ЭОП, различающихся по поколениям (I, II, II+, III), конструкции (канальные, плоские), спектральной чувствительности (от ближнего УФ до ближнего ИК диапазона) и специализированному назначению. Это и высокочувствительные ЭОП для астрономических наблюдений, и миниатюрные преобразователи для медицинских зондов, и скоростные ЭОП-регистраторы для научных экспериментов. Подобное многообразие выдвигает высокие и разнообразные требования к их характеристикам, что, в свою очередь, формирует сложную задачу объективного и точного контроля качества.

Анализ нормативной, научной и патентной литературы показывает, что базовые параметры, определяющие эксплуатационное качество ЭОП, хорошо известны и стандартизированы. [4] К ним, в первую очередь, относятся: предельное разрешение, частотно-контрастная характеристика (ЧКХ), коэффициент усиления яркости, равномерность свечения экрана и уровень шумов. Контроль этих параметров является обязательным на этапах разработки, приемо-сдаточных и эксплуатационных испытаний. Существуют нормативные документы, регламентирующие отдельные процедуры испытаний, такие как, например, контроль испытательным напряжением, описанный в ГОСТ 21815.5-86 [2].

Таким образом, состояние вопроса характеризуется наличием устойчивой научно-технической проблемы: существует объективная потребность в высоко-точной и воспроизводимой оценке параметров ЭОП, которую не могут удовлетворить устаревшие визуальные методики. Это определяет актуальность разработки инженерной методики и макета автоматизированного измерительного стенда, призванного устранить субъективность, повысить скорость и точность контроля.

Контроль разрешающей способности электронно-оптических преобразователей

Разрешающая способность электронно-оптического преобразователя (ЭОП) является одной из ключевых характеристик, определяющих качество формируемого изображения. Она характеризует способность системы различать мелкие детали объекта и обычно выражается в виде максимального числа различимых пар линий на единицу длины (линий/мм).

Контроль разрешающей способности необходим:

- при разработке ЭОП;
- при приемо-сдаточных испытаниях;
- в процессе эксплуатации.

В соответствии с нормативными документами (например, ГОСТ Р 55842–2013), измерение данного параметра может выполняться различными методами, основанными на анализе тестовых изображений.

Наиболее распространенным методом является визуальный контроль разрешающей способности с использованием тест-объектов – стандартных мир

На вход ЭОП подается изображение тест-объекта, содержащего группы чередующихся черных и белых линий с различной пространственной частотой.

Оператор наблюдает выходное изображение и определяет максимальную группу линий, которая еще различима.

Современный подход заключается в замене визуального наблюдения на регистрацию изображения с помощью цифровых сенсоров. Фотоэлектрический метод контроля разрешающей способности электронно-оптического преобразователя основан на регистрации выходного изображения с помощью цифрового фотоприемного устройства, такого как ПЗС- или КМОП-камера, с последующей компьютерной обработкой полученных данных. В отличие от традиционного визуального подхода, при котором оценка проводится оператором, в данном случае изображение тест-объекта сначала формируется на входе ЭОП, проходит через преобразователь, а затем фиксируется камерой в виде цифрового массива яркостей. Это позволяет перейти от субъективной оценки к количественному анализу, обеспечивая более высокую точность и воспроизводимость результатов измерений.

В процессе обработки зарегистрированного изображения анализируется ряд параметров, характеризующих качество воспроизведения тестового объекта. В первую очередь оценивается контраст между чередующимися светлыми и темными линиями, так как именно снижение контраста при увеличении простран-

ственной частоты указывает на предел разрешающей способности системы. Также учитывается степень размытости границ между элементами изображения, наличие и уровень шумов, а также возможные искажения, вносимые как самим ЭОП, так и регистрирующей камерой. На основе распределения яркости вдоль выбранных профилей изображения определяется, при какой пространственной частоте линии становятся неразличимыми или их контраст падает ниже заданного порогового значения. Такой подход позволяет не только точно определить разрешающую способность, но и создать основу для дальнейшего анализа характеристик системы, включая построение частотно-контрастной характеристики и оценку равномерности изображения по полю.

Данный метод основан на количественной оценке контраста между черными и белыми линиями тест-объекта.

Разрешение определяется как максимальная пространственная частота, при которой контраст остается выше заданного порога (например, от 10 % до 20 %).

Контраст рассчитывается по формуле 1.

$$C = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}}; \quad (1)$$

где $I_{\max}$ – интенсивность светлых участков;

$I_{\min}$ – интенсивность темных участков;

C – контраст.

Типовые измерительные стенды для контроля разрешающей способности ЭОП

Контроль разрешающей способности электронно-оптических преобразователей осуществляется с использованием специализированных измерительных стендов, обеспечивающих формирование тестового изображения, его преобразование и последующий анализ [9]. В зависимости от уровня автоматизации и применяемых средств регистрации различают классические (визуальные), полуавтоматические и автоматизированные измерительные стенды. Пример стенда показан на рис. 1.



Рис. 1. Стенд для контроля параметров ЭОП

Классический измерительный стенд предназначен для визуального контроля разрешающей способности и широко применяется благодаря своей простоте и соответствию нормативным методикам [9].

В состав такого стенда, как правило, входят: источник света, обеспечивающий равномерную подсветку тест-объекта; тест-объект (мира), содержащий группы линий различной пространственной частоты; коллиматор или объектив, формирующий изображение тест-объекта на входе ЭОП; сам электронно-оптический преобразователь; а также наблюдательная система (окуляр или микроскоп), через которую оператор оценивает качество изображения.

Принцип работы стенда заключается в проецировании изображения мира на вход ЭОП с последующим визуальным наблюдением выходного изображения. Оператор определяет максимальную группу линий, которые еще различимы, и по соответствующей шкале устанавливает значение разрешающей способности.

Несмотря на простоту и широкое распространение, данный тип стендов обладает рядом существенных недостатков. Основным из них является субъективность результатов, обусловленная зависимостью от индивидуальных особенностей зрения оператора, его опыта и условий наблюдения.

Полуавтоматические стенды с фотофиксацией

Полуавтоматические измерительные стенды представляют собой что-то среднее между визуальным и автоматизированными системами.

В состав таких стендов, помимо элементов классической схемы, включается цифровая камера, устанавливаемая на выходе ЭОП или в окулярной части. Камера фиксирует изображение тест-объекта, которое затем может быть сохранено, увеличено и проанализировано с использованием программного обеспечения.

Работа стенда заключается в том, что оператор, наблюдая изображение на экране компьютера, определяет границу различимости линий, однако при этом имеет возможность использовать дополнительные инструменты: масштабирование, изменение контраста, построение профилей яркости. Это позволяет повысить точность измерений по сравнению с чисто визуальным методом.

К преимуществам данного типа стендов относятся возможность документирования результатов, снижение влияния субъективного фактора и повышение удобства анализа. Однако окончательное решение все еще принимается оператором, что не исключает субъективности полностью.

Автоматизированные измерительные стенды

Автоматизированные измерительные стенды представляют собой современный и перспективный вариант систем контроля размещающей способности ЭОП. В отличие от классических и полуавтоматических решений, они позволяют проводить полный цикл измерений практически без участия оператора в анализе результатов.

Типовой автоматизированный стенд включает стабилизированный источник света, стандартный тест-объект с известными параметрами, оптическую си-

стему формирования изображения, сам электронно-оптический преобразователь, цифровую камеру высокого разрешения и вычислительный блок с специализированным программным обеспечением.

Принцип работы такого стенда заключается в автоматическом захвате изображения тест-объекта после его прохождения через ЭОП.

Далее программное обеспечение анализирует распределение яркости вдоль профилей линий, вычисляет контраст между элементами, определяет границу различимости и автоматически рассматривает значение разрешающей способности. Дополнительно система может строить графики, сохранять результаты в базе данных, проводить статистическую обработку и формировать отчеты.

Основными преимуществами автоматизированных стендов являются высокая объективность, точность и воспроизводимость результатов, а также возможность полной автоматизации процесса. Именно поэтому такие системы сегодня наиболее востребованы.

Частотно-контрастная характеристика

Более точной характеристикой качества изображения является частотно-контрастная характеристика (ЧКХ), которая описывает зависимость контраста изображения от пространственной частоты.

Разрешающая способность может быть определена как граничная пространственная частота, при которой контраст изображения падает до заданного уровня. Таким образом, она является частным случаем анализа ЧКХ.

Методы определения ЧКХ могут основываться на анализе тестовых изображений, а также на использовании функций отклика системы, таких как функция рассеяния края и линия рассеяния. Однако данные методы требуют сложной математической обработки и не всегда удобны для практической реализации.

Постановка задачи

Анализ существующих методов показывает, что визуальные подходы обладают высокой субъективностью, а методы на основе полной ЧКХ – сложностью реализации и трудоемкостью. В связи с этим актуальной является разработка метода контроля разрешающей способности ЭОП, который обеспечивает:

- объективность измерений;
- возможность полной автоматизации;
- достаточную точность;
- простоту и надежность реализации в лабораторных и производственных условиях.

Предлагаемый подход

В качестве перспективного решения предлагается использование автоматизированного фотоэлектрического метода на основе цифровой обработки изображений.

Суть подхода заключается в следующем:

- формирование изображения стандартного тест-объекта (миры) на входе

ЭОП;

- регистрация выходного изображения с помощью цифровой камеры;
- автоматический анализ распределения яркости вдоль профилей линий;
- расчет контраста по формуле (1) для каждой пространственной частоты;
- определение предельной частоты, при которой контраст падает ниже заданного порога.

Данный метод исключает влияние оператора, повышает точность и воспроизводимость результатов, позволяет документировать данные и интегрировать их в единую систему контроля параметров ЭОП. Он может быть реализован в составе автоматизированного измерительного стенда и использован как на этапе разработки, так и при приемосдаточных испытаниях.

Заключение

В работе проведен анализ методов контроля разрешающей способности электронно-оптических преобразователей. Показано, что существующие методы либо обладают высокой субъективностью, либо требуют сложной реализации.

Обоснована целесообразность использования автоматизированных методов, основанных на цифровой обработке изображений. Предложенный подход позволяет повысить точность и объективность измерений и может быть использован при разработке современных измерительных стендов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Буткевич, В. Г. Электронно-оптические приборы и преобразователи / В. Г. Буткевич, В. П. Калашников. – М. : Радио и связь, 1988. – 320 с. – Текст : непосредственный.
2. ГОСТ 21815.5–86. Приборы электронно-оптические. Методы испытаний. – М. : Издательство стандартов, 1987. – 32 с. – Текст : непосредственный.
3. ГОСТ Р 55842–2013. Приборы электронно-оптические. Методы измерений параметров. – М. : Стандартинформ, 2014. – 24 с. – Текст : непосредственный.
4. ГОСТ Р 55843–2013. Приборы электронно-оптические. Методы измерения частотно-контрастных характеристик. – М. : Стандартинформ, 2014. – 18 с. – Текст : непосредственный.
5. Гуревич А. С. Оптико-электронные приборы и системы. – М. : Физматлит, 2010. – 384 с. – Текст : непосредственный.
6. Иванов В. А., Соколов А. Н. Приборы ночного видения на основе электронно-оптических преобразователей. – М. : Машиностроение, 2006. – 256 с. – Текст : непосредственный.
7. Костюков В. П. Оптико-электронные приборы наблюдения и прицеливания. – СПб. : Политехника, 2012. – 288 с. – Текст : непосредственный.
8. Лебедев В. М., Смирнов Ю. И. Методы контроля параметров электронно-оптических преобразователей // Оптический журнал. – 2015. – Т. 82, № 6. – С. 45–52. – Текст : непосредственный.
9. Мальцев А. Н. Измерительные стенды в оптико-электронном приборостроении. – Новосибирск : СГГА, 2011. – 180 с. – Текст : непосредственный.

© В. П. Цыплаков, Д. М. Никулин, 2026

М. В. Чикирисов¹✉, Т. Н. Хацевич¹

Оценка хроматизма положения одиночной линзы и двухлинзового дублета в спектральном диапазоне 0,4–1,1 мкм

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: misha.chikirisov@mail.ru

Аннотация. Актуальность оценивания хроматизма положения для одиночной линзы и двухлинзового дублета определяется необходимостью оптимального синтеза исходных систем при оптическом проектировании объективов с расширенным рабочим спектральным диапазоном для телевизионных камер, работающих в режимах «день / ночь». Целью статьи является определение соотношения между значениями хроматизма положения изображения в оптических системах в спектральном диапазоне $F' - C'$ и в расширенном спектральном диапазоне 0,4 – 1,1 мкм. Исследование проводилось методами теории хроматизма и компьютерного проектирования оптических систем. Установлено, что отношение хроматизма положения в рассматриваемых диапазонах для одиночной линзы составляет от 2,8 до 3,1 (в среднем 2,9) в зависимости от марки материала линзы, для ахроматического дублета – колеблется от 7 до 11, при этом среднее значение составляет 9.

Ключевые слова: хроматизм положения, спектральный диапазон, средняя дисперсия, частная дисперсия

M. V. Chikirisov¹✉, T. N. Khatsevich¹

Estimation of the Chromaticity of the Position of a Single lens and a Double-Lens Doublet in the Spectral Range of 0,4–1,1 Microns

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: misha.chikirisov@mail.ru

Abstract. The relevance of assessing the chromaticity of the position for a single lens and a double-lens doublet is determined by the need for optimal synthesis of the initial systems in the optical design of lenses with an extended operating spectral range for television cameras operating in day/night modes. The purpose of the article is to determine the relationship between the chromaticity values of the image position in optical systems in the spectral range $F' - C'$ and in the extended spectral range of 0,4 – 1,1 microns. The research was carried out using the methods of chromatic theory and computer-aided design of optical systems. It was found that the ratio of position chromaticity in the examined ranges for a single lens range from 2,8 to 3,1 (on average 2.9), depending on the brand of lens material, for an achromatic doublet it ranges from 7 to 11, with the average value being 9.

Keywords: Chromaticity of position, spectral range, average variance, partial variance

Введение

Основным инженерным методом проектирования оптических систем современных оптико-электронных приборов является компьютерное проектирование с использованием программ по расчету оптических систем [1]. Важнейшим эта-

пом в процессе расчета оптических систем является этап создания исходной (стартовой) системы, которая на втором этапе подвергается оптимизации, то есть изменению конструктивных параметров таким образом, чтобы максимально приблизиться к требованиям, формулируемым разработчиком в целевых показателях оптимизационной функции. Эффективному оптимизации и оптического проектирования в целом во многом определяется возможностями, заложенными в исходной системе. На этапе выбора или синтеза исходной системы прежде всего учитывается возможность коррекции в изображении хроматических аберраций первого порядка. Теория хроматизма [2] дает математический аппарат для вычисления хроматизма положения и хроматизма увеличения изображения как одиночных оптических компонентов, так и систем, состоящих из нескольких компонентов. К условию ахроматизации часто добавляются дополнительные условия, например для устранения термооптической аберрации положения [3, 4], для работы в двух спектральных диапазонах [5] и др.

В оптико-электронных приборах спектральный диапазон работы объектива определяется спектральной характеристикой приемника излучений, с которым он сопрягается, с учетом светофильтров, используемых в приборе. Спектральный диапазон работы современных матричных приемников излучений, используемых в телевизионных оптико-электронных приборах, составляет от 0,4 до 1,1 мкм [6], то есть он превышает спектральный диапазон чувствительности человеческого глаза. Поэтому в телевизионных камерах перед приемником могут устанавливаться светофильтры или наносится соответствующие покрытия на оптические поверхности объектива, отсекающие инфракрасное излучение, соответствующее участку инфракрасной чувствительности приемника излучений. В визуальных наблюдательных оптических системах, в которых изображение рассматривается глазом наблюдателя, в качестве рабочего спектрального диапазона при расчете оптической системы объектива, используется диапазон от 0,48 до 0,64 мкм (между линиями $F' - C'$). Для того, чтобы в телевизионных камерах полностью использовать излучение, соответствующее спектральному диапазону чувствительности современных матричных приемников излучений, необходимо, чтобы объектив камеры обеспечивал качественное формирование изображения в расширенном спектральном диапазоне от 0,4 до 1,1 мкм. С учетом вышесказанного представляет интерес ответ на вопрос, каково соотношение между значениями хроматизма положения изображения в оптических системах в спектральном диапазоне $F' - C'$ и в расширенном спектральном диапазоне 0,4 – 1,1 мкм. Целью статьи и является поиск ответа на поставленный вопрос. Значимость (актуальность) такого знания определяется необходимостью оптимального синтеза исходных систем при оптическом проектировании объективов с расширенным рабочим спектральным диапазоном для телевизионных камер, работающих в режимах «день / ночь».

Методы и материалы

В теории хроматизма методы оценки хроматической аберрации положения изображения (хроматизма положения) базируются на дифференцировании инварианта Аббе для преломляющей поверхности по длине волны, определении зависимости отрезка s' от дисперсионных свойств материала и обобщении результатов на произвольное количество преломляющих поверхностей или компонентов в оптической системе [2, 7]. Провести сравнение хроматизма положения изображения в видимом спектральном диапазоне $F' - C'$ и в расширенном спектральном диапазоне 0,4 – 1,1 мкм наиболее просто можно для одиночной линзы, стоящей изображение предмета, находящегося в бесконечности. Теория хроматизма дает простую формулу для расчета:

$$\Delta S'_{\lambda_1 \lambda_2} = -\frac{f'}{v_{\lambda_0}}, \quad (1)$$

где $\Delta S'_{\lambda_1 \lambda_2}$ – хроматизм положения между изображениями бесконечно далекого предмета, построенными одиночной тонкой линзой, с помощью наименьшей λ_1 и наибольшей λ_2 длин волн рабочего спектрального диапазона; f' – фокусное расстояние линзы для основной длины волны λ_0 рабочего спектрального диапазона;

$v_{\lambda_0} = \frac{n_{\lambda_0} - 1}{n_{\lambda_1} - n_{\lambda_2}}$ – коэффициент средней дисперсии материала линзы, при этом индекс при показателе преломления n соответствует указанным длинам волн.

В качестве основной длины волны в диапазоне $F' - C'$ использована линия e , в диапазоне 0,4–1,1 мкм – длина волны 0,75 мкм.

Используя каталог отечественных оптических стекол, содержащийся в широко используемой программе по компьютерному расчету оптических систем (zemax), были составлены диаграммы по принципу диаграммы Аббе для каждого из исследуемых спектральных диапазонов (рис.1), то есть определены положения морок стекол в системе координат «показатель преломления – коэффициент средней дисперсии». Сравнение диаграмм, приведенных на рис. 1 а и 1 б, показывает, что диапазоны изменения коэффициентов средней дисперсии исследуемых марок стекол существенно отличаются: для расширенного спектрального диапазона 0,4–1,1 мкм он примерно в три раза меньше, чем для видимого. В соответствии с формулой (1) хроматизм положения изображения, построенного одиночной линзой, обратно пропорционален коэффициенту средней дисперсии и будет увеличиваться при расширении рабочего спектрального диапазона.

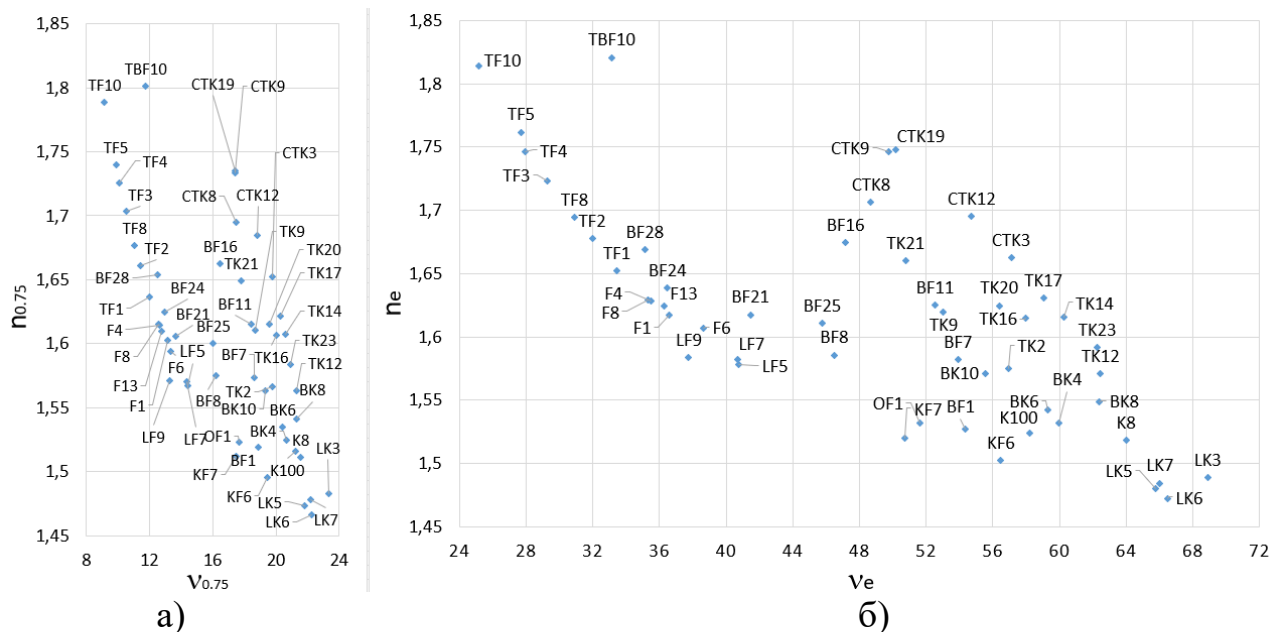


Рис. 1. Диаграммы «показатель преломления – коэффициент средней дисперсии» отечественных марок стекол для спектральных диапазонов: а) 0,4–1,1 мкм; б) $F' - C'$

В рамках учебной научно-исследовательской работы магистрантом были проведены расчеты хроматизма положения для одиночной линзы для 12 марок стекол, соответствующих различным группам оптических стекол, результаты которых приведены на рис. 2. Расчеты проводились как по формуле (1), так и путем прямой трассировки лучей соответствующего спектрального диапазона через линзу с фокусным расстоянием 100 мм. При этом отличие в результатах не превышало 3 %. На рис. 2 для каждой из марок материалов приведены значения хроматизма положения, выраженные в миллиметрах для каждого из диапазонов.

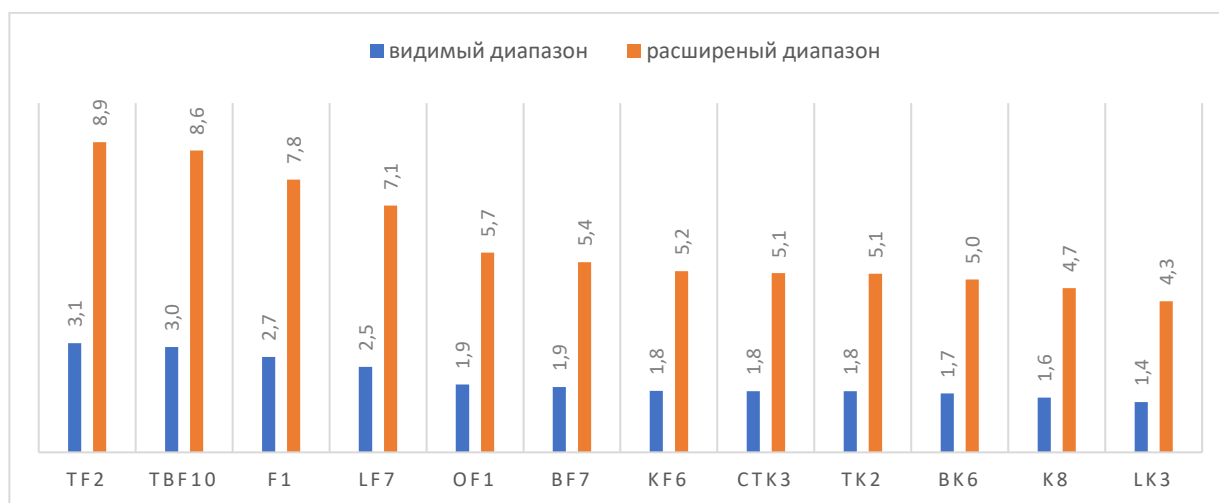
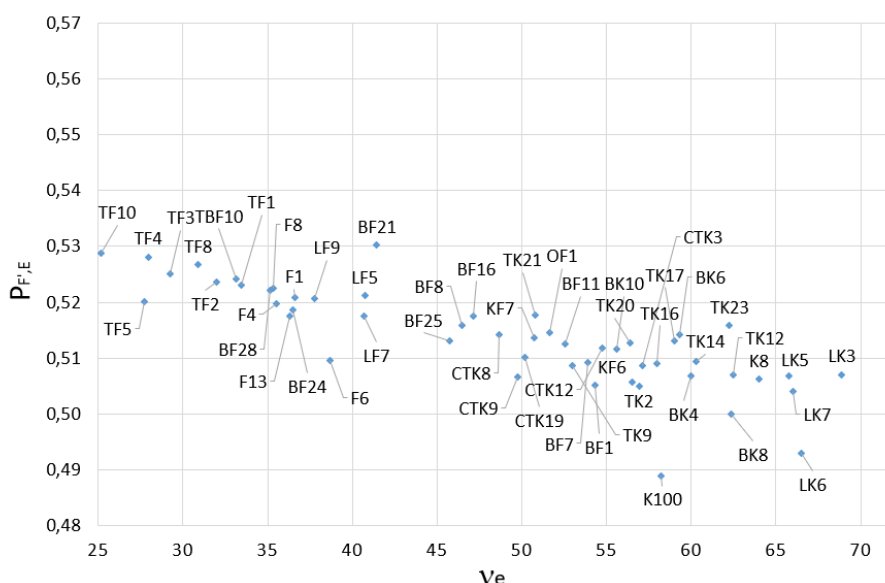


Рис. 2. Хроматизм положения одиночной линзы для двух диапазонов по результатам расчета хода лучей

Оценка хроматизма положения в оптической системе, состоящей из двух склеенных линз, проведена на примере ахроматического склеенного дублета. В теории хроматизма показано, что чем больше абсолютная разность коэффициентов средней дисперсии, тем меньше абсолютное значение оптических сил в склеенном компоненте. Последнее является благоприятным для коррекции aberrаций широких пучков лучей, прежде всего сферической aberrации. Остаточный хроматизм (вторичный спектр) $\Delta S'_{\lambda 1 \lambda 0}$ в изображении, построенном ахроматическим дублетом для бесконечно удаленного предмета, рассчитывается по формуле [7]:

где $p_1 = \frac{n_{\lambda 11} - n_{\lambda 01}}{v_{\lambda 11} - v_{\lambda 21}}$ и $p_2 = \frac{n_{\lambda 12} - n_{\lambda 02}}{v_{\lambda 12} - v_{\lambda 22}}$ – коэффициенты частной дисперсии для материала соответственно первой и второй линз склеенного дублета; v_1, v_2 – коэффициенты средней дисперсии материала соответственно первой и второй линз склеенного дублета.



223

нов: а) 0,4–1,1 мкм; б) $F' - C'$

Сравнение диаграмм, представленных на рис. 3 а и 3 б, показывает, что в спектральном диапазоне 0,4–1,1 мкм примерно в три раза возрастает различие в значениях коэффициентов частных дисперсий, что в совокупности с уменьшением диапазона коэффициентов средних дисперсий приводит к возрастанию хроматических aberrаций в двухлинзовом дублете в диапазоне 0,4–1,1 мкм по сравнению с видимым спектральным диапазоном. Результаты количественной оценки хроматизма положения в исследуемых диапазонах приводятся в следующем разделе.

Результаты и обсуждение

Оценка вторичного спектра в ахроматическом склеенном дублете проводилась по формуле (2) для 30 комбинаций марок материалов. В качестве примера в табл. 1 представлены результаты расчетов для пяти из них.

Таблица 1 – Сравнение хроматизма положения в склеенном дублете в видимом диапазоне и диапазоне 0,4–1,1 мкм

Комбинация марок	Видимый диапазон $F' - C'$			Расширенный диапазон 0,4–1,1 мкм			Отношение
	p_1 p_2	v_1 v_2	$-1/\operatorname{tg} \gamma$	p_1 p_2	v_1 v_2	$-1/\operatorname{tg} \gamma$	
ТФ2 ТК21	0,524 0,5142	31,963 50,7559	1903	0,8297 0,8059	11,4388 17,816	268	7,1
ТФ4 БК8	0,5271 0,5068	27,94 59,95	1572	0,8366 0,7856	10,07 20,67	207	7,6
ТФ8 ЛК7	0,5267 0,5041	30,903 66,022	1554	0,8304 0,7668	11,057 22,215	176	8,8
ТФ5 ЛК3	0,5275 0,5038	27,31 69,5	1778	0,8379 0,765	9,86 23,3397	185	9,6
БФ25 ТК14	0,5165 0,5086	45,787 60,199	1827	0,8097 0,7839	16,068 20,636	177	10,3

В табл.1 использовано обозначение $\operatorname{tg} \gamma = \frac{p_1 - p_2}{v_1 - v_2}$, определяющее угол наклона прямой, соединяющей две марки стекол склеенного дублета на диаграммах, приведенных на рис.3 а и 3 б в каждом из исследуемых спектральных диапазонов. В этом случае значение коэффициента $\frac{-1}{\operatorname{tg} \gamma}$ характеризует, какую часть от фокусного расстояния составляет хроматизм положения в склеенном дублете. Последний столбец в табл.1 определяет отношение хроматизма положения в диапазоне 0,4–1,1 мкм к хроматизму положения в видимом диапазоне.

Обобщая результаты по 30 комбинациям материалов, отмечается, что отношение хроматизма положения в рассматриваемых диапазонах для ахроматического дублета колеблется от 7 до 11, при этом среднее значение составляет 9.

В качестве примера на рис. 4 приведен график хроматизма положения в двухлинзовом дублете, смоделированном из марок стекол ТФ4-БК8 (вторая строка в табл. 1). Оптические силы линз в дублете рассчитывались так, чтобы в изображении был устранен хроматизм положения для длин волн 0,4 и 1,1 мкм, а фокусное расстояние равнялось 100 мм. Расчет, выполненный в компьютерной программе по расчету оптических систем, показал, что остаточный хроматизм положения в диапазоне 0,4-1,1 мкм в 7,2 раза больше, чем в видимом диапазоне. Можно принять, что относительная погрешность найденного соотношения (7–10 раз) не превышает 10 %.

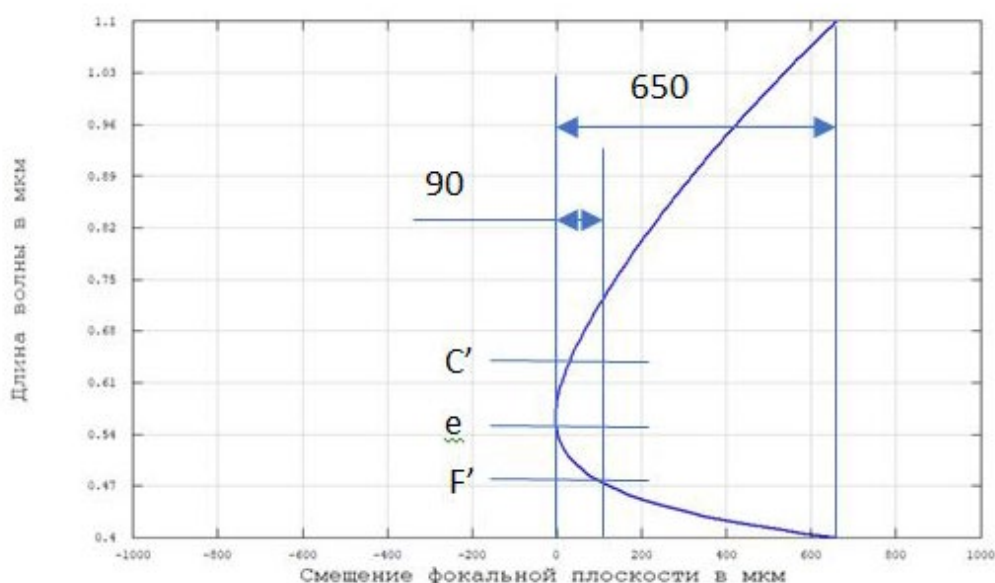


Рис.4. Хроматизм положения дублета из марок ТФ4-БК8

Для сравнения полученного результата с имеющими в литературе выбрана работа [8], посвященная особенностям вторичного спектра объективов коллиматоров, работающих в диапазоне длин волн 400—900 нм, авторы которой отмечают, что «при использовании комбинаций «обычных» стекол в спектральном диапазоне 400–900 нм происходит увеличение вторичного спектра в 7,5 раз по сравнению со спектральным диапазоном 480–643,8 нм». При расширении спектрального диапазона по сравнению с диапазоном, использованным для анализа в [8], ожидаемо должно получиться большее увеличение хроматизма положения. Найденное в данной работе среднее значение 9 может рассматриваться как коэффициент, характеризующий соотношение между хроматизмом положения в изображении ахроматического двухлинзового дублета в спектральном диапазоне 0,4-1,1 мкм и в видимом диапазоне 0,48–0,6438 мкм. В зависимости от комбинаций марок материалов значение коэффициента может составлять от 7 до 11.

Заключение

На основании вышеизложенного, можно утверждать, что соотношение между значениями хроматизма положения изображения в расширенном спектральном диапазоне 0,4 – 1,1 мкм по сравнению с таковым в спектральном диапазоне 0,48 – 0,6438 мкм составляет:

– в одиночных линзах от 2,8 до 3,1 (в среднем 2,9) в зависимости от марки материала линзы;

– в ахроматических линзовых дублетах от 7 до 11 (в среднем 9) в зависимости от использованных марок материалов.

Знание такой зависимости может быть полезным на этапе синтезе исходных оптических систем в процессе оптического проектирования объективов с расширенным рабочим спектральным диапазоном для телевизионных камер, работающих в режимах «день / ночь».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Хацевич Т. Н. Компьютерные методы проектирования оптических систем: учебник / Т. Н. Хацевич. – Новосибирск: СГУГиТ, 2022 – 156 с.
2. Чуриловский, В. Н. Теория хроматизма и аберраций третьего порядка / В. Н. Чуриловский — Ленинград: Машиностроение. Ленингр. отд-ние, 1968. — 312 с.
3. Романова Г. Э. Исследование аберрационных свойств и возможности пассивной атермализации оптических систем, работающих в области 8–12 мкм систем / Г. Э. Романова, Г. Пысь // ГЕО Сибирь, Междунар. науч. конф. «СибОптика-2015»: сб. материалов в 3 т. Т. 2. – 2015. – С. 10-17.
4. Khatsevich T., Druzhkin E. Passive athermalization of optical systems for thermal devices // Proc. SPIE 11916, 27th International Symposium on Atmospheric and Ocean Optics, Atmospheric Physics, 119160J (15 December 2021); doi: 10.1117/12.2601732.
5. Khatsevich T., Shmelev E., Development of dual-band infrared lenses // Proc. SPIE 12780, 29th International Symposium on Atmospheric and Ocean Optics: Atmospheric Physics, 127800N (17 October 2023); doi: 10.1117/12.2689347.
6. FRAME e-shop theme [Электронный ресурс] / URL: <https://kit-frame.ru/imx482-tehnicheskie-vozmozhnosti-sravnenie-harakteristik> (дата обращения 26.04.2026)
7. Зверев. В. А. Оптические материалы. Часть 1. Учебное пособие для конструкторов оптических систем и приборов. / В. А. Зверев, Е. В. Кривоустова, Т. В. Точилина. – Санкт-Петербург: СПбГУ ИТМО, 2009. – 244 с.
8. Грамматин А. П. Особенности вторичного спектра объективов коллиматоров, работающих в диапазоне длин волн 400-900 нм / А. П. Грамматин, Е. А. Цыганок // Изв. вузов. Приборостроение. – 2011. – Т.54, №9. – С. 75-77.

© М. В. Чикирисов, Т. Н. Хацевич, 2026

Р. А. Чупин¹✉, А. В. Шабурова¹

Инновационные подходы в организации производства

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: romik1221@bk.ru

Аннотация. В современных условиях быстрой цифровизации и конкуренции возрастает требование для предприятий в более эффективных методах организации процессов. В данной статье производится анализ инновационных подходов к организации производства. Как инструмент реализации рассматривается бережливое производство как наиболее универсальному и результативный. Рассмотрены основные концепции: Индустрия 4.0, гибкое производство, всеобщее продуктивное обслуживание оборудования, метод шести сигм, кайдзен и теория ограничений. В качестве предмета исследования выступает самолетостроительное предприятие. Цель работы – провести сравнительный анализ подходов и обосновать приоритет бережливого производства. Показать, что применение системы канбан, 5С и точно в срок при минимальных затратах повышает производительность, снижает брак и сокращает время циклов. Результаты подтверждают, что в условиях неопределенности и ресурсных ограничений бережливое производство остается наиболее эффективным подходом, а его сочетание с цифровыми технологиями открывает новые перспективы развития.

Ключевые слова: инновационные подходы, организация производства, бережливое производство, Индустрия 4.0, система канбан

R. A. Chupin¹✉, A. V. Shaburova¹

Innovative Approaches to Production Organization

¹Siberian State University of Geosystems and Technologies,
Novosibirsk, Russian Federation
e-mail: romik1221@bk.ru

Abstract. In modern conditions of rapid digitalization and intense competition, enterprises face an increasing need for more efficient methods of process organization. This article analyzes innovative approaches to production organization. Lean production is considered as the main tool of implementation, being the most universal and effective one. The following key concepts are examined: Industry 4.0, agile manufacturing, Total Productive Maintenance (TPM), Six Sigma, Kaizen, and Theory of Constraints. The subject of the study is an aircraft manufacturing enterprise. The aim of the work is to conduct a comparative analysis of these approaches and to substantiate the priority of lean production. The paper demonstrates that the application of the Kanban system, 5S, and Just-in-Time (JIT) principles with minimal costs increases productivity, reduces defects, and shortens production cycle times. The results confirm that under conditions of uncertainty and resource constraints, lean production remains the most effective approach, while its integration with digital technologies opens new prospects for development.

Keywords: innovative approaches, production organization, lean production, Industry 4.0, Kanban system

Введение

Современное производство сталкивается с острыми проблемами: рост конкуренции, ускоренная цифровизация, необходимость снижения затрат и повышения качества при ограниченных ресурсах. Особенно остро эти вызовы проявляются на самолетостроительных предприятиях, где высокая сложность процессов, длительные циклы и жесткие требования к качеству продукции требуют радикального повышения эффективности. Использование традиционных методов организации производства не позволяет обеспечить соответствия всем современным требованиям предприятий. К таким относятся скорость и гибкость производства, снижение потерь времени, материалов, финансов.

В результате перечисленных проблем возникает потребность в инновационных решениях и инструментах. В качестве таких решений выступают такие инструменты бережливого производства как система канбан, 5С и точно в срок.

Цель статьи – провести сравнительный анализ инновационных подходов к организации производства и обосновать приоритет бережливого производства как наиболее эффективного инструмента. Для достижения цели решены следующие задачи: рассмотреть основные инновационные концепции, раскрыть сущность и инструменты бережливого производства, проанализировать их применение на примере самолетостроительного предприятия.

Методы и методики исследования

Исследование выполнено на основе системного подхода и сравнительного анализа. Что позволяет комплексно рассмотреть инновационные подходы к организации производства и выделить среди них наиболее эффективный инструмент.

Для достижения цели применялись следующие методы:

- контент-анализ научной литературы и отраслевых отчетов за период 2018–2025 годов (всего проанализировано более 40 источников) [1, 2];
- сравнительный метод: сопоставление бережливого производства и его ключевых инструментов с другими концепциями [3];
- анализ практических кейсов внедрения инструментов бережливого производства на промышленных предприятиях, включая самолетостроительные [4, 5];
- качественный и количественный анализ эффективности по ключевым показателям: сокращение времени производственного цикла, снижение уровня брака, рост производительности труда и экономия ресурсов.

Сравнение подходов проводилось по следующим критериям: затраты на внедрение, срок окупаемости, влияние на качество продукции, гибкость производственной системы, устойчивость к внешним изменениям.

Особое внимание уделено применению конкретных инструментов бережливого производства – системы канбан, 5С и точно в срок – на примере самолетостроительного предприятия. Это позволило показать их практическую ценность

в условиях высокой сложности технологических процессов и жестких требований к качеству и безопасности [6].

Таким образом, выбранный методический аппарат обеспечивает объективность сравнения и позволяет обосновать приоритет бережливого производства как основного инновационного инструмента.

Результаты исследования

В промышленности, в том числе в современном самолетостроении используется семь основных подходов организации производства представлены в табл. 1. Их главная задача снизить затраты и адаптацию к изменяющимся условиям рынка и повысить эффективность [7].

Таблица 1 – Подходы в организации производства

Подход	Основная цель	Ключевые особенности
Индустрия 4.0 / Цифровое производство	Полная цифровизация и автоматизация	Цифровые двойники, искусственный интеллект, интернет вещей
Гибкое производство	Быстрая адаптация к изменениям спроса	Модульные линии, короткие производственные циклы
Всеобщее продуктивное обслуживание оборудования	Максимальная доступность станков и оборудования	Предиктивное обслуживание, вовлечение операторов
Метод шести сигм	Снижение дефектов и вариативности	Статистический контроль качества
Кайдзен	Непрерывные мелкие улучшения	Участие всех сотрудников в предложениях
Теория ограничений	Устранение «узких мест»	Фокус на критических ресурсах
Умная фабрика	Интеграция интеллектуальных систем	Полностью автоматизированные «умные» линии

Индустрия 4.0 / Цифровое производство – ориентировано на внедрение цифровых технологий для создания «умных» производственных систем. Требуется больших инвестиций в оборудование и программное обеспечение, но дает высокий уровень автоматизации [8].

Гибкое производство – позволяет быстро перестраивать линии под новые заказы. Хорошо подходит для мелкосерийного и единичного типов производств, однако сложно в управлении.

Всеобщее продуктивное обслуживание оборудования – фокусируется на профилактике поломок и вовлечении персонала в обслуживание. Снижает простои, но требует высокой дисциплины.

Метод шести сигм – использует статистику для минимизации брака. Эффективен для стабильных процессов, но менее гибок при частых изменениях.

Кайдзен – основан на постоянных мелких улучшениях. Дешевый и универсальный подход, но результат становится явным на более длительном отрезке времени.

Теория ограничений – выявляет и устраняет главное «узкое место» в цепочке. Дает быстрый эффект, однако не решает все виды потерь.

Умная фабрика – следующий шаг Индустрии 4.0. Полностью интегрированные системы с автономным принятием решений. Требуется максимальных затрат и высокой квалификации кадров [7].

На основе подходов, представленных выше, можно сделать вывод, что для большинства из них требуются большие материальные затраты или в другом случае время на внедрение и отработку самого подхода прежде, чем он покажет свою эффективность. Именно эти показатели ограничивают их применение на предприятиях с ресурсными ограничениями.

Для решения таких проблем при ограниченных ресурсах на помощь приходит бережливое производство. Бережливое производство возникло в Японии в середине XX века на заводах Toyota благодаря работам Тайити Оно. Пять основных принципов бережливого производства: определение ценности для потребителя, анализ потока создания ценности, обеспечение непрерывного потока, организация вытягивающего производства, непрерывное совершенствование.

Дополнительно выделяют семь видов потерь: перепроизводство, ожидание, лишние транспортировки, лишние движения, переделки, излишние запасы и дефекты. Устранение этих потерь – основа всей системы [9].

К основным инструментам бережливого производства относятся: картирование потока создания ценности, система 5С (сортировка, соблюдение порядка, содержание в чистоте, стандартизация, совершенствование), система канбан, быстрая переналадка оборудования, точно в срок, выравнивание производства, защита от ошибок.

Особое внимание в исследовании уделено трем наиболее эффективным инструментам, применяемым в самолетостроительных предприятиях – системе канбан, 5С и точно в срок. Эти инструменты позволяют минимизировать запасы, организовать рабочее пространство и подавать материалы ровно тогда, когда они нужны [10, 11]. Сравнительный анализ бережливого производства и других подходов приведен в табл.2.

Таблица 2 – Сравнительный анализ бережливого производства и других подходов

Критерий	Бережливое производство (канбан, 5С, точно в срок)	Индустрия 4.0	Метод шести сигм	Кайдзен
Затраты на внедрение	Низкие	Высокие	Средние	Низкие
Скорость окупаемости	6–12 месяцев	2–4 года	12–18 месяцев	3–6 месяцев
Влияние на качество	Высокое (снижение брака до 80 %)	Высокое	Очень высокое	Среднее
Гибкость	Высокая	Высокая	Средняя	Высокая
Устойчивость к внешним изменениям	Высокая	Средняя	Средняя	Высокая

Бережливое производство выигрывает по соотношению «результат / затраты» [9].

Реальные примеры подтверждающие эффективность 2020–2025 годов.

В качестве классического и более яркого примера рассмотрим Toyota. В конце двадцатого века на предприятиях были внедрены следующие системы: канбан и точно в срок сократило, что время цикла на 50–70 % и брак на 80 %.

Российским примером выступает завод КАМАЗ – с 2010-х годов внедрена собственная производственная система на базе бережливого производства. Применение 5С и канбан дало рост производительности на 25–40 % и снижение запасов на 60 %.

Boeing – зарубежный авиационный кейс: инструменты бережливого производства (включая точно в срок) сократили время сборки самолетов на 30–50 %.

АО «Авиастар-СП» (Ульяновск) – российское самолетостроительное предприятие: внедрение системы 5С и канбан в 2020–2023 годах снизило время сборки узлов на 35–45 %, брак – на 50–70 %, а объем незавершенного производства сократился на 60 % [12, 13].

В результате мы видим для производственной отрасли следующие цифры: снижение времени на 30–70 %, снижение брака на производстве до 40 %, рост производительности на 25–40 %.

Таким образом мы видим, что бережливое производство в комбинации с инструментами канбан, 5С и точно в срок остается наиболее универсальным подходом. Оно не требует огромных финансовых вложений, имеет низкий срок окупаемости и устойчиво к санкциям, колебаниям спроса и сбоям поставок. На самолетостроительных предприятиях эти инструменты решают проблему длительных циклов и высокой сложности сборки. В условиях неопределенности или санкционного ограничения бережливое производство обеспечивает гибкость и минимальные потери, а его сочетание с цифровыми технологиями (Индустрия 4.0) открывает дальнейшие перспективы [7, 8].

Заключение

В результате проведенных исследований инновационных подходов в организации производства бережливое производство показало себя как наиболее эффективный и гибкий инструмент в ограниченных условиях. А наиболее одной из лучших комбинаций инструментов бережливого производства является связка из системы канбан, 5С и точно в срок. В самолетостроительной отрасли эти инструменты позволяют сократить время цикла на 30–70 %, снизить брак на 50–80 % и повысить производительность труда на 25–40 %.

Идея исследования полностью подтверждена: бережливое производство является основным и наиболее результативным инструментом среди всех рассмотренных инновационных подходов.

Внедрение рекомендуется начинать с участков сборки на предприятии. Сначала внедряется система 5С для организации рабочих мест и сокращению вспомогательного времени, затем система канбан и принцип «точно в срок». Следующим шагом станет обучения персонала новым компетенциям, обязанностью

руководства в таком случае станет внедрение их соблюдения в уже существующий менеджмент качества.

Перспективным направлением является сочетание бережливого производства с технологиями Индустрии 4.0, что приводит к созданию концепции бережливого производства 4.0. Это позволит сочетать низкозатратные инструменты с цифровыми двойниками и искусственным интеллектом.

Анализ и его результаты основаны на открытых данных и источниках 2018–2025 годов; результаты могут варьироваться в зависимости от конкретного предприятия и уровня организации его производственной системы.

В результате можно сделать следующий вывод: бережливое производство с инструментами канбан, 5С и точно в срок остается универсальным решением для повышения эффективности организации производства на предприятиях самых различных отраслей в том числе и самолетостроительных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Вялов А. В. Бережливое производство : учебное пособие. – Комсомольск-на-Амуре : ФГБОУ ВПО «КНАГТУ», 2014. – 100 с.
2. Давыдова Н. С. Бережливое производство. Развитие производственной системы организации : методическое пособие. – Ижевск : Институт экономики и управления ФГБОУ ВПО «УдГУ», 2015. – 58 с.
3. Бородулин А. Л., Казарин В. В., Косарева Н. С. Бережливое производство : учебное пособие. – СПб. : Питер, 2022. – 224 с.
4. Ключев А. В. Бережливое производство : учебное пособие для СПО / под ред. И. В. Ершовой. – Саратов ; Екатеринбург : Профобразование, 2019. – 87 с.
5. Виниченко В. А. Бережливое производство. Основы : учебное пособие. – Новосибирск : Изд-во НГТУ, 2020. – 100 с.
6. Туровец О. Г., Родионова В. Н. Генезис бережливого производства: российские истоки // Вестник Воронежского государственного технического университета. – 2015. – Т. 11. – № 1. – С. 68–74.
7. Бояринцева М. И. Практика применения бережливого производства на предприятиях авиастроения // Инновационная экономика: перспективы развития и совершенствования. – 2023. – № 4 (70). – С. 5–12. – URL: <https://cyberleninka.ru/article/n/praktika-primeneniya-berezhlivogo-proizvodstva-na-predpriyatiyah-aviastroeniya> (дата обращения: 14.04.2026).
8. Муравьева Е. В. Внедрение бережливого производства как фактор повышения конкурентоспособности авиастроительного предприятия АО «Авиастар-СП» // КиберЛенинка : науч. электрон. б-ка. – 2016. – URL: <https://cyberleninka.ru/article/n/vnedrenie-berezhlivogo-proizvodstva-kak-faktor-povysheniya-konkurentosposobnosti-aviastroitelnogo-predpriyatiya-ao-aviastar-sp> (дата обращения: 14.04.2026).
9. Трофимова Н. Н. Пятнадцать наиболее важных инструментов бережливого производства (Часть 1 и Часть 2) // КиберЛенинка : науч. электрон. б-ка. – 2022. – URL: <https://cyberleninka.ru/article/n/pyatnadsat-naibolee-vazhnyh-instrumentov-berezhlivogo-proizvodstva-chast-1-chast-2-1> (дата обращения: 14.04.2026).
10. Бояринцева М. И. Инновационные подходы к повышению эффективности производственных процессов на предприятиях авиакосмической и авиаремонтной сферы // КиберЛенинка : науч. электрон. б-ка. – 2025. – URL: <https://cyberleninka.ru/article/n/innovatsionnye>

podhody-k-povysheniyu-effektivnosti-proizvodstvennyh-protseessov-na-predpriyatiyah-aviakosmicheskoy-i (дата обращения: 14.04.2026).

11. Крамаренко Н. С. Совместимость Индустрии 4.0 с моделью управления бережливое производство и модернизация концепции в эпоху цифровизации // КиберЛенинка : науч. электрон. б-ка. – 2024. – URL: <https://cyberleninka.ru/article/n/sovместimost-industrii-4-0-s-modelyu-upravleniya-berezhlivoe-proizvodstvo-i-modernizatsiya-kontseptsii-v-epohu-tsifrovizatsii> (дата обращения: 14.04.2026).

12. Полковникова Е. Е. Использование технологий бережливого производства в аэрокосмической отрасли // КиберЛенинка : науч. электрон. б-ка. – 2017. – URL: <https://cyberleninka.ru/article/n/ispolzovanie-tehnologiy-berezhlivogo-proizvodstva-v-aerokosmicheskoy-otrasli> (дата обращения: 14.04.2026).

13. Нестеренко Д. В. Взаимосвязь робастного проектирования и бережливого проектирования в авиакосмической промышленности // КиберЛенинка : науч. электрон. б-ка. – 2017. – URL: <https://cyberleninka.ru/article/n/vzaimosvyaz-robastnogo-proektirovaniya-i-berezhlivogo-proektirovaniya-v-aviakosmicheskoy-promyshlennosti> (дата обращения: 14.04.2026).

© Р. А. Чупин, А. В. Шабурова, 2026

Д. А. Шергин^{1✉}, А. Н. Поликанин¹

Анализ уязвимостей веб-интерфейсов оптических роутеров

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: shergindanil717@gmail.com

Аннотация. В условиях активного использования телекоммуникационной инфраструктуры на оптоволоконные технологии доля абонентов, подключенных по технологии GPON, достигла максимального уровня за все время, что влечет за собой рост успешных атак на оптические терминалы с веб-интерфейсами управления. Актуальность работы обусловлена отсутствием специализированных автоматизированных инструментов для анализа защищенности данного класса устройств, а также ростом числа кибератак на сетевое оборудование в 2025 году. В данной статье проведен анализ актуальных уязвимостей веб-интерфейсов оптических роутеров на основе методики OWASP с учетом архитектурных особенностей встраиваемых устройств, а также разработан предварительный алгоритм автоматизированного программного обеспечения для анализа защищенности веб-интерфейсов оптических роутеров. В качестве нормативной основы анализа использована методика OWASP. В статье также определен перечень уязвимостей, наиболее актуальных именно для данного класса устройств.

Ключевые слова: информационная безопасность, безопасность инфраструктуры, оптический роутер, волоконно-оптическая линия передачи данных

D. A. Shergin^{1✉}, A. N. Polikanin¹

Development of a Virtual Stand for Practical Testing of Active Directory Information Security

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: shergindanil717@gmail.com

Abstract. As the telecommunications infrastructure actively shifts toward fiber-optic technologies, the share of subscribers connected via GPON has reached an all-time high, resulting in a growing number of successful attacks on optical network terminals with embedded web management interfaces. The relevance of this work is driven by the absence of specialized automated tools for security analysis of this device class, as well as the increase in cyberattacks targeting network equipment in 2025. This article analyses current vulnerabilities in optical router web interfaces based on the OWASP methodology, taking into account the architectural characteristics of embedded devices, and proposes a preliminary algorithm for automated software designed to assess the security of optical router web interfaces. The Open Worldwide Application Security Project (OWASP) methodology serves as the normative basis for the analysis. The article also identifies the set of vulnerabilities most relevant to this specific class of devices.

Keywords: information security, infrastructure security, optical router, optic data transmission line

Введение

На сегодняшний день активно развивается инфраструктура широкополосного доступа, которая представляет из себя совокупность из различных техниче-

ских устройств и сетей, обеспечивающих стабильное и высокоскоростное подключение к интернету [1]. Основой данного прогресса является оптическая передача информации, которая происходит посредством внедрения и популяризации волоконно-оптической линии передач, подключаемых к оптическим роутерам, как в частных домах, так и в организациях [2]. Каждое из этих устройств имеет встроенный веб-интерфейс, он служит для управления и настройки роутера. Данный веб-интерфейс является основной поверхностью атаки [3]. Оптический роутер, рассматриваемый как отдельно встраиваемое устройство, в отличие от отдельных корпоративных систем, часто не получает должного внимания [4]. Отсутствие практики регулярного обновления программного обеспечения, версии прошивки роутера, обновления учетных данных, все это подвергает опасности ключевые узлы в сети.

Злоумышленники не игнорируют этот факт. По данным «Информзащиты», за первые семь месяцев 2025 года число кибератак на сетевые устройства – маршрутизаторы, системы контроля доступа и камеры видеонаблюдения выросло на 24% по сравнению с аналогичным периодом 2024 года [5]. Основными жертвами стали организации из сферы информационных технологий и телекоммуникационного сектора, на которые пришлось 63% инцидентов. А статистика Positive Technologies показывает, что доля успешных атак на компьютеры, сервера и сетевое оборудование в период с середины 2024 по середину 2025 год является наибольшей среди всех категорий рис. 1 [6].

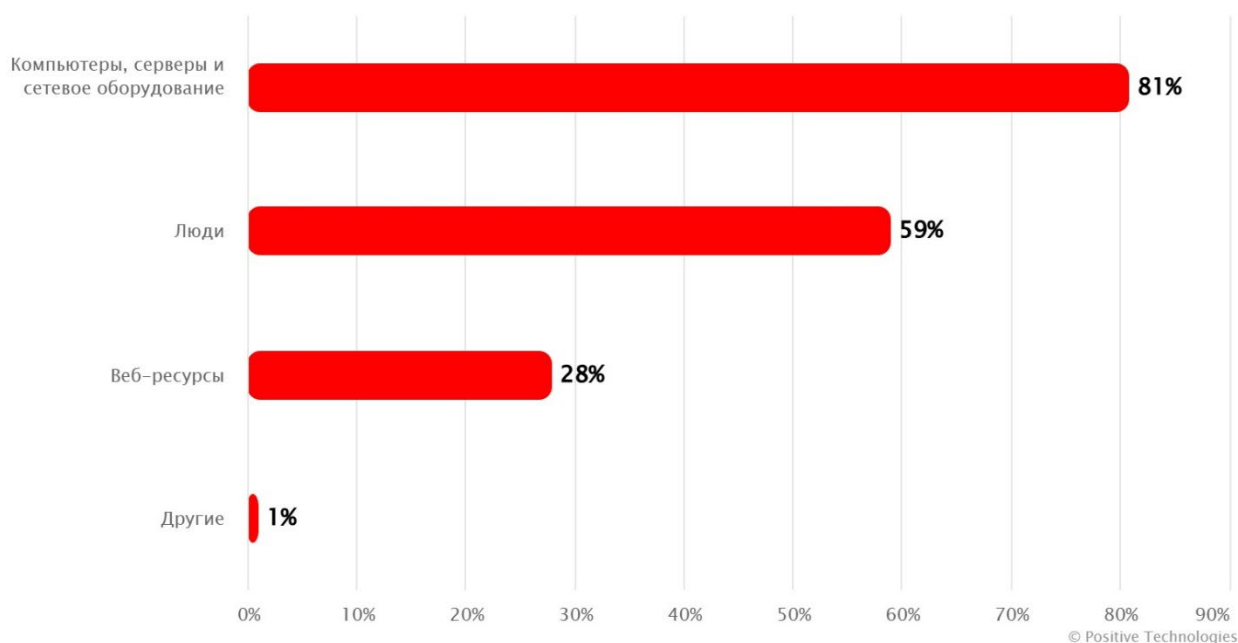


Рис. 1. Доля успешных атак от общего количества

Цель данной статьи: изучить и проанализировать основные уязвимости, которые могут содержать веб-интерфейсы оптических роутеров и разработать

предварительный алгоритм для автоматизированного программного обеспечения анализа защищенности веб-интерфейсов оптических роутеров.

Анализ актуальных уязвимостей

На текущий момент основной документ в сфере информационной безопасности, который определяет наиболее значимые риски для веб-приложений это методика Open Worldwide Application Security Project (далее – OWASP). Так как веб-интерфейс или система управления – это часть веб-приложения, то данную методику можно считать подходящей для текущего анализа [7-8].

В 2025 году OWASP опубликовали свежую подборку актуальных типов уязвимостей для веб-приложений. Они включают в себя:

- нарушение контроля доступа ();
- небезопасная настройка конфигурации ();
- использование компонентов с известными уязвимостями ();
- криптографические сбои ();
- инъекции ();
- небезопасная архитектура приложения ();
- сбой аутентификации;
- нарушение целостности программного обеспечения и данных;
- нарушение в работе системы регистрации и оповещения событий информационной безопасности;
- неправильная обработка ошибок.

Для веб-интерфейса оптического роутера наиболее актуальными уязвимостями были определены: сбой аутентификации, нарушение контроля доступа, инъекции, небезопасная настройка конфигурации и использование компонентов с известными уязвимостями. Выбор именно этих категорий обусловлен не произвольным решением, а совокупностью технических особенностей для данного класса устройств, которые описаны в статье далее.

Сбой аутентификации занимает особое место среди угроз для оптических терминалов. Так как парольная политика встраиваемых устройств часто не контролируется администратором, абонентское оборудование поступает к конечному пользователю с заводскими учетными данными, нередко одинаковыми для всей партии устройств конкретного вендора. Пользователь зачастую не меняет их либо из-за отсутствия технических знаний, либо потому что провайдер не требует этого явно. Так, в устройствах FiberHome AN5506 исследователи обнаружили более двадцати пяти жестко прописанных в прошивке учетных записей [9], а CVE-2021-27137 фиксирует аналогичную проблему в роутерах ZTE. Предсказуемость или полное отсутствие защиты на входе делает все остальное содержимое интерфейса открытым.

Нарушение контроля доступа логически продолжает предыдущую проблему. Даже при наличии формы входа многие CGI компоненты оптических терминалов допускают прямое обращение без предварительной аутентификации, достаточно знать путь. Это следствие архитектуры встраиваемых устройств и их веб-серверов. Разработчики прошивок нередко реализуют проверку сессии не

централизованно, а на уровне каждого обработчика по отдельности, что неизбежно приводит к пропускам.

Инъекции, прежде всего внедрение команд операционной системы (OS Command Injection), реализуются через поля, которые веб-интерфейс передает напрямую в системные вызовы: команды для диагностики ping и traceroute, поля настройки DNS и NTP. Встроенный веб-сервер выполняет их с правами суперпользователя, поскольку оптический терминал представляет из себя однопользовательскую систему без разделения привилегий. В результате злоумышленник может получить полный контроль над устройством через обычную строку в форме ввода. CVE-2023-28771 в оборудовании Zuxel и CVE-2024-21833 в ряде ONT-устройств подтверждают, что данный класс уязвимостей по-прежнему активно встречается в актуальных версиях устройств [10].

Небезопасная настройка конфигурации в контексте оптических роутеров проявляется прежде всего в том, что веб-интерфейс зачастую работает по протоколу HTTP, а не HTTPS, то есть все передаваемые данные, включая учетные данные, не шифруются. Параллельно с веб-интерфейсом нередко остаются включены Telnet и незащищенный SSH со стандартными портами.

Отключение неиспользуемых сервисов и принудительное использование защищенных протоколов является базовым требованием безопасности, которое производители бюджетного абонентского оборудования систематически игнорируют.

Использование компонентов с известными уязвимостями, наиболее системная проблема. Прошивки оптических терминалов строятся на базе открытых компонентов: веб-серверов GoAhead и mini_httpd, интерпретатора BusyBox, библиотек OpenSSL. Производители фиксируют версии этих компонентов на момент выпуска устройства и крайне редко выпускают обновления прошивки, а если и выпускают, пользователи их не устанавливают. В результате устройство, работающее пять лет без обновлений, несет в себе весь накопленный за это время груз известных CVE в своих зависимостях.

Остальные категории из методики OWASP не могут быть применимы к веб-интерфейсам оптических роутеров либо сложно верифицируемы автоматически без доступа к исходному коду прошивки, либо не формируют самостоятельного вектора атаки в рамках анализа именно веб-интерфейса. Это не означает их отсутствия в реальных устройствах, однако их исследование выходит за рамки задач автоматизированного сканирования и требует иных методов – в частности, анализа прошивки [11].

Практическая часть исследования

В рамках практической части исследования были отобраны основные актуальные типы уязвимостей, которые способно обнаружить автоматизированное программное обеспечение и построен предварительный алгоритм будущего автоматизированного программного обеспечения для анализа защищенности веб-интерфейсов оптических роутеров рис. 2.

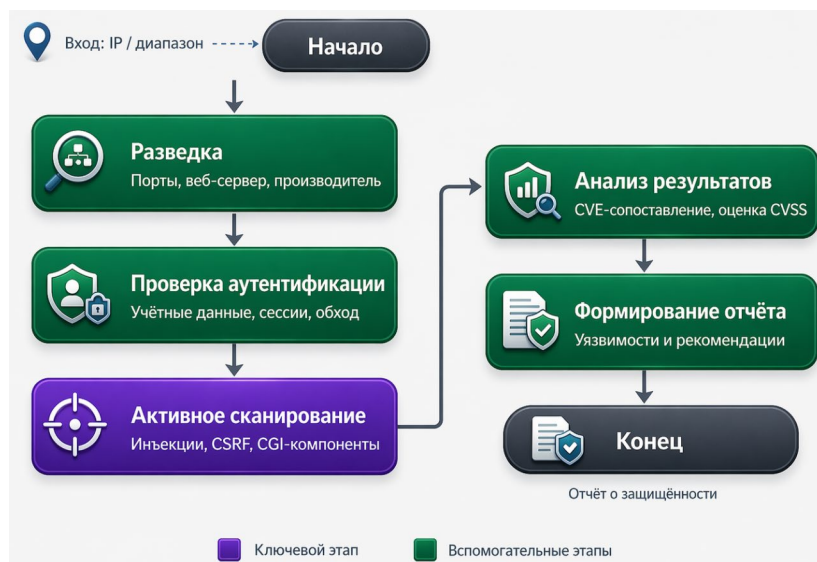


Рис. 2. Предварительный алгоритм программы

Цель данного алгоритма заключается в полном или практически полном покрытии всех поверхностей атаки и поиске уязвимостей, которые учитывают специфику оптических роутеров, их архитектуру и условия эксплуатации

Заключение

Данное исследование является аналитической основой разработки автоматизированного программного обеспечения для анализа защищенности веб-интерфейсов оптических роутеров. Предполагается, что данный анализ поможет лучше разобраться в специфике уязвимостей исследуемых устройств. В результате данной работы были определены актуальные уязвимости для веб-интерфейсов оптических роутеров, учитывающие специфику программных и архитектурных характеристик исследуемых устройств.

Дальнейшее исследование предполагает программную реализацию описанного алгоритма, его тестирование на реальных устройствах и разработку адаптированной метрики оценки критичности обнаруженных уязвимостей с учетом специфики устройств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кодиров Ф. Э. Технология GPON / Ф. Э. Кодиров, В. Г. Ачилова // Математическое и информационное моделирование: сб. статей. – Тюмень, 2018. – С. 176-181.
2. Оптоволоконные технологии в системах передачи данных / Е. А. Бадеева, Д. А. Усачев, И. А. Чернов [и др.] // Вестник Пензенского государственного университета. – 2022. – № 2(38). – С. 64-69.
3. Магжанов, М. М. Выявление недостатков аутентификации при проверке наличия пользовательской сессии в веб - интерфейсе администрирования домашнего роутера / М. М. Магжанов // фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации : сборник статей Международной научно-практической конференции,

Уфа, 27 декабря 2020 года. Том Часть 2. – Уфа: Общество с ограниченной ответственностью "ОМЕГА САЙНС", 2020. – С. 54-57.

4. Казарин О. В. Безопасность программного обеспечения компьютерных систем. - / О.В. Казарин. – М.: Московский государственный университет леса, 2003. – 212 с.

5. CNEWS. «Информзащита»: атаки на сетевое и охранное оборудование выросли почти на четверть в 2025 году. – Текст : электронный // OWASP : [сайт]. – URL: https://safe.cnews.ru/news/line/2025-08-15_informzashchita_ataki_na (дата обращения 01.04.2026).

6. Актуальные киберугрозы для организаций в СНГ: H2 2024 – Q3 2025. – Текст : электронный // Positive Technologies : [сайт]. – URL: <https://ptsecurity.com/research/analytics/cis-cyberthreat-landscape-h2-2024-q3-2025> – (дата обращения: 30.03.2026).

7. OWASP. OWASP Top 10:2025. – Текст : электронный // OWASP : [сайт]. – URL: <https://owasp.org/Top10/2025/> (дата обращения 01.04.2026).

8. OWASP. OWASP IoT. – Текст : электронный // OWASP : [сайт]. – URL: <https://owasp.org/www-project-internet-of-things/> (дата обращения 12.04.2026).

9. ANTI-MALWARE. В роутерах FiberHome нашли три десятка бэкдоров и других уязвимостей. – Текст : электронный // ANTI-MALWARE : [сайт]. – URL: <https://www.anti-malware.ru/news/2021-01-18-114534/34750> (дата обращения 07.04.2026).

10. NIST. CVE-2023-28771 Detail. – Текст : электронный // NIST : [сайт]. – URL: <https://nvd.nist.gov/vuln/detail/cve-2023-28771> (дата обращения 12.04.2026).

11. Зонов, А. С. Сканер прошивок оптических роутеров: подходы к обнаружению программных закладок / А. С. Зонов, А. В. Шабурова // Интерэкспо Гео-Сибирь. – 2025. – Т. 6. – С. 65-69.

© Д. А. Шергин, А. Н. Поликанин, 2026

Ю. О. Якович^{1✉}, А. Н. Поликанин¹

Использование технологий квантового шифрования в системах контроля управления доступом

¹ Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
e-mail: yakovich.yury@yandex.ru

Аннотация. Развитие квантовых вычислений создает угрозу для криптографической защиты систем контроля управления доступом (СКУД), основанной на алгоритмах RSA и ECC. Цель статьи – анализ применения квантового распределения ключей (QKD) для защиты каналов связи в СКУД. Рассмотрены протокол BB84 и стандарты постквантовой криптографии NIST. На основе анализа практических проектов (Южная Корея, Великобритания) обоснована многоуровневая архитектура защиты: использование QKD на уровне «контроллер–сервер» и постквантовых алгоритмов на нижних уровнях. Гибридный подход обеспечивает устойчивость к угрозе «сначала собери, потом расшифруй» без полной замены инфраструктуры.

Ключевые слова: квантовая криптография, квантовое распределение ключей, система контроля управления доступом, СКУД, BB84, постквантовая криптография, защита каналов связи

Y. O. Yakovich^{1✉}, A. N. Polikanin¹

Application of Quantum Encryption Technologies in Access Control Systems

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: yakovich.yury@yandex.ru

Abstract. The development of quantum computing poses a threat to the cryptographic protection of access control systems (ACS) based on RSA and ECC algorithms. This article analyzes the use of quantum key distribution (QKD) to secure communication channels in ACS. The BB84 protocol and NIST post-quantum cryptography standards are considered. Based on an analysis of practical projects (South Korea, UK), a multi-layered security architecture is substantiated: the use of QKD at the controller-server level and post-quantum algorithms at the lower levels. This hybrid approach ensures resilience to the "assemble first, then decrypt" threat without completely replacing the infrastructure.

Keywords: quantum cryptography, quantum key distribution, access control system, BB84, post-quantum cryptography, communication channel protection

Введение

Актуальность исследования обусловлена развитием квантовых вычислений, угрожающих безопасности криптографических протоколов СКУД. Криптографическая защита в СКУД реализуется на уровнях: идентификатор–считыватель (AES-128), считыватель–контроллер (OSDP), контроллер–сервер [1, 2]. Алгоритм Шора способен скомпрометировать RSA и ECC [3]. К середине 2030-х годов квантовые компьютеры нарушат безопасность классического шифрования; правительства

ряда стран устанавливают 2030–2035 гг. как срок миграции на квантово-устойчивые алгоритмы [4]. Дополнительную угрозу представляет стратегия «harvest now, decrypt later». Квантовое распределение ключей (QKD) – метод передачи ключей, безопасность которого основана на законах квантовой физики [5].

Цель статьи – анализ возможностей применения QKD для защиты каналов связи между элементами СКУД и обоснование архитектурного подхода к интеграции. Задачи: анализ уязвимостей криптографии СКУД; обзор протоколов QKD и стандартов NIST; систематизация практических примеров; разработка рекомендаций по интеграции.

Задачи: анализ уязвимостей криптографии СКУД; обзор протоколов QKD и стандартов NIST; систематизация практических примеров; разработка рекомендаций по интеграции.

Методы и материалы

Исследование выполнено методом аналитического обзора научных публикаций и стандартов за 2020–2026 гг. Базу составили статьи из журналов *Advances in Optics and Photonics*, *ACM Computing Surveys*, *Advanced Photonics*, документы NIST, ETSI, ITU-T, документация ID Quantique, Toshiba, Cisco.

Базовым протоколом QKD является BB84 (Беннет, Брассар, 1984 г.) [6]. Его безопасность основана на принципе неопределенности Гейзенберга и теореме о запрете клонирования квантовых состояний. Отправитель (Алиса) кодирует биты в поляризационных состояниях одиночных фотонов, используя два неортогональных базиса: прямолинейный (0° , 90°) и диагональный (45° , 135°). Получатель (Боб) случайно выбирает базис измерения. После передачи стороны сравнивают базисы по открытому каналу и отбрасывают несовпавшие результаты. Оставшиеся биты формируют секретный ключ [7].

Ключевое свойство протокола – обнаружение перехвата: измерение фотона злоумышленником неизбежно вносит ошибки. Уровень ошибок оценивается по QBER; при QBER выше $\sim 11\%$ канал считается скомпрометированным. Для формирования итогового ключа применяются процедуры согласования информации и усиления секретности [5, 7].

Наряду с BB84 развиваются протоколы на основе непрерывных переменных (CV-QKD), кодирующие информацию в амплитуде и фазе когерентных импульсов. Их преимущество – совместимость с существующим оптоволоконным и стандартными детекторами. В 2026 г. исследователи из Университета Падуи продемонстрировали интегральный приемник на стеклянной платформе (3,2 Мбит/с на 9,3 км, QRNG 42,7 Гбит/с) [8].

В августе 2024 г. NIST утвердил стандарты постквантовой криптографии: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), предназначенные для замены RSA и ECC [9]. Организациям рекомендовано начать миграцию на новые алгоритмы.

Результаты и обсуждение

Анализ практических проектов подтверждает зрелость QKD для защиты каналов связи. ID Quantique и SK Broadband развернули квантово-защищенную

сеть в Южной Корее (48 ведомств, 800 км) с непрерывным обновлением ключей [10]. BT, Toshiba и HSBC создали в Лондоне квантово-защищенную банковскую сеть; HSBC первым применил QKD совместно с PQC для защиты торгового терминала при моделировании валютной сделки на 30 млн евро [11].

Cisco разработала интерфейс SKIP для доставки квантовых ключей в IPsec и MACsec, поддерживаемый более чем десятью производителями [12]. Deutsche Telekom и Juniper Networks протестировали квантово-защищенное MACsec-шифрование по ETSI API [10]. В Китае QKD защищает каналы управления энергосетей, в Швейцарии – каналы передачи электоральных данных. Toshiba и NEC реализовали QKD с мультиплексированием по одному оптоволокну [11].

На основании анализа предлагается многоуровневая архитектура защиты каналов СКУД с использованием QKD (рис. 1). Модель включает: ML-KEM на уровне идентификатор-считыватель; симметричное шифрование с квантовыми ключами на уровне считыватель-контроллер; ротацию ключей через QKD на уровне контроллер-сервер.

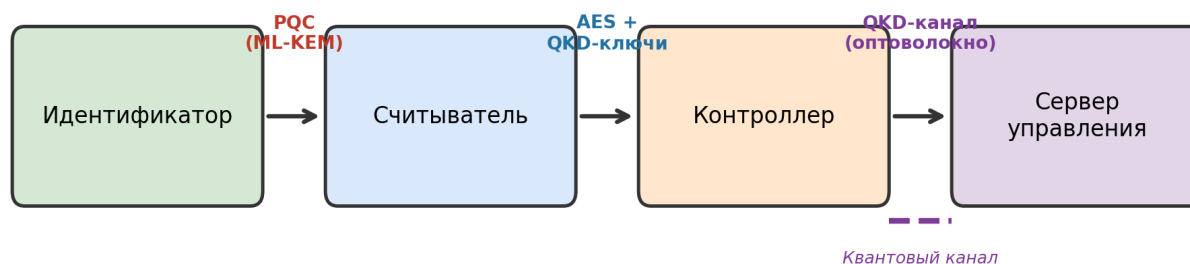


Рис. 1. Многоуровневая архитектура защиты каналов СКУД с использованием QKD

Внедрение QKD сопряжено с ограничениями: дальность – 100–150 км без ретрансляторов [7]; стоимость высока, хотя рынок растет. QKD требует предварительной аутентификации и подвержена атакам на оборудование, однако стандарты ISO/IEC 23837, ETSI ISG QKD, ITU-T серии 380x последовательно устраняют уязвимости [5].

Заключение

В соответствии с целью и задачами проведен анализ применения QKD для защиты каналов СКУД. Установлено, что RSA и ECC уязвимы перед квантовыми атаками, тогда как AES сохраняет устойчивость при надежном распределении ключей.

Обзор протоколов BB84 и CV-QKD показал, что QKD достигли уровня практического применения. Систематизация проектов (сети в Южной Корее, Великобритании; интерфейсы SKIP и ETSI QKD) подтверждает возможность шифрования каналов на существующей инфраструктуре.

Обоснована многоуровневая архитектура защиты СКУД: QKD на уровне контроллер–сервер, постквантовые алгоритмы NIST (FIPS 203–205) на уровне конечных устройств. Гибридный подход обеспечивает устойчивость СКУД к квантовым угрозам без полной замены инфраструктуры. Дальнейшие исследования направлены на разработку прототипа СКУД с модулем QKD.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. – М. : Горячая линия – Телеком, 2020. – 272 с.
2. Стасенко Л. Применение методов шифрования в СКУД // Системы безопасности. – 2022. – URL: https://www.aktivsb.ru/statii/primenenie_metodov_shifrovaniya_v_skud.html (дата обращения: 20.03.2026).
3. Shor P. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. – IEEE, 1994. – P. 124–134.
4. World Economic Forum. Quantum-Safe Migration: An Opportunity to Modernize Cryptography. – 2026. – URL: <https://www.weforum.org/stories/2026/01/quantum-safe-migration-cryptography-cybersecurity/> (дата обращения: 20.03.2026).
5. Pirandola S., Andersen U. L., Banchi L. et al. Advances in Quantum Cryptography // Advances in Optics and Photonics. – 2020. – Vol. 12, № 4. – P. 1012–1236.
6. Bennett C. H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Theoretical Computer Science. – 2014. – Vol. 560. – P. 7–11.
7. Mehic M., Niemiec M., Rass S. et al. Quantum Key Distribution: A Networking Perspective // ACM Computing Surveys. – 2020. – Vol. 53, № 5. – P. 1–41.
8. Avesani M. et al. Glass-based integrated quantum coherent receiver for CV-QKD and QRNG // Advanced Photonics. – 2026. – Vol. 8, № 2. – DOI: 10.1117/1.AP.8.2.026003.
9. NIST. Post-Quantum Cryptography FIPS Approved: FIPS 203, 204, 205. – 2024. – URL: <https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved> (дата обращения: 20.03.2026).
10. ID Quantique. Quantum Key Distribution: Integrated Solutions. – 2026. – URL: <https://www.idquantique.com/quantum-safe-security/integrated-solutions/> (дата обращения: 20.03.2026).
11. Building Resilient Security in the Age of Quantum Computing // ISACA Journal. – 2025. – Vol. 6. – URL: <https://www.isaca.org/resources/isaca-journal/issues/2025/volume-6/> (дата обращения: 20.03.2026).
12. Cisco. Quantum Key Distribution and the Path to Post-Quantum Computing. – 2025. – URL: <https://blogs.cisco.com/security/quantum-key-distribution-and-the-path-to-post-quantum-computing> (дата обращения: 20.03.2026).

© Ю. О. Якович, А. Н. Поликанин, 2026

СОДЕРЖАНИЕ

1. Д. М. Агеев, Д. М. Никулин. Стенд для контроля центрировки линз	3
2. А. А. Ануфриева, А. Ю. Чермошенцев. Методика выполнения обмерных работ методом наземной фотограмметрической съемки с применением панорамных камер	7
3. М. Е. Арапова, В. С. Ефремов. Автоматизация процесса поверки изделий с использованием искусственного интеллекта	14
4. Д. А. Бантос, И. О. Михайлов. Особенности использования и изготовления оптоволоконных катушек для беспилотных авиационных систем	22
5. К. В. Бондаренко. Анализ патентных решений и зарубежных разработок в области гиперспектральных систем для дистанционного зондирования	29
6. В. А. Васильева. Сравнение методов обработки для асферических зеркал и линз из разных материалов на станках алмазного микроточения	39
7. А. Д. Воропаев, В. М. Белов, Д. Л. Косов. Требования к цифровым доказательствам, полученным с использованием систем искусственного интеллекта	46
8. А. В. Галлямова, В. М. Белов. Содержание блока психофизических характеристик специалиста в области информационной безопасности	56
9. Н. С. Демин, В. В. Селифанов. Оценка эффективности системы защиты значимого объекта критической информационной инфраструктуры на основе сравнительного анализа методик оценки	63
10. К. А. Жуйков, А. В. Шабурова. Особенности синергии эффективных инструментов и подходов к управлению высокотехнологическими предприятиями	68
11. В. А. Захаров, А. В. Троеглазова. Сравнительный анализ нормативных подходов и практик управления киберрисками в кредитно-финансовых организациях	76
12. В. И. Ковынев, Е. А. Усанькова. Специфика механизма управления развитием наукоёмких производств в микроэлектронике	87
13. С. С. Кузьмин, А. Н. Поликанин. Сравнительный анализ способов обнаружения БПЛА	92
14. А. В. Кукса, Е. А. Усанькова. Конструкторско-технологическая оптимизация как инновационный подход к процессу производства	97
15. А. С. Лаптева, Е. С. Агеенко. Необходимость и проблематика внедрения 3D-формата в процесс территориального планирования	101
16. П. О. Лозовский, А. В. Шабурова. Роль организаций как операторов персональных данных	109
17. А. Я. Маршнина, В. В. Селифанов. Проблемные аспекты разработки и внедрения системы управления информационной безопасностью в IT- компании	117

18. Н. А. Мжельский, Т. Н. Хацевич. Анализ оптических систем современных миниатюрных объективов для камер смартфонов	124
19. М. Д. Михайлов, Е. А. Усанькова. Оптимизация процессов жизненного цикла инновационной продукции в условиях цифровой экономики	133
20. Е. С. Мишечкин, М. П. Егоренко, Н. А. Гурин. Сравнение глубокого шлифования и полирования классическим методом с предлагаемым методом на примере подложек для оптических покрытий лазерных систем.....	141
21. А. С. Москаленко, Е. Н. Кулик. Оценка ресурсного потенциала территории на основе автоматизированного дешифрирования космических снимков и комплексного геоморфологического анализа	149
22. Е. С. Панюкова, А. В. Шабурова. Оценка результативности и прогнозирование показателей эффективности СМК наукоемких предприятий на основе методов компьютерного моделирования	155
23. М. В. Пилипич, А. В. Шабурова. Построение системы защиты информации, для системы оповещения населения города.....	162
24. С. Д. Плотников. Методика исследования точности и воспроизводимости метрических характеристики 3D-сканов и цифровых изображений	172
25. К. С. Редколес. Разработка структуры методики расчета дальности действия низкоуровневых телевизионных систем на основе гибридного электровакуумного фотоприемного устройства.....	180
26. М. Д. Рублев, А. В. Шабурова. Совершенствование защиты объектов критической информационной инфраструктуры в организации	186
27. А. Р. Сабилов, М. М. Шляхова. Исследование метода семантической сегментации изображений с помощью искусственного интеллекта	191
28. П. Е. Самсонов, А. Ю. Чермошенцев. Разработка методики экологического картографирования по данным дистанционного зондирования Земли	198
29. А. И. Ступин, В. В. Селифанов. Разработка методики испытаний государственной информационной системы: подходы, этапы и практические рекомендации.....	206
30. В. П. Цыплаков, Д. М. Никулин. Обзор методов контроля разрешающей способности ЭОП	212
31. М. В. Чикирисов, Т. Н. Хацевич. Оценка хроматизма положения одиночной линзы и двухлинзового дублета в спектральном диапазоне 0,4–1,1 мкм	219
32. Р. А. Чупин, А. В. Шабурова. Инновационные подходы в организации производства	227
33. Д. А. Шергин, А. Н. Поликанин. Анализ уязвимостей веб-интерфейсов оптических роутеров.....	234
34. Ю. О. Якович, А. Н. Поликанин. Использование технологий квантового шифрования в системах контроля управления доступом	240

CONTENTS

1. D. M. Ageev, D. M. Nikulin. Lens Centering Verification Stand.....	3
2. A. A. Anufrieva, A. Y. Chermoshentsev. Methodology of Surveying Works Using Terrestrial Photogrammetry with Panoramic Cameras	7
3. M. E. Arapova, V. S. Efremov. Automation of the product verification process using artificial intelligence.....	14
4. D. A. Bantos, I. O. Mikhailov. Features of Using and Manufacturing of Fiber Optic Coils for Unmanned Aerial Vehicles.....	22
5. K. V. Bondarenko. Analysis of Patent Solutions and Foreign Developments in the Field of Hyperspectral Systems for Remote Sensing	29
6. V. A. Vasileva. Comparison of processing methods on diamond micro- machining machines for aspherical mirrors and lenses made of different materials	39
7. A. D. Voropaev, V. M. Belov, D. L. Kosov. Requirements for Digital Evidence Obtained Using Artificial Intelligence Systems.....	46
8. A. V. Gallyamova, V. M. Belov. Contents of a Set of Psychophysical Characteristics of an Information Security Specialist.....	56
9. N. S. Demin, V. V. Selifanov. Assessment of the Effectiveness of the Critical Information Infrastructure Protection System Based on Comparative Analysis of Assessment Methods	63
10. K. A. Zhuykov, A. V. Shaburova. Features of the Synergy of Effective Tools and Approaches to Managing High-Tech Enterprises.....	68
11. V. A. Zakharov, A. V. Troeglazova. Comparative Analysis of Regulatory Approaches and Practices for Managing Cyber Risks in Credit and Financial Organizations	76
12. V. I. Kovynev, E. A. Ysankova. The Specifics of the Mechanism for Managing the Development of Science-Intensive Production in Microelectronics	87
13. S. S. Kuzmin, A. N. Polikanin. Comparative Analysis of UAV Detection Methods	92
14. A. V. Kuksa, E. A. Usankova. Design and technological optimization as an innovative approach to the production process	97
15. A. S. Lapteva, E. S. Ageenko. Necessity and Problems of Implementing the 3D Format in the Territorial Planning Process.....	101
16. P. O. Lozovsky, A. V. Shaburova. The Role of Organizations as Personal Data Controllers	109
17. A. Y. Marshinina, V. V. Selifanov. Problematic Aspects of Developing and Implementing of Information Security Management System Processes in IT Company	117
18. N. A. Mzhelskiy, T. N. Khatsevich. Analysis of the Optical Systems of Modern Miniature Smartphone Camera Lenses	124

19. M. D. Mikhailov, E. A. Usankova. Optimizing the life Cycle Processes of Innovative Products in the Digital Economy	133
20. E. S. Mishechkin, M. P. Egorenko, N. A. Gurin. Comparison of Deep Grinding and Polishing using the Classical Method with the Proposed Method using Laser-Resistant Coatings as an Example.....	141
21. A. S. Moskalenko, E. N. Kulik. Assessment of the territory resource potential based on automated interpretation of space images and complex geomorphological analysis.....	149
22. E. S. Panyukova, A. V. Shaburova. Assessing Effectiveness and Predicting Performance Indicators of the Quality Management System of High-Tech Enterprises Based on Computer Modeling Methods	155
23. M. V. Pilipich, A. V. Shaburova. Building an Information Protection System for the City's Public Warning System	162
24. S. D. Plotnikov. Methodology for studying the accuracy and reproducibility of metric characteristics of 3D scans and digital images	172
25. K. S. Redkoles. Development of a Methodological Framework for Operating Range Calculation of Low-Light-Level Television Systems Based on Hybrid Electro-Vacuum Photodetectors.....	180
26. M. D. Rublyov, A. V. Shaburova. Improving the Protection of Critical Information Infrastructure Facilities in an Organization	186
27. R. Sabirov, M. M. Shlyakhova. Research on Semantic Image Segmentation Methods using Artificial Intelligence	191
28. P. E. Samsonov, A. Y. Chermoshentsev. Development of a Methodology for Environmental Mapping Based on Earth Remote Sensing Data	198
29. A. I. Stupin, V. V. Selifanov. Development of a Testing Methodology for a State Information System: Approaches, Stages and Practical Recommendations	206
30. V. P. Tsyplakov, D. M. Nikulin. Review of Methods for Controlling the Resolution of Image Intensifier Tubes	212
31. M. V. Chikirisov, T. N. Khatsevich. Estimation of the Chromaticity of the Position of a Single Lens and a Double-Lens Doublet in the Spectral Range of 0,4–1,1 Microns	219
32. R. A. Chupin, A. V. Shaburova. Innovative Approaches to Production Organization	227
33. D. A. Shergin, A. N. Polikanin. Development of a Virtual Stand for Practical Testing of Active Directory Information Security.....	234
34. Y. O. Yakovich A. N. Polikanin. Application of Quantum Encryption Technologies in Access Control Systems	240

Научное издание

ИНТЕРЭКСПО ГЕО-СИБИРЬ

XXII Международный научный конгресс

Сборник материалов в 9 т.

Т. 6

Магистерская научная сессия

«ПЕРВЫЕ ШАГИ В НАУКЕ»

Материалы публикуются в авторской редакции

Компьютерная верстка *Я. А. Лесных*

Изд. лиц. ЛР № 020461 от 04.03.1997.

Подписано в печать 12.08.2026. Формат 60 × 84 1/16.

Усл. печ. л. 14,41. Тираж 25 экз. Заказ 143.

Гигиеническое заключение

№ 54.НК.05.953.П.000147.12.02. от 10.12.2002.

Издательско-полиграфический центр СГУГиТ

630108, Новосибирск, ул. Плахотного, 10.

Отпечатано в издательско-полиграфическом центре СГУГиТ

630108, Новосибирск, ул. Плахотного, 8.