

Международный журнал информационных технологий и энергоэффективности



Том 9 Номер 10 (48)



2024



СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

1.	Балашов О.В., Букачев Д.С. Классификация критериев выбора альтернатив при принятии управленческих решений	5
	Balashov O.V., Bukachev D.S. Classification of criteria for selecting alternatives when making managerial decisions	
2.	Балашов О.В., Букачев Д.С. Суриков А.А. Интеграция конфигураций на базе «1С: ПРЕДПРИЯТИЕ» с цифровыми платформами	12
	Balashov O.V., Bukachev D.S., Surikov A.A. Integration of configurations based on "1S: ENTERPRISE" with digital platforms	
3.	Авдалян А.А. Критическая уязвимость - CVE-2023-27350	18
	Avdalyan A.A. Critical vulnerability - CVE-2023-27350	
4.	Авдалян А.А. SNYK CODE: как защитить код от уязвимостей	22
	Avdalyan A.A. SNYK CODE: how to protect your code from vulnerabilities	
5.	Авдалян А.А. Юридические аспекты в DFIR	26
	Avdalyan A.A. Legal aspects in DFIR	
6.	Гаджиев Г.К. Методы обнаружения и предотвращения атак на мобильные	30
	Gadzhiev G.K. Methods for detecting and preventing attacks on mobile devices	
7.	Гаджиев Г.К. Развитие технологий квантовой криптографии и их роль в обеспечении информационной безопасности	34
	Gadzhiev G.K. Development of quantum cryptography technologies and their role in ensuring information security	
8.	Гаджиев Г.К. Защита персональных данных и приватности в эпоху цифровизации: вызовы и решения	38
	Gadzhiev G.K. Protection of personal data and privacy in the era of digitalization: challenges and solutions	
9.	Астахов К.А. Разработка архитектурных решений для создания ВЭБ-сервиса по разворачиванию сайтов научных мероприятий.	42
	Astakhov K.A. Development of architectural solutions for the creation of a web service for the deployment of scientific event sites	
10.	Любченко Э.М. Метод получения карт высот на основе генеративно-состязательной сети	51

	Lyubchenko E.M. Method of generating heightmaps based on generative adversarial network	
11.	Подгорнов М.Д. Модель системы массового обслуживания «ПОЧТИ-ТОЧНО-В-СРОК»	59
	Podgornov M.D. The queuing system «ALMOST-JUST-IN-TIME» model	
12.	Овсянников Р.Я. Применение VLAN в сетях CISCO: эффективность и настройка	65
	Ovsyannikov R.Ya. Using VLANS in CISCO networks: efficiency and configuration	
13.	Иванов Ю.П., Красненков Н.С. Сравнительный анализ финитно-временного с обратной связью и спектрально-финитного без обратной связи методов обработки измерительной информации	70
	Ivanov Yu.P., Krasnenkov N.S. Comparative analysis of finite-time feedback and spectral-finite non-feedback measurement processing methods	
14.	Иванов Ю.П., Красненков Н.С. Сравнительный анализ спектрально-финитного без обратной связи метода обработки измерительной информации и фильтра Калмана	77
	Ivanov Yu.P., Krasnenkov N.S. Comparative analysis of the spectral-finite method of processing measurement information without feedback and the Kalman filter	
15.	Туртыгин А.А. Реализация протокола аутентификации с нулевым разглашением с использованием меток	83
	Turtygin A.A. Implementation of zero-knowledge authentication protocol using labels	
16.	Марква Т.Д. Безопасность и приватность в блокчейн сетях. методы и технологии защиты данных	90
	Markva T.D. Security and privacy in blockchain networks. data protection methods and technologies	
17.	Марква Т.Д. Блокчейн и искусственный интеллект. возможности и перспективы совместного использования	96
	Markva T.D. Blockchain and artificial intelligence. opportunities and prospects for sharing	
18.	Вилясов А.Р., Мелькин М.В., Левкин Н.Е. Цифровые двойники: технология, формирующая будущее	104
	Viryasov A.R., Melkin M.V., Levkin N.E. Digital twins: the technology shaping the future	
19.	Кондрашов А.С., Куснуяров Р.Э. Поддержка фоновой работы: прерывание процессов шифрования/дешифрования при остановке работы АРМ	110
	Kondrashov A.S., Khusnuyarova R.E. Support for background work: interruption of encryption/decryption processes when the automated control system is stopped	
20.	Кириллов Д.О. Ключевая роль исследований в области динамики полета, систем управления и моделирования для развития авиационных наук	119

	Kirillov D.O. The key role of research in the field of flight dynamics, control systems and simulation for the development of aviation sciences.	
21.	Кириллов Д.О. Современные проблемы аэродинамики воздушных судов	125
	Kirillov D.O. Modern problems of aircraft aerodynamics.	
22.	Яковицкий С.А., Иванов А.А., Вавринюк С.А. Совершенствование системы управления информационными операциями ВВС США	132
	Yakovitsky S.A., Ivanov A.A., Vavrinyuk S.A. Improving the U.S. air force information operations management system	
23.	Марква Т.Д. Устойчивый блокчейн. пути минимизации энергопотребления	136
	Markva T.D. A stable blockchain. ways to minimize energy consumption	
ЭНЕРГЕТИКА И ЭНЕРГОЭФФЕКТИВНОСТЬ		
24.	Мартынов А.П., Головинов В.В., Гладкина Е.М., Малышев А.М., Гаркушин Д.М. Актуальность разработки методов количественной оценки надежности электроэнергетических систем	142
	Martynov A.P., Golovinov V.V., Gladkina E.M., Malyshev A.M., Garkushin D.M. The relevance of the development of quantitative methods reliability assessments of electric power systems	
25.	Канарейкин А.И. Термонапряженное состояние твэла с переменным коэффициентом линейного расширения	148
	Kanareykin A.I. Thermally stressed state of a fuel element with a variable coefficient of linear expansion	
ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ		
26.	Зиннуров Т.А., Ионов И.А. Обследование и оценка несущей способности демонтируемых сталежелезобетонных пролетных строений	154
	Zinnurov T.A., Ionov I.A. The survey and the calculation of the carrying capacity of dismantled composite bridge spans	
27.	Ворганов А.А., Котенёв Е.В., Курдюмов И.А., Каленский И.А., Федоров А.М. Анализ воздействия лазерного излучения на оптические устройства БПЛА	165
	Varganov A.A., Kotenev E.V., Kurdyumov I.A., Kalensky I.A., Fedorov A.M. Analysis of the effect of laser radiation on UAV optical devices	



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 519.816

КЛАССИФИКАЦИЯ КРИТЕРИЕВ ВЫБОРА АЛЬТЕРНАТИВ ПРИ ПРИНЯТИИ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ

¹Балашов О.В., ²Букачев Д.С.

¹АО «РАДИОЗАВОД», НИО-4, Смоленск, Россия, (214027, г. Смоленск, улица Котовского, 2), e-mail: smradio@mail.ru

²ФГБОУ ВО «СМОЛЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Смоленск, Россия (214000, г. Смоленск, ул. Пржевальского, 4), e-mail: dsbuka@yandex.ru

Статья посвящена важности классификации критериев при принятии управленческих решений. В условиях растущей неопределенности и динамично изменяющейся среды систематизация критериев позволяет эффективно оценивать альтернативы, что минимизирует вероятность принятия ошибочных решений. Рассматриваются основные категории критериев, используемых для оценки управленческих решений, включая экономические, технические, социальные, экологические и политико-правовые. Авторы подчеркивают значимость многокритериального анализа (MCDM) для обеспечения сбалансированности при выборе альтернатив. Исследуются примеры классификации критериев из различных отраслей, таких как устойчивое развитие, промышленность и государственное управление. Предлагается системный подход к классификации критериев и подчеркивается актуальность данного вопроса в условиях современной экономики.

Ключевые слова: Генерация альтернатив, оценка альтернатив, классификация критериев, многокритериальный анализ (MCDM).

CLASSIFICATION OF CRITERIA FOR SELECTING ALTERNATIVES WHEN MAKING MANAGERIAL DECISIONS

¹Balashov O.V., ²Bukachev D.S.

¹JOINT-STOCK COMPANY "RADIO FACTORY", RESEARCH DEPARTMENT 4, Russia, (214027, Smolensk, street Kotovskogo, 2), e-mail: smradio@mail.ru

²FEDERAL STATE EDUCATIONAL INSTITUTION OF HIGHER EDUCATION SMOLENSK STATE UNIVERSITY, Smolensk, Russia (214000, Smolensk, street Przewalski, 4), e-mail: dsbuka@yandex.ru

The article is devoted to the importance of criteria classification in making managerial decisions. Under conditions of growing uncertainty and dynamically changing environment, the systematization of criteria allows to effectively evaluate alternatives, which minimizes the probability of making erroneous decisions. The main categories of criteria used to evaluate managerial decisions are considered, including economic, technical, social, environmental and political-legal ones. The authors emphasize the importance of multi-criteria analysis (MCDM) in balancing the selection of alternatives. Examples of criteria classification from different sectors such as sustainable development, industry and public administration are explored. A systematic approach to the classification of criteria is proposed and the relevance of this issue in today's economy is emphasized.

Keywords: Generation of alternatives, evaluation of alternatives, classification of criteria, multiple-criteria decision-making (MCDM).

При разработке системы поддержки принятия решений (СППР) возникла проблема определения перечня критериев для оценки альтернатив. Для упорядочивания этого процесса

было принято решение проанализировать существующие публикации. Анализ отечественной литературы показал, что данному вопросу уделяется недостаточное внимание, тогда как зарубежные авторы накопили определенный научно-практический потенциал в данной сфере.

Процесс разработки и принятия управленческих решений требует оценки множества факторов, таких как экономические, социальные, экологические и технологические. В условиях быстро изменяющейся внешней среды и увеличивающейся неопределённости важно использовать классификацию критериев, которая позволит систематизировать и упростить процесс выбора альтернатив. Без чёткой классификации сложно учесть все важные параметры при генерации альтернатив и оценке их качества, что может привести к принятию ошибочных решений.

Вопросы генерации и выбора альтернатив при принятии управленческих решений рассматриваются многими авторами.

Herbert A. Simon в своей статье [1] исследует процессы формирования проблем и генерации альтернатив в организационном контексте. Эта работа считается классической в изучении когнитивных процессов, связанных с выбором решений. Саймон анализирует процесс генерации альтернатив и эффективность методов для оптимизации данного процесса

Vladimir M. Ozerouy в своей работе [2] проводит обзор различных подходов к генерации альтернатив в многокритериальных задачах принятия решений. Он рассматривает методы многокритериальной оптимизации и предлагает классификацию подходов для различных областей применения, включая государственное управление и промышленное производство.

Pluchinotta, I. в соавторстве с Kazakçi, A.O., Giordano, R. [3] анализирует процессы генерации альтернатив в контексте разработки государственной политики. Исследование посвящено моделям и инструментам, которые могут помочь в создании оптимальных альтернатив для общественных решений, таких как водные ресурсы и устойчивое развитие.

Большинство исследований в области принятия управленческих решений так или иначе сводятся к методам многокритериального оценивания альтернатив, однако сам вопрос выбора совокупности критериев, которые используются для оценки и выбора альтернатив, остается открытым.

Часто управленческие решения требуют учёта множества противоречащих критериев. Например, в проектах по устойчивому развитию нужно учитывать как экономические показатели, так и воздействие на окружающую среду и социальные последствия. Это делает необходимым наличие методов и систем, которые помогут классифицировать и ранжировать эти критерии по степени важности. Классификация критериев позволяет упростить процесс принятия решений за счёт структурирования информации и системного анализа. Это особенно важно в условиях ограниченных ресурсов и времени, когда быстрый и точный выбор альтернатив критичен для успеха организации. Структурированные критерии могут быть использованы для создания моделей, таких как методы многокритериального анализа (MCDM), что делает процесс принятия решений более эффективным и прозрачным [4].

С развитием технологий и ростом доступности больших данных возникла необходимость в новых подходах к классификации критериев. Современные системы управления часто интегрируют данные из множества источников. Автоматизация процесса принятия решений требует структурированного подхода к классификации критериев и прозрачности процесса принятия решений. Чёткое понимание того, какие критерии использовались и как они были классифицированы, позволяет не только оптимизировать

выбор, но и сделать его обоснованным, что позволяет использовать алгоритмы машинного обучения для оптимизации принятия решений [5, 6]

Таким образом, актуальность задачи классификации критериев заключается в её значимости для повышения качества, эффективности и обоснованности управленческих решений в условиях многокритериальности, неопределённости и растущих требований к прозрачности процессов принятия решений.

Хотя общепринятой классификации критериев принятия решений нет, попытки категоризации критериев существуют.

К примеру, Taherdoost, Н. и Madanchian, М. [6] выделяют две основные категории критериев:

- Количественные критерии: включают легко измеримые параметры, такие как стоимость, прибыль, производительность. Эти критерии часто применяются для оценки эффективности и финансовых аспектов альтернатив.
- Качественные критерии: труднее поддаются измерению, так как включают такие аспекты, как удовлетворенность клиентов, социальная устойчивость и инновационность. Для их оценки используются качественные методы, такие как экспертные оценки и шкалирование.

Alsaig A. [4] предложил классифицировать критерии на основе их важности или веса. В этой классификации критерии делятся на:

- Главные критерии: критически важные для достижения цели, такие как безопасность или производительность в секторе здравоохранения.
- Второстепенные критерии: менее значимые, но также влияющие на процесс выбора, такие как эстетические характеристики или удобство использования. Важность критериев варьируется в зависимости от контекста применения, что учитывается при взвешивании.

В исследованиях Werners, В. и Zimmermann, Н.Ж. [5] используется теория нечетких множеств для классификации критериев, особенно в условиях неопределенности. Критерии делятся на:

- Детерминированные критерии: данные точны и известны.
- Нечеткие критерии: данные частично неизвестны или неопределённые. Такие критерии требуют использования методов, основанных на теории нечетких множеств и вероятностных моделей, чтобы учесть неопределенность в процессе принятия решений.

Многие современные исследования также подчеркивают важность временного аспекта в классификации критериев:

- Краткосрочные критерии: ориентированы на немедленные результаты, такие как снижение затрат или улучшение операционной эффективности.
- Долгосрочные критерии: включают такие факторы, как стратегическое развитие, устойчивость и инновации. Эти критерии важны для компаний, стремящихся к долгосрочной конкурентоспособности и устойчивости.

Наиболее конструктивные классификации критериев оценивания альтернатив, которые могут стать базой при решении конкретных задач, получены авторами, которые классифицируют критерии в конкретных секторах, таких как промышленность, здравоохранение, образование, экология и финансы.

Taherdoost, H. и Madanchian, M. в статье [6] предложили систематический обзор методов и концепций многокритериального анализа решений (MCDA), применимого в различных областях, включая финансы и инженерное проектирование. Авторы выделяют как качественные, так и количественные критерии, которые варьируются в зависимости от области применения и метода анализа.

Erdogan, S.A., Šaparauskas, J. и Turskis, Z в статье [7] представили модель выбора оптимальной альтернативы для устойчивого управления строительными проектами. Они использовали метод анализа иерархий, применяя его для оценки альтернатив с точки зрения устойчивости, что показало важность применения многокритериальных методов в строительной отрасли.

В книге «Multiple Criteria Decision Making» под редакцией Anand J. Kulkarni [8], описываются современные подходы к многокритериальному принятию решений с анализом теоретических основ и применением в таких областях, как оптимизация и образование, приведены примеры использования многокритериальных методов в реальных приложениях.

Эти работы демонстрируют, что классификация критериев варьируется в зависимости от целей и контекста принятия решений. Обобщая существующие попытки классифицировать критерии принятия решений, можно предложить следующую классификацию.

1. Экономические критерии (относятся к финансовым аспектам и анализируют, насколько альтернатива рентабельна):

- Стоимость: включает капитальные и операционные затраты.
- Рентабельность: предполагаемая прибыль от выбранного решения.
- Возврат инвестиций (ROI): анализирует время, за которое вложенные средства будут возвращены.
- Риски: оценка возможных финансовых рисков, таких как колебания цен, валютные риски, финансовая нестабильность.

2. Технические критерии (относятся к техническим аспектам, особенно важны в промышленности и инженерии).

- Надёжность: способность оборудования или процесса стабильно функционировать в течение длительного времени.
- Совместимость: насколько альтернатива совместима с существующими системами или инфраструктурой.
- Инновации: уровень использования новых технологий и решений.

3. Социальные критерии (используются для оценки воздействия альтернатив на людей и общество в целом):

- Создание рабочих мест: как альтернатива влияет на рынок труда и занятость.
- Социальная справедливость: оценка того, насколько альтернатива улучшает социальные условия.
- Этические нормы: соблюдение прав человека, экологических стандартов и корпоративной ответственности.

4. Экологические критерии: (касаются воздействия на окружающую среду и устойчивого развития):

- Устойчивое развитие: насколько решение способствует снижению использования невозобновляемых ресурсов и переходу к устойчивым технологиям.

- Загрязнение и выбросы: уровень загрязнения воздуха, воды, выбросы углекислого газа.
 - Утилизация отходов: насколько легко отходы от деятельности могут быть переработаны или утилизированы без вреда для окружающей среды.
5. Политические и правовые критерии (оценивают влияние политических и правовых факторов на принятие решения)
- Соблюдение законодательства: насколько альтернатива соответствует текущим правовым нормам и требованиям.
 - Поддержка правительства: возможное государственное финансирование или налоговые льготы.
6. Временные критерии (касается временных рамок, в которые должна быть реализована альтернатива):
- Время реализации: как быстро решение может быть внедрено и начать функционировать.
 - Долговечность: оценка долгосрочных последствий выбора.
7. Культурные и организационные критерии (оценивают, насколько альтернатива соответствует организационным и культурным нормам):
- Организационная культура: соответствие альтернативы ценностям и культуре компании.
 - Восприятие сотрудников: как альтернатива будет воспринята внутри организации.
- Например, при выборе альтернативы для нового производственного комплекса менеджеры могут использовать следующие критерии:
- Экономические: стоимость проекта и ожидаемая прибыль.
 - Технические: надёжность оборудования и его совместимость с существующими линиями.
 - Экологические: выбросы углекислого газа и возможность переработки отходов.
 - Социальные: количество создаваемых рабочих мест и влияние на местное население.
 - Временные: сроки завершения строительства и ввода в эксплуатацию.
- Таким образом, классификация критериев позволяет системно подходить к определению их перечня, что помогает принимать более обоснованные и устойчивые решения.

Список литературы

1. Simon, H.A. (1991). Problem Formulation And Alternative Generation In The Decision Making Process. In: Chikán, A. (eds) Progress in Decision, Utility and Risk Theory. Theory and Decision Library, vol 13. Springer, Dordrecht. URL: https://doi.org/10.1007/978-94-011-3146-9_4.
2. Ozeroy, V.M. (1985). Generating Alternatives in Multiple Criteria Decision Making Problems: A Survey. In: Haimen, Y.Y., Chankong, V. (eds) Decision Making with Multiple Objectives. Lecture Notes in Economics and Mathematical Systems, vol 242. Springer, Berlin, Heidelberg. URL: https://doi.org/10.1007/978-3-642-46536-9_23.
3. Pluchinotta, I., Kazakçi, A.O., Giordano, R. et al. Design Theory for Generating Alternatives in Public Decision Making Processes. Group Decis Negot 28, 341–375 (2019). URL: <https://doi.org/10.1007/s10726-018-09610-5>.

4. Alsaig, A., Alsaig, A., Alagar, V. (2024). A Critical Review of Multi Criteria Decision Analysis Method for Decision Making and Prediction in Big Data Healthcare Applications. In: Huang, DS., Premaratne, P., Yuan, C. (eds) Applied Intelligence. ICAI 2023. Communications in Computer and Information Science, vol 2015. Springer, Singapore. URL: https://doi.org/10.1007/978-981-97-0827-7_8.
5. Werners, B., Zimmermann, H.J. (1989). Evaluation and Selection of Alternatives Considering Multiple Criteria. In: Jovanović, A.S., Kussmaul, K.F., Lucia, A.C., Bonissone, P.P. (eds) Expert Systems in Structural Safety Assessment. Lecture Notes in Engineering, vol 53. Springer, Berlin, Heidelberg. URL: https://doi.org/10.1007/978-3-642-83991-7_10.
6. Taherdoost, H.; Madanchian, M. (2023) Multi-Criteria Decision Making (MCDM) Methods and Concepts. Encyclopedia 2023, 3, 77-87. URL: <https://doi.org/10.3390/encyclopedia3010006>.
7. Erdogan, S.A.; Šaparauskas, J.; Turskis, Z. A Multi-Criteria Decision-Making Model to Choose the Best Option for Sustainable Construction Management. Sustainability 2019, 11, 2239. URL: <https://doi.org/10.3390/su11082239>.
8. Anand J. (2022) Kulkarni Multiple Criteria Decision Making: Techniques, Analysis, and Applications. URL: <https://link.springer.com/book/10.1007/978-981-16-7414-3>.

References

1. Simon, H.A. (1991). Problem Formulation And Alternative Generation In The Decision Making Process. In: Chikán, A. (eds) Progress in Decision, Utility and Risk Theory. Theory and Decision Library, vol 13. Springer, Dordrecht. URL: https://doi.org/10.1007/978-94-011-3146-9_4.
2. Ozernoy, V.M. (1985). Generating Alternatives in Multiple Criteria Decision Making Problems: A Survey. In: Haimes, Y.Y., Chankong, V. (eds) Decision Making with Multiple Objectives. Lecture Notes in Economics and Mathematical Systems, vol 242. Springer, Berlin, Heidelberg. URL: https://doi.org/10.1007/978-3-642-46536-9_23.
3. Pluchinotta, I., Kazakçi, A.O., Giordano, R. et al. Design Theory for Generating Alternatives in Public Decision Making Processes. Group Decis Negot 28, 341–375 (2019). URL: <https://doi.org/10.1007/s10726-018-09610-5>.
4. Alsaig, A., Alsaig, A., Alagar, V. (2024). A Critical Review of Multi Criteria Decision Analysis Method for Decision Making and Prediction in Big Data Healthcare Applications. In: Huang, DS., Premaratne, P., Yuan, C. (eds) Applied Intelligence. ICAI 2023. Communications in Computer and Information Science, vol 2015. Springer, Singapore. URL: https://doi.org/10.1007/978-981-97-0827-7_8.
5. Werners, B., Zimmermann, H.J. (1989). Evaluation and Selection of Alternatives Considering Multiple Criteria. In: Jovanović, A.S., Kussmaul, K.F., Lucia, A.C., Bonissone, P.P. (eds) Expert Systems in Structural Safety Assessment. Lecture Notes in Engineering, vol 53. Springer, Berlin, Heidelberg. URL: https://doi.org/10.1007/978-3-642-83991-7_10.
6. Taherdoost, H.; Madanchian, M. (2023) Multi-Criteria Decision Making (MCDM) Methods and Concepts. Encyclopedia 2023, 3, 77-87. URL: <https://doi.org/10.3390/encyclopedia3010006>.

7. Erdogan, S.A.; Šaparauskas, J.; Turskis, Z. A Multi-Criteria Decision-Making Model to Choose the Best Option for Sustainable Construction Management. Sustainability 2019, 11, 2239. URL: <https://doi.org/10.3390/su11082239>.
 8. Anand J. (2022) Kulkarni Multiple Criteria Decision Making: Techniques, Analysis, and Applications. URL: <https://link.springer.com/book/10.1007/978-981-16-7414-3>.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.428.4

ИНТЕГРАЦИЯ КОНФИГУРАЦИЙ НА БАЗЕ «1С: ПРЕДПРИЯТИЕ» С ЦИФРОВЫМИ ПЛАТФОРМАМИ

¹Балашов О.В., ²Букачев Д.С., ³Суриков А.А.

¹АО «РАДИОЗАВОД», НИО-4, Смоленск, Россия, (214027, г. Смоленск, улица Котовского, 2), e-mail: smradio@mail.ru

ФГБОУ ВО «СМОЛЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Смоленск, Россия (214000, г. Смоленск, ул. Пржевальского, 4), e-mail: ²dsbuka@yandex.ru, ³sur114@yandex.ru

При разработке сложных систем учета и поддержки принятия решений всегда актуален вопрос интеграции с внешними информационными системами и цифровыми платформами. В данной статье рассматривается интеграция платформы «1С: Предприятие» с сервисами Московской биржи. В настоящее время на базе «1С: Предприятие» отсутствуют какие-либо открытые интеграционные решения для Московской биржи. В работе проанализированы основные интерфейсы API Московской биржи и создана демонстрационная конфигурация с модулем для интеграции с Мосбиржей на базе ISS-API. Полученные результаты могут быть применены при решении различных задач: от выгрузки данных для последующей аналитики до написания собственных торговых роботов.

Ключевые слова: Система учёта, цифровая платформа, интеграция, 1С: Предприятие, Московская биржа, API.

INTEGRATION OF CONFIGURATIONS BASED ON "1S: ENTERPRISE" WITH DIGITAL PLATFORMS

¹Balashov O.V., ²Bukachev D.S., ³Surikov A.A.

¹JOINT-STOCK COMPANY "RADIO FACTORY", RESEARCH DEPARTMENT 4, Russia, (214027, Smolensk, street Kotovskogo, 2), e-mail: smradio@mail.ru

²FEDERAL STATE EDUCATIONAL INSTITUTION OF HIGHER EDUCATION SMOLENSK STATE UNIVERSITY, Smolensk, Russia (214000, Smolensk, street Przewalski, 4), e-mail: dsbuka@yandex.ru, ³sur114@yandex.ru

When developing complex accounting and decision support systems, the issue of integration with external information systems and digital platforms is always relevant. This article considers the integration of the 1C: Enterprise platform with the services of the Moscow Exchange. Currently, there are no open integration solutions for the Moscow Exchange based on 1C: Enterprise. The paper analyzes the main API interfaces of the Moscow Exchange and creates a demonstration configuration with a module for integration with the Moscow Exchange on the basis of ISS-API. The results obtained can be applied in solving various tasks: from data unloading for further analytics to writing your own trading robots.

Keywords: Accounting system, digital platform, integration, 1C: Enterprise, Moscow Exchange, API.

«1С: Предприятие» – это мощная платформа для разработки прикладных решений в сфере бухучёта, торговли и документооборота. Большинство пользователей воспринимают её именно как платформу для управленцев и экономистов, поскольку на рынке представлено множество прикладных продуктов в этих сферах [1].

Однако сама по себе платформа «1С: Предприятие» – это универсальная среда разработки. Она позволяет реализовать любые задачи, которые можно реализовать с помощью

других языков программирования. Кроме того, наличие интегрированных средств автоматизации проектирования и разработки ПО существенно сокращает время на рутинные операции.

Как и любая другая среда, «1С: Предприятие» поддерживает механизмы взаимодействия с внешними системами. Это очень важно, поскольку таким образом появляется возможность разрабатывать прикладные решения, используя данные и мощности внешних систем или управляя ими, не покидая привычной системы учёта.

На сегодняшний день уже существуют решения для интеграции «1С: Предприятие» и популярных маркетплейсов: интеграция в той или иной степени присутствует в конфигурациях «1С: Розница», «1С: УНФ», «1С: Управление торговлей», «1С: Комплексная автоматизация», «1С: ERP» и «1С: Бухгалтерия», кроме того, существуют сторонние решения для интеграции [2, 3]. Это позволяет продавцам на маркетплейсах выгружать данные сразу в систему учёта и формировать отчетность. Однако для формирования ценовой политики организации, отслеживания экономических показателей, в том числе, влияющих на денежно-кредитную политику ЦБ РФ, для принятия управленческих решений требуется также интеграция системы учёта с цифровыми платформами, позволяющими управлять финансами, ценными бумагами и прочими активами.

На сегодняшний день основной платформой, занимающейся торговлей ценными бумагами в России, является ПАО «Московская биржа» [4]. Поэтому особый интерес вызывает возможность интеграции «1С: Предприятие» именно с Московской биржей. Результаты поисковых запросов показывают, что в настоящее время на базе «1С: Предприятие» отсутствуют какие-либо открытые интеграционные решения для Московской биржи.

Классический вариант интеграции с внешней системой – интеграция через API. API (Application Programming Interface – программный интерфейс приложения) – это набор способов и правил, по которым различные программы взаимодействуют между собой и обмениваются данными.

У Мосбиржи очень разветвленная и проработанная структура API [5] (Рисунок 1), поскольку с Мосбиржей взаимодействует большое количество торговых терминалов, интернет-ресурсов и аналитических платформ, например, MetaTrader, QUIK или Investing.com. Предлагается как платный высокоскоростной API (подойдёт для активной торговли с помощью роботов), так и бесплатный информационно-статистический API (ISS-API), который вполне пригоден для получения информации о стоимости валют или котировок ценных бумаг.

Interfaces

MOEX APIs to securely organize order messaging and market data flow.

Market Data API

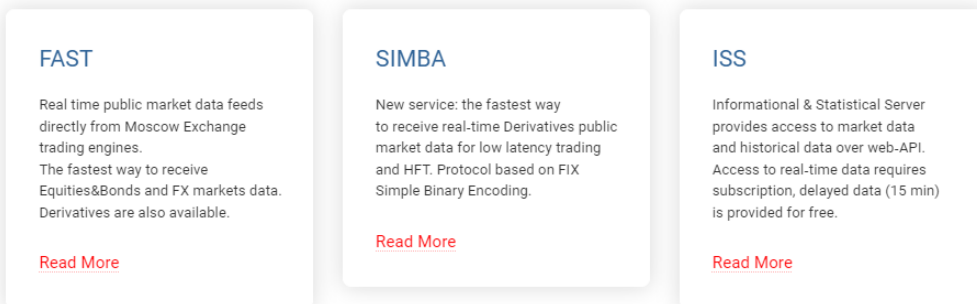


Рисунок 1 – Варианты интерфейсов API Московской биржи

Описание функционала API сопровождается примерами. Однако стоит отметить, что примеров кода на языке платформы «1С: Предприятие» на площадке Мосбиржи нет. Есть лишь примеры на языках Python и VB.NET [6].

Поскольку интеграция «1С: Предприятие» и Московской биржи представляет определенный интерес, но какие-либо значимые интеграционные решения для Московской биржи на сегодняшний день отсутствуют, задача адаптации и тестирования примеров использования ISS-API для «1С: Предприятие» является практически значимой.

На Рисунке 2 показано описание некоторых ISS-запросов [7].

[/iss/securities](#)

Список бумаг торгуемых на московской бирже.

[/iss/securities/{security}](#)

Получить спецификацию инструмента. Например: <https://iss.moex.com/iss/securities/IMOEX.xml>

[/iss/securities/{security}/indices](#)

Список индексов в которые входит бумага

[/iss/securities/{security}/aggregates](#)

Агрегированные итоги торгов за дату по рынкам

[/iss/index](#)

Получить глобальные справочники ISS. Например: <https://iss.moex.com/iss/index.xml>

Рисунок 2 – Варианты ISS-запросов к Мосбирже

Каждый ISS-API-запрос – это HTTP-запрос к серверу биржи, который можно отправить из любой программы, в том числе, и из «1С: Предприятие». На корректно составленный запрос сервер биржи вернет ответ установленного формата. Ответы на запросы могут быть сгенерированы в двух вариантах – в форматах JSON и XML. Оба формата используются для межпрограммного взаимодействия.

На Рисунке 3 показан результат выполнения запроса для получения котировок ценных бумаг в браузере с ответом в формате JSON:

```
{
  "marketdata": {
    "columns": ["SECID", "MARKETPRICE"],
    "data": [
      ["ABIO", 93.32],
      ["ABRD", 268.4],
      ["ACKO", null],
      ["AFKS", 23.722],
      ["AFLT", 61.65],
      ["AGRO", 1415.4],
      ["AKRN", 15604],
      ["ALRS", 71.46],
```

Рисунок 3 – Фрагмент ответа ISS-сервера Мосбиржи в формате JSON

На Рисунке 4 – результат выполнения того же запроса в браузере с ответом в формате XML:

```
<document>
  <data id="marketdata">
    <rows>
      <row SECID="ABIO" MARKETPRICE="93.32"/>
      <row SECID="ABRD" MARKETPRICE="268.4"/>
      <row SECID="ACKO" MARKETPRICE=""/>
      <row SECID="AFKS" MARKETPRICE="23.722"/>
      <row SECID="AFLT" MARKETPRICE="61.65"/>
      <row SECID="AGRO" MARKETPRICE="1415.4"/>
      <row SECID="AKRN" MARKETPRICE="15604"/>
      <row SECID="ALRS" MARKETPRICE="71.46"/>
```

Рисунок 4 – Фрагмент ответа ISS-сервера Мосбиржи в формате XML

Платформа «1С: Предприятие» содержит инструменты для парсинга данных из обоих форматов. Для определенности далее рассматриваются варианты с ответами в формате JSON.

В ходе исследования возможностей ISS-API языковыми средствами платформы «1С: Предприятие» был создан программный модуль для работы с Мосбиржей. Запрос к бирже оформлен в виде функции *ПолучитьЦены* (Рисунок 5).

```
Функция ПолучитьЦены() Экспорт
    ТЗ = Новый ТаблицаЗначений;
    ТЗ.Колонки.Добавить("Название", Новый ОписаниеТипов("Строка"));
    ТЗ.Колонки.Добавить("Цена", Новый ОписаниеТипов("Число"));
    Данные = Новый Массив;
    HTTPСоединение = Новый HTTPСоединение("iss.moex.com");
    Запрос = Новый HTTPЗапрос("/iss/engines/stock/markets/shares/boards/TQBR/" +
        "securities.json?iss.meta=off&iss.only=marketdata&" +
        "marketdata.columns=SECID,MARKETPRICE");
    Попытка
        Ответ = HTTPСоединение.Получить(Запрос);
        Если Ответ.КодСостояния = 200 Тогда
            Чтение = Новый ЧтениеJSON;
            Чтение.УстановитьСтроку(Ответ.ПолучитьТелоКакСтроку());
            Данные = ПрочитатьJSON(Чтение);
            Чтение.Закрыть();
            Для Каждого Элемент Из Данные.marketdata.data Цикл
                Стр = ТЗ.Добавить();
                Стр.Название = Элемент[0];
                Стр.Цена = Элемент[1];
            КонецЦикла;
        КонецЕсли;
    Искключение;
    КонецПопытки;

    Возврат ТЗ;
КонецФункции
```

Рисунок 5 – Листинг функции *ПолучитьЦены*

Порядок работы функции *ПолучитьЦены* следующий:

1. Создается таблица значений со столбцами *Название* и *Цена*.
2. Формируется запрос к серверу биржи.
3. Осуществляется попытка получить ответ на запрос.
4. Если не возникло ошибки, читаются данные JSON-структуры.
5. Просматривается массив значений и построчно заполняется ранее созданная таблица значений.

Для фильтрации ценных бумаг по тикеру была создана ещё одна функция – *ПолучитьЦенуПоТикеру*. Она получает таблицу значений, используя функцию *ПолучитьЦены*, после чего ищет в таблице нужный тикер и, если находит, возвращает стоимость ценной бумаги (Рисунок 6).

```
Функция ПолучитьЦенуПоТикеру(Тикер) Экспорт
    Цены = ПолучитьЦены();
    НайденнаяСтрока = Цены.Найти(Тикер, "Название");
    Если НайденнаяСтрока <> Неопределено Тогда
        Возврат(НайденнаяСтрока.Цена);
    Иначе
        Возврат(-1);
    КонецЕсли;
КонецФункции
```

Рисунок 6 – Листинг функции *ПолучитьЦенуПоТикеру*

Для тестирования механизма взаимодействия с сервером биржи был создан справочник *ЦенныеБумаги*, содержащий конкретные наименования ценных бумаг и их тикеры. Для вывода результатов взаимодействия был создан отчет *КотировкиЦБ*. При создании отчета использовалась схема компоновки данных на базе запроса к справочнику *ЦенныеБумаги* с вычисляемым полем, которое определяется как результат выполнения функции

Получить Цену По Тикеру от тикера в текущей строке отчета. Результат формирования отчета Котировки ЦБ показан на Рисунке 7:



Наименование	Тикер	Цена
Сбербанк	SBER	327,93
Газпром	GAZP	118,31
Норильский Никель	GMKN	130,08
Лукойл	LKOH	7 241,50
Яндекс	YNDX	4 090,00

Рисунок 7 – Результат формирования отчета *Котировки ЦБ*

При формировании отчета для каждой строки по тикеру определилась цена. Поскольку источник данных для отчета – это справочник *Ценные Бумаги*, в отчет попали только те бумаги, которые присутствуют в справочнике.

Таким образом, используя API Мосбиржи, удалось создать простой и наглядный пример интеграции «1С: Предприятие» с такой мощной внешней цифровой платформой, как Московская биржа. Способов применения такой интеграции – много: от выгрузки данных для последующей аналитики до написания собственных торговых роботов.

Список литературы

1. Программные продукты фирмы «1С». URL: <https://1c.ru/rus/products/products.htm>. (дата обращения...)
2. RDV Маркет. Интеграция 1С с маркетплейсами URL: <https://rdv-market.ru>.
3. ИнфоСофт. Управление маркетплейсами на 1С. URL: <https://marketplace.is1c.ru>.
4. Московская биржа. URL: <https://www.moex.com>.
5. Интерфейсы API Московской биржи. URL: <https://www.moex.com/a7939>
6. Примеры использования ISS API на Python и VB.NET. URL: <https://www.moex.com/a2920>.
7. Официальное описание методов ISS-API Московской биржи. URL: <https://iss.moex.com/iss/reference/?lang=ru>.

References

1. Programmnye produkty firmy «1S». URL: <https://1c.ru/rus/products/products.htm>.
 2. RDV Market. Integraciya 1S s marketplejsami URL: <https://rdv-market.ru>.
 3. nfoSoft. Upravlenie marketplejsami na 1S. URL: <https://marketplace.is1c.ru>.
 4. Moskovskaya birzha. URL: <https://www.moex.com>.
 5. Interfejsy API Moskovskoj birzhi. URL: <https://www.moex.com/a7939>
 6. Primery ispol'zovaniya ISS API na Python i VB.NET. URL: <https://www.moex.com/a2920>.
 7. Oficial'noe opisanie metodov ISS-API Moskovskoj birzhi. URL: <https://iss.moex.com/iss/reference/?lang=ru>.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056.55

КРИТИЧЕСКАЯ УЯЗВИМОСТЬ - CVE-2023-27350

Авдалян А.А.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
sharmanka228@gmail.com

В данной статье рассматривается уязвимость CVE-2023-27350, обнаруженная в приложении PaperCut NG/MF, широко используемом для управления процессами печати в крупных организациях. Особое внимание уделяется резкому росту числа атак, связанных с этой уязвимостью, что обусловлено её характером как zero-click эксплойта, не требующего взаимодействия пользователя и позволяющего полностью автоматизировать доставку вредоносного ПО. В статье подробно объясняется механизм уязвимости, показаны методы её эксплуатации, предлагаются стратегии защиты, а также подчеркивается важность соблюдения принципов безопасности, включая необходимость тщательной очистки после установки программного обеспечения.

Ключевые слова: CVE-2023-27350, zero-click эксплойт, автоматизация, доставка вредоносного ПО, защита, очистка после установки, уязвимость, безопасность.

CRITICAL VULNERABILITY - CVE-2023-27350

Avdalyan A.A.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: sharmanka228@gmail.com

This article examines the vulnerability CVE-2023-27350, discovered in the PaperCut NG/MF application, widely used to manage printing processes in large organizations. Particular attention is paid to the sharp increase in the number of attacks related to this vulnerability, due to its nature as a zero-click exploit that does not require user interaction and allows for fully automated malware delivery. The article explains in detail the mechanism of the vulnerability, shows methods of its exploitation, suggests protection strategies, and emphasizes the importance of following security principles, including the need for thorough cleaning after installing software.

Keywords: CVE-2023-27350, zero-click exploit, automation, malware delivery, protection, post-installation cleanup, vulnerability, security.

Введение

8 марта 2023 года был выпущен патч для уязвимости CVE-2023-27350, которая обнаружена в приложении PaperCut NG/MF — веб-ориентированном программном обеспечении, используемом крупными организациями для управления процессами печати. Уязвимость позволяет злоумышленникам удаленно получить административный доступ к веб-приложению и использовать легитимную функциональность скриптов для выполнения кода на сервере с правами SYSTEM.

Однако, в последующие месяцы была зафиксирована активная эксплуатация этой уязвимости в дикой природе. Количество атак увеличивается, включая доставку вредоносного ПО с использованием C2-фреймворков, таких как CobaltStrike, и даже программ-вымогателей.

Среди групп, стоящих за активной эксплуатацией, фигурируют известные АРТ-группы, включая C10p.

Стремительное увеличение числа атак, связанных с уязвимостью CVE-2023-27350, вызвано её природой как zero-click эксплойта, не требующего взаимодействия пользователя. Этот тип уязвимости позволяет злоумышленникам полностью автоматизировать процесс доставки вредоносного ПО на уязвимые системы. В данном руководстве мы подробно разберем природу этой уязвимости, продемонстрируем её возможные методы эксплуатации, предложим меры защиты и обсудим основополагающий принцип безопасности, напомнивший нам об актуальности темы — необходимость тщательной очистки после установки программного обеспечения.

Paper cut

PaperCut — это популярное программное обеспечение для управления печатью, которое используется организациями по всему миру для контроля и управления услугами печати и копирования. В линейке продуктов PaperCut предлагаются два схожих решения, размещаемых на собственных серверах:

PaperCut NG — решение для управления и контроля процессов печати.

PaperCut MF — аналогичный продукт, но с расширенными функциями копирования и сканирования[2].

Компания PaperCut объявила, что не обновленные серверы MF и NG активно подвергаются атакам, так как они уязвимы к обходу аутентификации, описанному ниже.

CVE-2023-27350

Инициатива Zero Day (ZDI-23-233) описывает CVE-2023-27350 как уязвимость, которая позволяет неаутентифицированному удаленному злоумышленнику выполнить произвольный код и скомпрометировать сервер приложения PaperCut. Эта уязвимость также напрямую связана с CVE-2023-27351, которая, используя ту же самую уязвимость, описанную ниже, позволяет злоумышленнику извлекать информацию (имена пользователей, электронные почты и хэши паролей) из базы данных пользователей, хранящейся в PaperCut[5].

Эта уязвимость имеет два аспекта и изначально возникает из-за уязвимости обхода аутентификации. Это позволяет неаутентифицированному удаленному злоумышленнику обойти страницу входа и получить административный доступ к консоли PaperCut, просто сделав запрос к URL, который изначально использовался в процессе установки приложения.

Этот запрос инициирует класс SetupCompleted, который, как показано в приведенном ниже блоке кода, включает вызов метода Java performLogin(), передавая аргумент Admin в качестве параметра LoginType.

Приложение обычно вызывает эту функцию только после того, как пользователь успешно прошел проверку в процессе обычного входа в систему. Однако в данном случае присутствует уязвимость типа Session Puzzling в классе SetupCompleted — логическая уязвимость, возникающая, когда функции сессии и аутентификации используются для разных целей. Эксплуатируя эту уязвимость, приложение ошибочно подтверждает сессию администратора для неаутентифицированного пользователя.

Этот обход аутентификации приводит к удаленному выполнению кода путем злоупотребления встроенной функцией "скриптинга" в консоли администратора. Если уязвимость будет использована, злоумышленник может вставить произвольный JavaScript в

скрипт шаблона печати. Отключение параметра конфигурации песочницы дает скриптам прямой доступ к среде выполнения Java, что позволяет выполнить произвольный код. Код может быть выполнен по требованию, просто сохранив скрипт[4]. Таким образом, простое редактирование скрипта может привести к удаленному выполнению кода.

Ситуацию усугубляет то, что выполненные скрипты работают в контексте службы PrintCut, которая, в свою очередь, выполняется с полными привилегиями учетной записи NT AUTHORITY\SYSTEM в Windows (или учетной записи root в Linux). Таким образом, использование этой уязвимости предоставляет ранее неаутентифицированному злоумышленнику полный контроль над хостом[1]!

Влияние

Серьезность уязвимости CVE-2023-27350 проявилась в многочисленных случаях её активной эксплуатации злоумышленниками, которые использовали её для автоматизированных атак на целевые системы. После публикации PoC-эксплойта исследователи отметили массовые атаки на уязвимые серверы по всему миру, особенно в образовательном секторе, с участием таких группировок, как C10p. Поиск в Shodan в апреле 2023 года показал около 1 700 серверов PaperCut, доступных через интернет, что делает их привлекательными для атак. Злоумышленники также использовали легитимные инструменты ИТ-специалистов и такие угрозы, как Truebot, Buhtiransom, Mirai и майнеры криптовалют[3].

Заключение

В этой статье мы рассказали, насколько легко использовать уязвимость обхода аутентификации в PaperCut и злоупотребить функцией скриптов для достижения удаленного выполнения кода. Стоит отметить, что поскольку выполнение кода происходит через легитимную функцию, даже если вы установили патч для этой уязвимости, злоумышленники все равно могут воспользоваться ею, если вы настроили слабый пароль в приложении.

Список литературы

1. Гельфанд А. М. Способы выбора стежоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262
2. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.
3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348
5. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.

References

1. Gelfand A.M. Methods of choosing stegocontainers for data transmission //Regional informatics and information security. - 2020. – pp. 260-262
 2. Kushnir D. V. Research and development of methods for distributing confidential data via quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.
 3. Lesnova E. M., Pestov I. E. Development of a method for detecting and correcting errors for a distributed information network based on big data //Regional informatics and information security. - 2018. – pp. 236-240.
 4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348
 5. Petrova T. V. et al. Approaches for detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056.55

SNYK CODE: КАК ЗАЩИТИТЬ КОД ОТ УЯЗВИМОСТЕЙ

Авдалян А.А.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: sharmanka228@gmail.com

Статья "Snyk Code" представляет собой обзор и анализ решений по обеспечению безопасности кода, предлагаемых платформой Snyk. В статье рассматриваются ключевые возможности и функции Snyk Code, включая его способность выявлять уязвимости, анализировать зависимые библиотеки и интегрироваться с различными системами CI/CD. Особое внимание уделяется методам автоматического обнаружения и исправления уязвимостей на этапе разработки, а также практическому применению платформы в различных сценариях программирования. Статья также обсуждает преимущества использования Snyk Code для повышения надежности и безопасности программного обеспечения, а также его влияние на общий процесс разработки.

Ключевые слова: Snyk Code, безопасность кода, уязвимости, анализ зависимостей, CI/CD, автоматическое исправление, разработка программного обеспечения, платформы безопасности.

SNYK CODE: HOW TO PROTECT YOUR CODE FROM VULNERABILITIES

Avdalyan A.A.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: sharmanka228@gmail.com

The article "Snyk Code" is an overview and analysis of code security solutions offered by the Snyk platform. The article discusses the key features and functions of Snyk Code, including its ability to identify vulnerabilities, analyze dependent libraries, and integrate with various CI/CD systems. Special attention is paid to the methods of automatic detection and correction of vulnerabilities at the development stage, as well as the practical application of the platform in various programming scenarios. The article also discusses the benefits of using Snyk Code to improve the reliability and security of software, as well as its impact on the overall development process.

Keywords: Snyk Code, code security, vulnerabilities, dependency analysis, CI/CD, automatic correction, software development, security platforms.

Введение

В эпоху стремительного роста числа угроз безопасности программного обеспечения и увеличения сложности современных приложений, обеспечение защиты кода становится одной из важнейших задач для разработчиков. Одним из инструментов, предоставляющих эффективные решения в этой области, является Snyk Code. Эта платформа специально разработана для выявления уязвимостей в исходном коде и зависимостях на ранних стадиях разработки, что позволяет минимизировать риски и улучшить безопасность приложений.

Snyk Code предлагает интегрированные инструменты для анализа кода, которые автоматизируют процесс обнаружения уязвимостей и предоставляют рекомендации по их устранению. Использование таких решений особенно важно в условиях современных циклов

разработки программного обеспечения, где быстрая интеграция и тестирование кода являются ключевыми факторами успеха[1].

В данном контексте, статья направлена на глубокий анализ возможностей и особенностей Snyk Code, а также его роли в поддержке безопасной разработки программного обеспечения. Мы рассмотрим, как Snyk Code справляется с задачей обнаружения уязвимостей, интеграции с системами CI/CD, и как его использование может повлиять на общий процесс разработки и безопасность программных продуктов.

Snyk Code: Обеспечение безопасности кода на каждом этапе разработки

Обзор Snyk Code

Snyk Code — это передовая платформа для анализа и защиты исходного кода, разработанная для помощи разработчикам в выявлении и устранении уязвимостей на ранних стадиях разработки. Платформа интегрируется с различными средами разработки и системами CI/CD, обеспечивая непрерывный мониторинг кода на предмет потенциальных угроз безопасности[3].

Основные функции и возможности

Snyk Code предлагает ряд ключевых функций, способствующих улучшению безопасности кода:

Статический анализ кода: Платформа проводит глубокий статический анализ кода, выявляя потенциальные уязвимости и ошибки еще до выполнения программы. Это позволяет разработчикам оперативно устранять проблемы на ранних стадиях[4].

Анализ зависимостей: Snyk Code также анализирует сторонние библиотеки и зависимости, используемые в проекте. Это важно, поскольку уязвимости в зависимостях могут стать точками входа для атак.

Интеграция с CI/CD: Платформа легко интегрируется с популярными системами непрерывной интеграции и доставки (CI/CD), такими как Jenkins, GitHub Actions и GitLab CI. Это обеспечивает автоматическое сканирование кода и зависимостей на каждом этапе разработки и развертывания.

Интерактивные рекомендации: Snyk Code предоставляет детализированные рекомендации по исправлению уязвимостей, что позволяет разработчикам легко понять и устранить найденные проблемы[2].

Обратная связь в реальном времени: Платформа обеспечивает обратную связь в реальном времени, что позволяет разработчикам немедленно реагировать на обнаруженные уязвимости и интегрировать исправления в кодовую базу.

Преимущества использования Snyk Code

Использование Snyk Code приносит множество преимуществ:

Улучшение безопасности: Постоянный анализ кода и зависимостей помогает предотвратить внедрение уязвимостей в конечный продукт, тем самым повышая общий уровень безопасности приложения.

Сокращение времени на исправление: Благодаря детализированным рекомендациям по исправлению и автоматизированному анализу, разработчики могут быстрее исправлять уязвимости, минимизируя время, затрачиваемое на безопасность.

Снижение рисков: Проактивное обнаружение и устранение уязвимостей снижает риск потенциальных атак и утечек данных, что особенно важно для соблюдения стандартов безопасности и требований нормативных актов.

Интеграция в рабочий процесс: Интеграция Snyk Code с системами CI/CD позволяет seamlessly интегрировать анализ кода в процесс разработки, что делает его частью повседневной работы команды разработчиков.

Практическое применение и примеры

Рассмотрим несколько сценариев, в которых Snyk Code может быть полезен:

Проекты с открытым исходным кодом: В проектах с открытым исходным кодом, где разработчики часто работают с внешними зависимостями, Snyk Code помогает обнаруживать уязвимости в этих зависимостях и своевременно их устранять.

Корпоративные приложения: Для крупных компаний, где безопасность данных критична, Snyk Code обеспечивает постоянный контроль над безопасностью кода, снижая риски утечек и атак[5].

Мобильные и веб-приложения: Разработчики мобильных и веб-приложений могут использовать Snyk Code для анализа как клиентской, так и серверной части приложений, обеспечивая комплексную защиту.

Заключение

Snyk Code представляет собой мощный инструмент для обеспечения безопасности кода, предлагая ряд функций, которые помогают разработчикам своевременно обнаруживать и устранять уязвимости. Его интеграция с системами CI/CD и возможность анализа как исходного кода, так и зависимостей делают его незаменимым в современном процессе разработки программного обеспечения. Использование Snyk Code способствует не только улучшению безопасности приложений, но и оптимизации процессов разработки, что в конечном итоге позволяет создавать более надежные и защищенные программные продукты.

Список литературы

1. Бударный Г. С. и др. Исследование концепции ядра в различных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 411-417.
2. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
3. Шемякин С. Н. и др. Оценка расстояния единственности... Для некоторых блочных шифров //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 34-38.
4. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76.
5. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.

References

1. Budarny G. S. et al. Research of the kernel concept in various operating systems //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 411-417.
 2. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348.
 3. Shemyakin S. N. et al. Estimation of the uniqueness distance... For some block ciphers //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 34-38.
 4. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 4. – pp. 72-76.
 5. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch-Bruевич, 1996.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

ЮРИДИЧЕСКИЕ АСПЕКТЫ В DFIR

Авдалян А.А.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
sharmanka228@gmail.com

Статья "Legal Considerations in DFIR" предоставляет всесторонний обзор юридических аспектов, связанных с цифровыми форензическими расследованиями и реагированием на инциденты (DFIR). В работе рассматриваются ключевые правовые вопросы, которые могут возникнуть в процессе сбора, анализа и представления доказательств в цифровых расследованиях. В статье освещаются важные темы, такие как соблюдение законодательства о конфиденциальности данных, соблюдение правил допустимости доказательств в суде и взаимодействие с правоохранительными органами. Автор также обсуждает юридические риски и рекомендации по минимизации правовых последствий, а также предоставляет практические советы для профессионалов в области DFIR.

Ключевые слова: Цифровая форензика, реагирование на инциденты, юридические аспекты, конфиденциальность данных, допустимость доказательств, правоохранительные органы, правовые риски, минимизация последствий, расследование, правовая ответственность.

LEGAL ASPECTS IN DFIR

Avdalyan A.A.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: sharmanka228@gmail.com

The article "Legal Considerations in DFIR" provides a comprehensive overview of the legal aspects related to digital forensic investigations and Incident Response (DFIR). The paper examines the key legal issues that may arise in the process of collecting, analyzing and presenting evidence in digital investigations. The article highlights important topics such as compliance with data privacy laws, compliance with the rules of admissibility of evidence in court and interaction with law enforcement agencies. The author also discusses legal risks and recommendations for minimizing legal consequences, as well as provides practical advice for professionals in the field of DFIR.

Keywords: Digital forensics, incident response, legal aspects, data confidentiality, admissibility of evidence, law enforcement agencies, legal risks, minimization of consequences, investigation, legal responsibility.

Введение

В эпоху цифровых технологий и повсеместного использования информационных систем, вопросы цифровой безопасности и реагирования на инциденты (DFIR) приобрели особую значимость. Успешное проведение цифровых форензических расследований требует не только высокой квалификации в области технологий и методов сбора данных, но и глубокого понимания юридических аспектов, которые могут существенно повлиять на исход расследования и его правовые последствия.

Цифровая форензика занимается анализом электронных данных с целью выявления и документирования доказательств преступной деятельности или нарушения политики

безопасности. Однако, сбор и обработка таких данных требуют соблюдения строгих юридических норм и процедур, чтобы доказательства могли быть использованы в суде и не были признаны недопустимыми. Неправильное обращение с данными может привести к их порче, а также к юридическим последствиям, таким как санкции и репутационные потери.

Законодательство в области цифровой форензики постоянно эволюционирует, что требует от специалистов постоянного обновления знаний о правовых нормах, касающихся конфиденциальности данных, защиты личной информации и допустимости доказательств. Важными аспектами являются соблюдение требований по получению ордеров на обыск, правомерность доступа к данным и их анализ, а также соблюдение норм законодательства о защите данных, таких как Общий регламент по защите данных (GDPR) в Европе или Закон о защите персональных данных (ССРА) в США[2].

Данная статья нацелена на предоставление комплексного анализа юридических вопросов, связанных с DFIR, с акцентом на практические аспекты и рекомендации для профессионалов в этой области. Мы рассмотрим ключевые правовые принципы и практики, которые помогут избежать распространенных юридических ошибок и обеспечат успешное разрешение цифровых расследований.

Legal Considerations in DFIR

Законодательные основы и права доступа

Современные цифровые форензические расследования требуют строгого соблюдения законодательных норм, касающихся сбора и обработки данных. В различных юрисдикциях существуют законы, регулирующие доступ к цифровой информации и способы её получения. Например, в США часто используются ордера на обыск, которые дают правообладателям право доступа к электронным данным. В Европе правила, такие как Общий регламент по защите данных (GDPR), устанавливают ограничения на сбор и обработку персональной информации. Специалисты в области DFIR должны четко понимать и соблюдать эти нормы, чтобы избежать правовых последствий и обеспечить допустимость собранных доказательств в суде[3].

Принципы допустимости доказательств

Одним из ключевых аспектов в цифровых расследованиях является допустимость доказательств. Для того чтобы доказательства были признаны судом, они должны быть собраны и обработаны в соответствии с законами и стандартами. Это включает в себя обеспечение целостности данных, правильное документирование всех шагов процесса и соблюдение цепочки хранения доказательств. Профессионалы в области DFIR должны применять надлежащие методы для защиты доказательств от модификаций и утрат, чтобы сохранить их достоверность и обеспечить их принятие в суде.

Конфиденциальность и защита данных

Конфиденциальность данных является важным аспектом, требующим внимания в процессе цифровых расследований. Законодательства, такие как GDPR в Европе и Закон о защите персональных данных (ССРА) в США, обязывают организации обеспечивать защиту личной информации и уведомлять пользователей о сборе и обработке их данных. Специалисты в области DFIR должны гарантировать, что сбор данных осуществляется в рамках закона и что личная информация защищена от несанкционированного доступа.

Нарушение норм конфиденциальности может привести к значительным штрафам и юридическим последствиям[1].

Взаимодействие с правоохранительными органами

Правильное взаимодействие с правоохранительными органами имеет решающее значение для успешного проведения цифровых расследований. Специалисты должны быть готовы к сотрудничеству с правоохранительными органами, предоставляя им необходимые данные и документы в установленном формате. Это взаимодействие должно осуществляться в рамках правового поля и с соблюдением всех процессуальных норм. Также важно документировать все взаимодействия и обмен информацией с правоохранительными органами для обеспечения прозрачности и последующей проверки.

Примеры юридических рисков и решений

Примеры юридических рисков в DFIR включают неправильное обращение с данными, недостаточную документацию и нарушение конфиденциальности. Например, случай из практики, когда доказательства были признаны недопустимыми из-за недостаточной цепочки хранения, демонстрирует важность соблюдения всех требований. Для минимизации рисков рекомендуется внедрение четких процедур для сбора и обработки данных, регулярное обучение сотрудников и консультации с юридическими экспертами[4].

Рекомендации по соблюдению законодательства

Чтобы избежать юридических рисков и обеспечить успешное проведение цифровых расследований, следует придерживаться ряда рекомендаций. Во-первых, необходимо всегда получать соответствующие ордера и разрешения для доступа к данным. Во-вторых, важно обеспечить полное и точное документирование всех этапов расследования. В-третьих, следует регулярно обновлять свои знания о текущих изменениях в законодательстве и стандартах защиты данных. Также полезно иметь юридического консультанта для проверки и подтверждения соблюдения всех правовых требований[5].

Заключение

Правильное понимание и соблюдение юридических аспектов цифровых форензических расследований (DFIR) играют ключевую роль в обеспечении успешного и законного проведения расследований. Учет законодательных требований, связанных с доступом к данным, допустимостью доказательств и защитой конфиденциальности информации, а также грамотное взаимодействие с правоохранительными органами способствуют минимизации правовых рисков и укреплению доверия к результатам расследований. Для достижения наилучших результатов специалистам в области DFIR рекомендуется регулярно обновлять свои знания о правовых нормах и внедрять передовые практики, что поможет гарантировать соответствие законодательным требованиям и обеспечить надежность собранных доказательств.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.

2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.
4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

References

1. . Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in Earth space research. – 2020. – Vol. 12. – No. 1. - pp. 70-76.
 2. Minyaev A. A. Method for evaluating the effectiveness of an information protection system geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
 3. Chmutov M. V. et al. A study of the current IT infrastructure of an organization for the subsequent transition to a cloud architecture //Information security of the regions of Russia (IBRD-2017). Conference proceedings. – 2017. – pp. 535-537.
 4. Petrova T. V. et al. Approaches for detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
 5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to the classification of texts by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

МЕТОДЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ АТАК НА МОБИЛЬНЫЕ УСТРОЙСТВА

Гаджиев Г.К.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: gugac134@gmail.com

В статье рассматриваются основные методы защиты мобильных устройств от киберугроз. Включены такие меры, как использование антивирусного ПО, регулярные обновления ОС и приложений, VPN, многофакторная аутентификация, проверка прав доступа приложений и обучение пользователей. Также описаны современные подходы, включая ИИ и машинное обучение, мониторинг сетевой активности, сетевая сегментация и обновление политик безопасности. Применение этих методов обеспечивает комплексную защиту данных и личной информации на мобильных устройствах.

Ключевые слова: Киберугрозы, мобильные устройства, безопасность, антивирус, VPN, многофакторная аутентификация, ИИ, машинное обучение.

METHODS FOR DETECTING AND PREVENTING ATTACKS ON MOBILE DEVICES

Gadzhiev G.K.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: gugac134@gmail.com

The article discusses the main methods of protecting mobile devices from cyber threats. Measures included include the use of antivirus software, regular OS and application updates, VPN, multi-factor authentication, checking application permissions and user training. Modern approaches are also described, including AI and machine learning, network activity monitoring, network segmentation, and updating security policies. The use of these methods provides comprehensive protection of data and personal information on mobile devices.

Keywords: Cyber threats, mobile devices, security, antivirus, VPN, multi-factor authentication, AI, machine learning.

Введение

С развитием технологий и расширением возможностей мобильных устройств увеличивается их уязвимость перед различными видами кибератак. В настоящее время мобильные устройства становятся основными средствами доступа к информации и проведения финансовых операций, что привлекает внимание киберпреступников. Для защиты данных и личной информации на мобильных устройствах разрабатываются различные методы обнаружения и предотвращения атак. В данной статье рассмотрим основные методы защиты мобильных устройств от киберугроз.

Использование антивирусного программного обеспечения

Один из наиболее распространенных методов защиты мобильных устройств - использование антивирусного программного обеспечения. Антивирусные приложения сканируют файлы и приложения на устройстве на предмет вредоносных программ и вирусов. Они также могут предотвращать установку вредоносного программного обеспечения, контролируя доступ к недоверенным сайтам и блокируя подозрительные ссылки.

Регулярное обновление операционной системы и приложений на мобильных устройствах является одним из наиболее важных методов защиты от киберугроз. Производители операционных систем и разработчики приложений регулярно выпускают обновления, в которых исправляют обнаруженные уязвимости и улучшают безопасность системы. Пользователи должны следить за обновлениями и устанавливать их как можно скорее.[1]

Виртуальные частные сети (VPN) обеспечивают шифрование интернет-соединения и защиту данных от перехвата. При использовании VPN данные, передаваемые между мобильным устройством и удаленным сервером, защищены от кибератак и прослушивания третьими лицами. VPN также позволяют обходить блокировки и ограничения доступа к интернет-ресурсам.

При установке новых приложений на мобильное устройство необходимо внимательно изучать запросы на предоставление различных прав доступа. Некоторые приложения могут запрашивать излишние или ненужные права, которые могут быть использованы для получения доступа к личной информации или выполнения вредоносных действий. Пользователи должны быть осмотрительны и отказывать в предоставлении прав, если это кажется им подозрительным.[2]

Многофакторная аутентификация - это метод защиты, при котором для доступа к устройству или приложению требуется не только пароль или пин-код, но и дополнительный фактор аутентификации, такой как отпечаток пальца, голосовое распознавание или код, отправленный на зарегистрированный телефон или электронную почту. Этот метод повышает безопасность доступа к устройству и защищает от несанкционированного доступа.

Важной составляющей безопасности мобильных устройств является обучение пользователей основам кибербезопасности и правилам безопасного поведения в сети. Пользователи должны быть осведомлены о возможных угрозах и уметь распознавать подозрительные признаки, такие как фишинговые письма, вредоносные ссылки и приложения. Обучение пользователей помогает снизить риск успешной атаки и повышает общий уровень безопасности мобильных устройств.

Для обнаружения аномального поведения и потенциальных угроз мобильной безопасности может быть полезным внедрение систем мониторинга сетевой активности на мобильных устройствах. Эти системы могут анализировать сетевой трафик и обнаруживать необычные или подозрительные активности, такие как попытки взлома, атаки перехвата данных или внедрение вредоносного программного обеспечения.

Современные системы безопасности все чаще используют методы искусственного интеллекта (ИИ) и машинного обучения (МО) для обнаружения и предотвращения кибератак на мобильные устройства. [3] Эти технологии могут анализировать большие объемы данных и выявлять аномалии, которые могут указывать на наличие угрозы безопасности. Например, системы ИИ и МО могут обнаруживать необычные попытки доступа к устройству, аномальные сетевые запросы или атаки фишингом.

Разработка и развертывание защищенных мобильных приложений является важным аспектом обеспечения безопасности мобильных устройств. Разработчики должны следовать передовым практикам безопасности программного обеспечения, таким как использование шифрования данных, проверка входных данных на предмет уязвимостей и регулярные аудиты безопасности приложений.[4]

Сетевая сегментация может помочь уменьшить потенциальные угрозы безопасности, разделяя сеть на отдельные сегменты и ограничивая доступ к чувствительным данным и ресурсам. Это позволяет изолировать потенциально компрометированные устройства от остальной части сети и предотвращать распространение атак на мобильные устройства на другие участки сети.

Регулярное обновление политик безопасности и процедур является важным аспектом обеспечения безопасности мобильных устройств. Организации должны периодически пересматривать свои политики и процедуры безопасности, учитывая новые угрозы и технологии. [5] Это позволит адаптироваться к изменяющейся угрозой среде и улучшить защиту мобильных устройств.

Заключение

Обеспечение безопасности мобильных устройств является важной задачей в условиях роста числа киберугроз и увеличения объема цифровой активности. Для защиты данных и личной информации на мобильных устройствах используются различные методы обнаружения и предотвращения атак, такие как использование антивирусного программного обеспечения, регулярное обновление операционной системы и приложений, использование VPN, проверка прав доступа приложений, многофакторная аутентификация и обучение пользователей. Комплексное применение этих методов позволяет обеспечить надежную защиту мобильных устройств от киберугроз и повысить уровень безопасности в целом.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
2. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.
3. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.
4. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018. – С. 149-149.
5. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 266-270.

References

1. Volkogonov V. N., Gelfand A.M., Derevyanko V. S. Relevance of automated control systems //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 262-266.
 2. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. - 2018. – No. 8. – pp. 91-97.
 3. Orlov G. A., Krasov A.V., Gelfand A.M. Application of Big Data in the analysis of big data in computer networks //High-tech technologies in space exploration of the Earth. – 2020. – Vol. 12. – No. 4. – pp. 76-84.
 4. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics "RI-2018". – 2018. – pp. 149-149.
 5. Volkogonov V. N., Gelfand A.M., Karamova M. R. Ensuring the security of personal data during their processing in personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 266-270
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

РАЗВИТИЕ ТЕХНОЛОГИЙ КВАНТОВОЙ КРИПТОГРАФИИ И ИХ РОЛЬ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гаджиев Г.К.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
gugac134@gmail.com

Введение квантовой криптографии представляет собой революционное направление в области информационной безопасности, особенно актуальное в свете развития квантовых компьютеров и растущих вычислительных угроз. Квантовая криптография, основываясь на принципах квантовой механики, предлагает непревзойденные уровни защиты данных за счет использования квантовых свойств частиц. В статье рассматриваются ключевые принципы квантовой криптографии, включая принцип неделимости квантового состояния, квантовую телепортацию и квантовое шифрование. Основные преимущества квантовой криптографии, такие как абсолютная безопасность, невозможность подслушивания и высокая скорость передачи данных, обсуждаются наряду с вызовами, включая техническую сложность и ограничения на расстояние передачи. Перспективы применения квантовой криптографии обширны и охватывают защиту критической инфраструктуры, медицинских данных, финансовых транзакций и облачных вычислений. Статья подчеркивает, что несмотря на существующие вызовы, квантовая криптография имеет потенциал стать фундаментом будущих систем информационной безопасности, обеспечивая надежную защиту данных в цифровом мире.

Ключевые слова: Квантовая криптография, информационная безопасность, квантовые компьютеры, квантовая телепортация, квантовое шифрование.

DEVELOPMENT OF QUANTUM CRYPTOGRAPHY TECHNOLOGIES AND THEIR ROLE IN ENSURING INFORMATION SECURITY

Gadzhiev G.K.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: gugac134@gmail.com

The introduction of quantum cryptography represents a revolutionary direction in the field of information security, especially relevant in light of the development of quantum computers and growing computing threats. Quantum cryptography, based on the principles of quantum mechanics, offers unmatched levels of data security by exploiting the quantum properties of particles. The article discusses the key principles of quantum cryptography, including the principle of indivisibility of a quantum state, quantum teleportation and quantum encryption. The main advantages of quantum cryptography, such as absolute security, the impossibility of eavesdropping, and high data transfer rates, are discussed along with the challenges, including technical complexity and limitations on transmission distance. The application prospects for quantum cryptography are broad and span the protection of critical infrastructure, medical data, financial transactions and cloud computing. The article emphasizes that despite existing challenges, quantum cryptography has the potential to become the foundation of future information security systems, providing reliable data protection in the digital world.

Keywords: Quantum cryptography, information security, quantum computers, quantum teleportation, quantum encryption.

Введение

С развитием цифровых технологий и распространением интернета возросла значимость вопросов информационной безопасности. Современные методы шифрования, основанные на классической криптографии, сталкиваются с угрозами со стороны вычислительных атак и развития квантовых компьютеров. В этой связи разработка и применение квантовой криптографии становится все более актуальной задачей.

Основные принципы квантовой криптографии

Квантовая криптография основана на использовании квантовых свойств физических объектов, таких как фотоны, для обмена и защиты информации. Основные принципы квантовой криптографии включают:

Согласно этому принципу, нельзя скопировать или измерить квантовое состояние без его разрушения. Это обеспечивает безопасность передачи информации, так как любая попытка перехвата или прослушивания сигнала приведет к изменению его состояния и обнаружению подслушивателя.[1]

Этот принцип позволяет передавать информацию между двумя точками без физической передачи частиц. Вместо этого используется перенос квантового состояния между двумя удаленными точками, что обеспечивает безопасную передачу информации.

Этот принцип заключается в использовании квантовых свойств для создания криптографических ключей и шифрования данных. Это позволяет создавать абсолютно безопасные системы шифрования, которые невозможно взломать с помощью классических методов.

Квантовая криптография обладает рядом преимуществ, которые делают ее привлекательной для применения в системах информационной безопасности:

Использование принципов квантовой механики обеспечивает абсолютную безопасность передачи информации. Даже с учетом развития квантовых компьютеров, методы квантовой криптографии остаются устойчивыми к вычислительным атакам.

Принцип неделимости квантового состояния и принцип квантовой телепортации обеспечивают невозможность подслушивания при передаче информации, что делает квантовую криптографию идеальным инструментом для защиты конфиденциальных данных.[2]

Квантовая криптография позволяет передавать данные с очень высокой скоростью, что делает ее эффективной для использования в сетях высокоскоростной передачи данных.

Несмотря на многочисленные преимущества, у квантовой криптографии есть и некоторые недостатки и вызовы, которые следует учитывать:

Внедрение квантовой криптографии требует высокотехнологичного оборудования и специализированных знаний, что может быть сложно и затратно для многих организаций.

Квантовая телепортация и передача квантовых состояний ограничены расстоянием, что может ограничивать применение квантовой криптографии в глобальных сетях.

Для успешного внедрения квантовой криптографии необходимо интегрировать ее с существующими системами информационной безопасности, что может потребовать значительных усилий и времени.

Несмотря на вызовы и недостатки, квантовая криптография обладает большим потенциалом и широкими перспективами применения в обеспечении информационной безопасности:[3]

Применение квантовой криптографии может привести к развитию квантовых сетей, которые будут обеспечивать абсолютную безопасность передачи информации между узлами сети.

Квантовая криптография может быть использована для защиты критической инфраструктуры, такой как системы управления энергоснабжением и транспортные сети, от кибератак и кибершпионажа.[4]

В сфере здравоохранения квантовая криптография может обеспечить безопасную передачу медицинских данных и личной информации пациентов, что критически важно для обеспечения конфиденциальности и целостности этих данных.

В финансовом секторе квантовая криптография может использоваться для защиты финансовых транзакций и данных клиентов от киберпреступников и мошенников.

Квантовая криптография может улучшить безопасность облачных вычислений, защищая данные, хранимые и передаваемые через облачные сервисы, от утечек и атак.

Заключение

Квантовая криптография представляет собой инновационную и перспективную область в обеспечении информационной безопасности. Основываясь на принципах квантовой механики, она предлагает уникальные преимущества, такие как абсолютная безопасность передачи данных и невозможность их подслушивания. [5] Однако внедрение квантовой криптографии сопряжено с рядом технических и организационных вызовов, включая необходимость сложного оборудования, ограничения на расстояние передачи данных и интеграцию с существующими системами. Несмотря на эти вызовы, потенциал квантовой криптографии в различных областях — от защиты критической инфраструктуры и медицинских данных до финансовых транзакций и облачных вычислений — делает её важным инструментом для будущего цифровой безопасности. Развитие квантовых сетей и дальнейшее совершенствование квантовых технологий обещают значительно усилить защиту информации и способствовать созданию новых, более безопасных систем связи. С учетом продолжающегося прогресса в данной области, квантовая криптография имеет все шансы стать ключевым элементом обеспечения безопасности в цифровом мире.

Список литературы

1. Виткова Л. А., Ахрамеева К. А., Грузинский Б. А. Использование геометрических хеш-функций в информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности. – 2017. – Т. 37. – №. 3. – С. 5-9.
2. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом // СПб.: СПбГУТ. – 2014. – Т. 176.
3. Ахрамеева К. А. и др. Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии // Телекоммуникации. – 2020. – №. 8. – С. 14-20.
4. Березина Е. О., Виткова Л. А., Ахрамеева К. А. Классификация угроз информационной безопасности в сетях IOT // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 11-18.
5. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 111-114. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.

References

1. Tsvetkova L. A., Vakhrameeva K. A., Gruzinsky B. A. The use of geometric hash functions in information security // News of higher educational institutions. Light industry technology. - 2017. – Vol. 37. – No. 3. – pp. 5-9.
2. Nechaeva K. A. Development of undetectable stegosystems for channels with noise // St. Petersburg: SPbSUT. – 2014. – Vol. 176.
3. Akhrameeva K. A. et al. Analysis of the means of exchanging hidden data by intruders on the Internet using steganography methods // Telecommunications. - 2020. – No. 8. – pp. 14-20.
4. Berezina E. O., Tsvetkova L. A., Vakhrameeva K. A. Classification of information security threats in IT networks // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 11-18.

5. Virrich E. V., Ferapontova S. S. On the issue of personal data audit //Actual problems of infotelecommunications in science and education (APINO 2018). – 2018. – pp. 111-114.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРИВАТНОСТИ В ЭПОХУ ЦИФРОВИЗАЦИИ: ВЫЗОВЫ И РЕШЕНИЯ

Гаджиев Г.К.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
gugac134@gmail.com

В условиях стремительного развития технологий и цифровизации защита персональных данных и приватности становится одной из ключевых задач современного общества. В статье рассматриваются основные вызовы, связанные с обеспечением кибербезопасности, включая рост объема персональных данных, угрозы кибератак, сбор данных без согласия и недостаточную защиту в организациях. Анализируются подходы к решению этих проблем, такие как внедрение современных технологий безопасности, соблюдение законодательства, обучение сотрудников и развитие международного сотрудничества. Особое внимание уделяется роли граждан в защите своих данных и созданию культуры безопасности на всех уровнях общества.

Ключевые слова: Цифровизация, персональные данные, кибербезопасность, приватность, утечка данных, кибератаки, защита данных, шифрование, законодательство о защите данных.

PROTECTION OF PERSONAL DATA AND PRIVACY IN THE ERA OF DIGITALIZATION: CHALLENGES AND SOLUTIONS

Gadzhiev G.K.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: gugac134@gmail.com

With the rapid development of technology and digitalization, the protection of personal data and privacy is becoming one of the key tasks of modern society. The article examines the main challenges associated with ensuring cybersecurity, including the growth of personal data, the threat of cyber attacks, the collection of data without consent and insufficient protection in organizations. Approaches to solving these problems are analyzed, such as the introduction of modern security technologies, compliance with legislation, employee training and the development of international cooperation. Particular attention is paid to the role of citizens in protecting their data and creating a culture of security at all levels of society.

Keywords: Digitalization, personal data, cybersecurity, privacy, data leakage, cyber attacks, data protection, encryption, data protection legislation.

Введение

В современном цифровом мире, где технологический прогресс стремительно продвигает нас к цифровой трансформации в различных сферах жизни, защита персональных данных и приватности становится все более актуальной и критической задачей. Организации и частные лица сталкиваются с растущими угрозами безопасности данных и нарушениями приватности, которые могут привести к серьезным последствиям. В данной статье рассматриваются вызовы и решения в области защиты персональных данных и приватности в эпоху цифровизации.

Рост объема персональных данных.

Одним из ключевых вызовов в обеспечении защиты данных является взрывной рост объема персональных данных, создаваемых и хранимых в цифровой форме. С развитием интернета, цифровых платформ, социальных сетей, мобильных приложений и интернета вещей, каждый пользователь генерирует большое количество данных о своей жизни, привычках, предпочтениях и финансовых операциях. Это создает огромный потенциал для злоумышленников получить доступ к этим данным и злоупотребить ими [1].

С ростом объема цифровых данных увеличивается и уровень киберугроз. Хакерские атаки, вирусы, фишинг, атаки малваре и другие формы киберпреступности становятся все более изощренными и распространенными. Организации и частные лица подвергаются риску утечек данных, финансовых потерь, утраты репутации и других негативных последствий.

Многие компании собирают и используют персональные данные пользователей без их явного согласия или даже осведомленности. Это может включать сбор данных через онлайн-трекинг, аналитику поведения пользователей, использование куки-файлов и другие методы. Подобные практики могут нарушать приватность и индивидуальные права пользователей [2].

Многие организации не обеспечивают должного уровня защиты для хранящихся у них данных. Уязвимости в сетевых системах, слабые пароли, недостаточное шифрование данных - все это делает персональную информацию уязвимой для кибератак и утечек. Недостаточная защита данных может привести к серьезным нарушениям безопасности и утечкам конфиденциальной информации.

Современные данные могут быть переданы через границы и храниться на серверах в различных странах. Это создает сложности в обеспечении соблюдения законодательства о защите данных, так как различные страны имеют разные правила и требования к хранению и использованию персональной информации. Это также означает, что данные могут подвергаться риску перехвата и злоупотребления на протяжении всего пути их передачи через интернет [3].

Решения для обеспечения защиты персональных данных:

- Внедрение современных технологий безопасности: Организации должны активно использовать современные технологии для защиты данных, такие как шифрование, многофакторная аутентификация, системы мониторинга безопасности и идентификации аномального поведения [4].
- Соблюдение законодательства: Компании должны строго соблюдать законы и нормативные акты о защите данных, включая Общий регламент по защите данных (GDPR) в Европейском союзе и другие региональные законы о защите данных.
- Обучение персонала: Важно обучать сотрудников компаний и организаций принципам безопасности данных и правильным процедурам обращения с конфиденциальной информацией, чтобы снизить риск утечек данных из-за человеческого фактора.
- Разработка прозрачной политики конфиденциальности: Организации должны разработать и публично опубликовать политику конфиденциальности, в которой четко определены цели сбора данных, способы их использования и права пользователей [5].
- Развитие международного сотрудничества: Государства и международные организации должны сотрудничать в области разработки стандартов безопасности данных и обмена информацией о киберугрозах для обеспечения более эффективной защиты персональных данных.
- Активная роль граждан и потребителей: Граждане и потребители должны быть проактивны в защите своих персональных данных. Это включает осознанное использование интернет-сервисов, регулярное обновление паролей, отказ от сомнительных приложений и веб-сайтов, а также внимательное отношение к запросам на предоставление персональной информации.

- Развитие инновационных методов защиты данных: Непрерывное исследование и разработка новых методов и технологий для защиты данных является важным аспектом обеспечения кибербезопасности в эпоху цифровизации. Это включает в себя использование искусственного интеллекта, машинного обучения, блокчейна и других инновационных подходов.
- Создание культуры безопасности данных: Не менее важно создать культуру безопасности данных как на уровне организаций, так и в обществе в целом. Это включает в себя проведение обучающих мероприятий, освещение вопросов кибербезопасности в СМИ, мотивацию сотрудников и граждан к ответственному обращению с данными.

Заключение

Защита персональных данных и приватности является неотъемлемой частью кибербезопасности в эпоху цифровизации. С ростом объема данных и угроз кибербезопасности становится все более важно разрабатывать эффективные стратегии и методы защиты данных, соблюдать законодательство и создавать культуру безопасности как на уровне организаций, так и в обществе в целом. Только совместные усилия всех заинтересованных сторон позволят обеспечить надежную защиту персональных данных и приватности в эпоху цифровой трансформации.

Список литературы

1. Бирих Э. В. и др. Исследование вопросов повышения уровня защищенности органов исполнительной власти //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – [С. 107-110].
2. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – [С. 72-76].
3. Герлинг Е. Ю. Исследование эффективности методов обнаружения стегосистем, использующих широкополосное вложение //Телекоммуникации. – 2014. – №. 1. – [С. 06-12].
4. Ковцур М. М. и др. Исследование способов удаленного перехвата трафика в корпоративных сетях //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия. – 2021. – Т. 1. – [С. 68-75].
5. Герлинг Е. Ю. и др. Анализ и выявление психологических аспектов внутренних угроз на объектах связи //Известия высших учебных заведений. Технология легкой промышленности. – 2018. – Т. 39. – №. 1. – [С. 13-16].

References

1. Birikh E. V. et al. Research on issues of increasing the level of protection of executive authorities //Actual problems of infotelecommunications in science and education (APINO 2018). – 2018. – [pp. 107-110].
2. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – №. 4. – [Pp. 72-76].
3. Gerling E. Y. Investigation of the effectiveness of methods for detecting stegosystems using broadband embedding //Telecommunications. – 2014. – №. 1. – [Pp. 06-12].

4. Kovtsur M. M. et al. Research of methods of remote interception of traffic in corporate networks //Bulletin of the St. Petersburg State University of Technology and Design. Series. – 2021. – Vol. 1. – [pp. 68-75].
 5. Gerling E. Yu. et al. Analysis and identification of psychological aspects of internal threats at communication facilities //News of higher educational institutions. Light industry technology. - 2018. – vol. 39. – No. 1. – [pp. 13-16].
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.15

РАЗРАБОТКА АРХИТЕКТУРНЫХ РЕШЕНИЙ ДЛЯ СОЗДАНИЯ ВЕБ-СЕРВИСА ПО РАЗВЕРТЫВАНИЮ САЙТОВ НАУЧНЫХ МЕРОПРИЯТИЙ

Астахов К.А.

ФГБОУ ВО "МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (125993, Москва, Волоколамское ш., д. 4), e-mail: kir190477@mail.ru

Цель: Определить основные подходы и концепции построения архитектуры веб сервиса, который позволил бы создавать и разворачивать типовые сайты научных мероприятий.

Метод: исследование всевозможных подходов разработки приложений, а также стеков технологий, которые могли бы быть использованы для решения задачи создания подобных сервисов.

Результат: получены основные концепции для решения данной задачи, определен стек технологий и реализована концепция построения архитектуры веб сервиса, позволяющая оптимально и эффективно использовать ресурсы, которые могли бы быть предоставлены в рамках реализации поставленного в задаче интернет приложения.

Ключевые слова: Разработка; веб-разработка; архитектура приложений.

DEVELOPMENT OF ARCHITECTURAL SOLUTIONS FOR THE CREATION OF A WEB SERVICE FOR THE DEPLOYMENT OF SCIENTIFIC EVENT SITES

Astakhov K.A.

MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (125993, Moscow, Volokolamskoye shosse, 4), e-mail: kir190477@mail.ru

Purpose: To identify the main approaches and concepts for building a web service architecture that would allow you to create and deploy typical sites for scientific events.

Method: the study of various approaches to application development, as well as technology stacks that could be used to solve the problem of creating such services.

Result: the basic concepts for solving this problem have been obtained, the technology stack has been defined and the concept of building a web service architecture has been implemented, allowing optimal and efficient use of resources that could be provided as part of the implementation of the Internet application set in the task.

Keywords: Development; web development; application architecture.

Современная научная среда стремительно развивается, и проведение научных мероприятий становится неотъемлемой частью этого процесса. Создание веб-сайтов для научных мероприятий является важным элементом успешной организации и популяризации мероприятий. В данной работе рассматривается идея разработки интернет-сервиса, позволяющего легко и быстро создавать типовые сайты для научных мероприятий.

Актуальность, разрабатываемого интернет-сервиса для разворачивания типовых сайтов научных мероприятий, объясняется несколькими важными факторами:

1) Современная диджитализация.

В современном мире диджитализация стала неотъемлемой частью организации событий. Создание веб-сайтов является одним из ключевых элементов современной коммуникации и

информационной публикации. Он предоставляет участникам мероприятий быстрый и удобный доступ к информации.[1]

2) Сокращение времени и ресурсов.

Традиционное создание веб-сайтов может быть сложным и затратным процессом, требующим навыков разработки и дизайна. Интернет-сервис для создания сайтов определенного формата позволяет экономить время и ресурсы организаторов мероприятий.

3) Доступность.

Сервисы для создания сайтов делают эту технологию доступной для широкого круга пользователей. Даже люди без специальных знаний в веб-разработке могут создать профессионально выглядящий сайт для своего мероприятия.[2]

4) Снижение ошибок и обновление информации.

Интернет-сервисы предоставляют удобные инструменты для редактирования и обновления информации на сайте. [3] Это помогает избежать ошибок в расписании и предоставлении актуальной информации.

5) Усиление профессионального восприятия.

Данный интернет-сервис обладает всеми необходимыми инструментами для создания сайта, имеющего привлекательный дизайн и необходимый функционал для сайта с такой спецификой.

В рамках поставленной задачи следует понимать, чтобы получить наиболее эффективное и оптимизированное решение для данной задачи, необходимо учитывать следующие факторы:

- Масштабируемость: возможность легко добавлять новые функции и обрабатывать большой объём запросов.
- Надёжность: система должна быть отказоустойчивой.
- Производительность: быстрая обработка запросов и развертывание сайтов.

Основываясь на данных критериях, мы будем определять подходы и стеки технологий в следующих областях:

- архитектурные подходы
- стек технологий для сервисной разработки(backend)
- стек технологий для frontend разработки
- стек технологий для развертывания подобного сервиса

Рассмотрим архитектурные подходы, которые могли бы быть использованы в рамках данной работы:

Варианты архитектурного подхода:

- Микросервисная архитектура: каждый компонент системы может быть выделен в отдельный сервис. [4] Это позволяет масштабировать отдельные компоненты и упрощает сопровождение.
- Монолитная архитектура: все компоненты интегрированы в одно приложение. Этот вариант может быть проще в разработке и развертывании на начальном этапе, но менее гибок при масштабировании.
- Serverless/Function-as-a-Service (FaaS): использование функций, которые выполняются в облаке только по мере необходимости (например, развертывание сайта по триггеру). Подходит для событийно-ориентированных задач и снижения затрат на инфраструктуру.

Наиболее подходящий вариант — микросервисная архитектура, так как она обеспечивает высокую масштабируемость и гибкость в добавлении новых функций и изменении существующих. [5] Рассмотрев критерии и возможности каждого подхода, микросервисная архитектура наиболее целесообразна для решения данной задачи. Она обеспечит баланс между гибкостью, производительностью и возможностью масштабирования.

Далее проведем анализ и определим стеки технологий, которые могли бы быть использованы в рамках данной задачи

Backend часть.

Язык программирования: **golang (Go)**

Для задачи развертывания типовых сайтов научных мероприятий важно учитывать производительность, параллелизм, простоту развертывания и обслуживания. Go известен своей производительностью, простотой и встроенной поддержкой параллелизма, что делает его удобным для подобных задач. Go компилируется в машинный код, что обеспечивает высокую скорость выполнения. [6] Это важно для сервисов, которые должны быстро обрабатывать запросы и выполнять операции по развертыванию сайтов. Также язык golang предоставляет встроенную поддержку горутин и каналов, которые позволяют легко создавать конкурентные программы. Это удобно для задач развертывания, которые могут выполняться параллельно (например, развертывание нескольких сайтов одновременно).

Данный язык обладает простым и лаконичным синтаксисом, что упрощает разработку и поддержку кода. Разработка на Go позволяет быстро создавать надежные сервисы без сложных конструкций.

Go создает статически связанный исполняемый файл, который можно запускать на любой системе без дополнительных зависимостей. Это упрощает процесс развертывания и обеспечивает кроссплатформенность.[7]

Также Go оснащен богатой стандартной библиотекой, включающей инструменты для работы с сетью, HTTP-серверами, синхронизацией, JSON и многое другое. [8] Это позволяет быстро создавать веб-сервисы без необходимости в дополнительных лишних зависимостей. Также golang предлагает встроенную систему сборки и управления зависимостями (Go modules), которая упрощает управление проектом и его развертывание.

Исходя из преимуществ языка можно отметить, что go - отличный выбор для создания высокопроизводительных, надежных и легко масштабируемых интернет-сервисов.

Web фреймворк: **Fiber**

Для создания интернет-сервиса на Go есть несколько веб-фреймворков, и выбор подходящего зависит от требований задачи. В данном случае Fiber может быть хорошим выбором, учитывая его особенности и преимущества для создания высокопроизводительных веб-сервисов. Fiber построен на основе fasthttp, одного из самых быстрых HTTP-стеков для Go. Это делает Fiber крайне производительным и эффективным при обработке большого количества запросов, что важно для сервиса, который может обслуживать множество пользователей и быстро развертывать сайты. а благодаря оптимизированному процессу обработки запросов, Fiber обеспечивает низкие задержки, что способствует быстрому реагированию сервиса на пользовательские запросы.[9]

Fiber позволяет легко обрабатывать запросы асинхронно, что важно для задач, которые требуют высокой пропускной способности и быстрого развертывания сайтов. Более того, Fiber

предлагает гибкую и мощную систему маршрутизации, которая позволяет легко управлять различными путями и их обработчиками, что удобно при создании RESTful API для управления сайтами.[10]

Встроенные Middleware. Fiber поставляется с набором встроенных middleware (например, для работы с CORS, сессиями, сжатиями), которые могут быть полезны для разработки интернет-сервиса, избавляя от необходимости разрабатывать эти компоненты с нуля.

Малый размер и легковесность: Fiber разработан с акцентом на минимализм, что делает его легковесным и быстрым в развертывании. Это снижает нагрузку на систему и позволяет эффективнее использовать ресурсы.

Совместимость с существующей экосистемой: Fiber хорошо сочетается с другими библиотеками и инструментами Go, что позволяет использовать дополнительные модули для базы данных, авторизации и других задач без сложной интеграции.

Использование Fiber в контексте данной задачи позволит быстро и эффективно разработать высокопроизводительный и отзывчивый интернет-сервис для развёртывания типовых сайтов научных мероприятий.

База данных: **CockroachDB**

CockroachDB — это распределенная реляционная база данных, которая известна своей высокой доступностью, горизонтальной масштабируемостью и совместимостью с SQL. В контексте задачи по развёртыванию типовых сайтов научных мероприятий эти особенности могут быть особенно полезными. CockroachDB автоматически масштабируется горизонтально, добавляя новые узлы к кластеру. Это означает, что база данных может легко обрабатывать увеличение нагрузки, что полезно, когда количество сайтов и пользователей растет. Выбранная СУБД, спроектирована таким образом, чтобы быть устойчивой к сбоям, обеспечивая высокую доступность данных. Она использует автоматическое распределение и репликацию данных между узлами, что делает её способной продолжать работу даже при выходе из строя отдельных узлов. Это критически важно для интернет-сервиса, который должен быть доступен и надежен.[11]

Совместимость с SQL. CockroachDB полностью совместима с SQL, что упрощает работу с базой данных для разработчиков, знакомых с традиционными реляционными системами. Это облегчает создание и выполнение сложных запросов для управления данными о сайтах и пользователях.[12]

Гео-репликация и низкая задержка. CockroachDB поддерживает географическое распределение данных, что позволяет хранить данные ближе к пользователям, уменьшая задержки при доступе к ним. Это особенно полезно для сервиса, который может иметь глобальных пользователей, посещающих сайты научных мероприятий из разных регионов.

Простое управление и автоматическое распределение. CockroachDB автоматизирует задачи распределения данных и балансировки нагрузки между узлами, что снижает административные усилия. Это позволяет сосредоточиться на разработке функционала сервиса, а не на управлении базой данных. [13] CockroachDB обеспечивает строгую согласованность транзакций, что гарантирует целостность данных при выполнении операций, таких как создание или обновление информации о сайтах. Это важно для обеспечения корректности и надежности данных.

Также CockroachDB легко развернуть в различных средах, включая локальные, облачные и гибридные инфраструктуры. Это упрощает настройку базы данных в зависимости от потребностей проекта.

Кэширование данных (не реляционная база данных): **redis**

Redis — это высокопроизводительное хранилище данных в памяти, которое часто используется для кэширования, управления сессиями и очередей задач. В контексте интернет-сервиса по развёртыванию типовых сайтов научных мероприятий Redis может существенно улучшить производительность и эффективность системы. Redis хранит данные в памяти, обеспечивая чрезвычайно быструю скорость доступа. Это делает его идеальным для кэширования часто запрашиваемых данных, таких как конфигурации сайтов, шаблоны страниц или результаты запросов к базе данных. Кэширование позволяет снизить нагрузку на основную базу данных и ускорить время отклика сервиса.

Redis отлично подходит для управления сессиями пользователей благодаря своей скорости и поддержке различных структур данных. Это позволяет хранить состояние сессий и быстро его извлекать, что особенно полезно для аутентификации и авторизации пользователей. Также данная БД поддерживает работу с очередями, что может быть использовано для распределения задач по развертыванию сайтов. Например, запросы на создание или обновление сайтов можно помещать в очередь, а затем обрабатывать асинхронно, чтобы не блокировать основной поток обработки запросов.

Публикация и подписка (Pub/Sub). Redis предоставляет механизм Pub/Sub, который позволяет создавать эффективную систему обмена сообщениями между различными компонентами сервиса. Это может быть полезно для оповещения различных частей системы о событиях, таких как завершение развертывания сайта.

Гибкость и поддержка различных структур данных. Redis поддерживает множество структур данных, включая строки, хеши, списки, множества и т.д. Это позволяет гибко использовать Redis для различных целей, будь то кэширование сложных объектов или хранение простых ключ-значений.

Простота развертывания и управления. Redis легко развернуть и управлять им. Он может быть быстро интегрирован в существующую инфраструктуру, а также предлагает механизмы резервного копирования и восстановления данных.

Высокая доступность и репликация. Redis поддерживает репликацию данных, что обеспечивает высокую доступность и отказоустойчивость. При сбоях в одном из экземпляров Redis может переключиться на резервный, обеспечивая непрерывность работы сервиса.

Контейнеризация: **Docker**

Docker — это инструмент контейнеризации, который позволяет изолировать и упаковать приложения с их зависимостями в контейнеры. В контексте интернет-сервиса для развёртывания типовых сайтов научных мероприятий использование Docker может упростить развертывание, управление и масштабирование приложения. Docker позволяет упаковать приложение и все его зависимости в единый контейнер. Это обеспечивает консистентное рабочее окружение при переносе приложения между различными этапами разработки, тестирования и производства. Разработчики и DevOps-инженеры будут уверены, что приложение работает одинаково везде, независимо от особенностей среды.

С Docker развертывание приложений становится проще и быстрее. Вы можете создавать образы контейнеров с настроенным приложением, которые легко развертываются на любой

машине, поддерживающей Docker. Это сокращает время настройки и развертывания новых инстансов сервиса. Docker позволяет легко масштабировать сервис, запуская дополнительные экземпляры контейнеров при росте нагрузки. Оркестрационные инструменты, такие как Kubernetes, могут использоваться вместе с Docker для управления кластером контейнеров, обеспечивая автоматическое масштабирование и балансировку нагрузки.

Облегчение CI/CD. Docker интегрируется с системами CI/CD, такими как GitLab CI/CD или GitHub Actions, позволяя автоматически собирать, тестировать и развертывать контейнеры. Это ускоряет процесс разработки и поставки новых версий приложения, обеспечивая непрерывную интеграцию и доставку.

Контейнеры Docker используют меньше ресурсов по сравнению с виртуальными машинами, так как они разделяют ядро операционной системы, но при этом изолируют процессы. Это позволяет более эффективно использовать ресурсы сервера и запускать больше инстансов сервиса на одном оборудовании. Также Если интернет-сервис разрабатывается по микросервисной архитектуре, Docker облегчает управление каждым микросервисом как отдельным контейнером. Это позволяет независимо разрабатывать, тестировать и развертывать компоненты системы.

Простота в управлении зависимостями. С Docker, все зависимости приложения (библиотеки, инструменты, конфигурации) включены в контейнер. Это устраняет проблемы с несовместимостями зависимостей и конфигураций на разных серверах или окружениях. В дополнение можно добавить, что Docker позволяет быстро создавать изолированные окружения для тестирования. Это удобно для автоматизации тестов, создания тестовых инстансов сервисов и проверки работы приложения в различных сценариях.

Использование Docker в рамках данной задачи обеспечивает эффективное управление окружением, упрощает развертывание и масштабирование, а также улучшает процесс разработки и тестирования интернет-сервиса для развёртывания типовых сайтов научных мероприятий.

Frontend часть сервиса:

Фреймворк: React

React — это JavaScript-библиотека для создания пользовательских интерфейсов, известная своей эффективностью и гибкостью. В контексте задачи по разработке интернет-сервиса для развёртывания типовых сайтов научных мероприятий, React может быть полезен для создания интуитивного и динамичного интерфейса административной панели и пользовательского взаимодействия. React позволяет создавать приложения из отдельных, переиспользуемых компонентов. Для административной панели, где есть множество повторяющихся элементов, таких как формы, списки и модальные окна, это облегчает разработку и поддержку кода. Компоненты можно легко собирать, изменять и использовать в разных частях приложения. React использует виртуальный DOM, который минимизирует операции с реальным DOM и повышает производительность приложения. Это важно для создания отзывчивого интерфейса административной панели, особенно при частом обновлении данных, например, при изменении настроек сайтов или просмотре статистики. С React также легко управлять состоянием приложения, что упрощает создание сложных и интерактивных пользовательских интерфейсов. Для административной панели это полезно для отслеживания состояния форм, фильтрации и сортировки данных, а также для управления сложными пользовательскими взаимодействиями.

React имеет обширную экосистему сторонних библиотек и инструментов, таких как React Router для управления маршрутизацией, Redux или Zustand для управления состоянием, а также множество компонентов и виджетов. Это ускоряет процесс разработки и позволяет легко расширять функциональность приложения.

React хорошо интегрируется с инструментами для серверного рендеринга (SSR) и статической генерации страниц, такими как Next.js. Это может быть полезно для создания страниц сайтов научных мероприятий с лучшей производительностью и SEO-оптимизацией.

React позволяет легко добавлять интерактивные элементы и динамические обновления интерфейса. Это важно для создания удобного и отзывчивого интерфейса, который позволяет администраторам быстро настраивать и развертывать сайты. Стоит добавить, что React также легко интегрируется с RESTful API, что упрощает взаимодействие с серверной частью интернет-сервиса, например, для управления сайтами, получения статистики и других операций.

Использование React для создания административной панели и пользовательского интерфейса в рамках данной задачи позволяет разработать производительное, динамичное и легко масштабируемое приложение, которое обеспечивает удобство взаимодействия для администраторов и пользователей.

Развертывание веб-сервиса (DevOps часть): **CI/CD: GitLab CI/CD**

GitLab CI/CD — это интегрированная в GitLab система непрерывной интеграции и доставки, которая позволяет автоматизировать сборку, тестирование и развертывание приложений. В контексте задачи по разработке интернет-сервиса для развёртывания типовых сайтов научных мероприятий, GitLab CI/CD может существенно облегчить процесс разработки и обеспечить быструю поставку новых функций. GitLab CI/CD тесно интегрирован с репозиториями в GitLab, что позволяет автоматически запускать процессы CI/CD при каждом изменении в коде (например, при коммитах или создании merge request). Это обеспечивает быстрый и автоматизированный процесс сборки и развертывания приложения.

GitLab CI/CD позволяет автоматизировать все этапы разработки, включая сборку, тестирование, линтинг, деплой и даже проверку безопасности. Это снижает количество ручной работы и минимизирует риск ошибок при развертывании новых версий приложения.

С GitLab CI/CD можно настраивать сложные пайплайны, состоящие из нескольких этапов и задач. Например, можно создать пайплайн, который сначала запускает тесты, затем создает Docker-образы для микросервисов, а после успешного прохождения всех проверок автоматически развертывает их на сервере или в облаке.

Поддержка контейнеров и Docker. GitLab CI/CD отлично поддерживает работу с Docker. Это позволяет создавать Docker-образы в рамках пайплайна, тестировать их и развертывать в контейнерных средах. Для задачи по развёртыванию сайтов это удобно, так как сам сервис и его компоненты могут быть упакованы в контейнеры. GitLab предоставляет мощные инструменты контроля доступа и безопасности, такие как доступ на основе ролей, интеграция с системами аутентификации, и проверка кода на уязвимости. Это важно для обеспечения безопасности процесса разработки и развертывания.

Мониторинг и трассировка: GitLab CI/CD предоставляет инструменты для мониторинга состояния пайплайнов, отслеживания истории развертываний и выявления проблем. Это облегчает отслеживание и диагностику проблем при развертывании новых версий приложения.

Простота в использовании. Одним из важных преимуществ GitLab CI/CD является факт того, что он имеет интуитивно понятный YAML-синтаксис для определения пайплайнов, что позволяет быстро настраивать и изменять процессы CI/CD. Это делает его доступным для разработчиков с различным уровнем опыта.

Использование GitLab CI/CD в рамках данной задачи обеспечивает автоматизацию, надежность и безопасность процесса разработки и развертывания интернет-сервиса для развёртывания типовых сайтов научных мероприятий, что ускоряет выпуск новых функций и повышает качество приложения.

Выводы

В ходе работы были определены и описаны технологии и методы для реализации веб-сервиса для развертывания типовых научных сайтов мероприятий. Были разобраны достоинства и причины, по которым были отобраны стеки технологий, описанных в статье. Был определен вид веб-сервисной архитектуры, наиболее подходящий для этой задачи. Опираясь на разработку решений задачи по созданию интернет-сервиса проведенной в статье, проясняется список требований и действий, позволяющий разработчику приступить к написанию такого интернет-сервиса.

Список литературы

1. Фаулер М. - "Шаблоны архитектуры корпоративных приложений" - Addison-Wesley Professional - 2015 - 560с.
2. Донован А. А., & Керниган, Б. В. - "Язык программирования Go" - Addison-Wesley Professional - 2015 - 400с.
3. Балбаерт И. - "Go веб-программирование" - Manning Publications - 2016 - 256с.
4. Ньюман С. - "Создание микросервисов: проектирование мелкозернистых систем" - O'Reilly Media - 2021 - 616с.
5. Бэнкс А., Порчелло Э. - "Изучаем React: современные шаблоны для разработки приложений на React" - O'Reilly Media - 2020 - 350с.
6. Виерух Р. - "Дорога к React: ваш путь к освоению чистого и практичного React.js" - Self-published - 2018 - 200с.
7. Редмонд Э., & Уилсон, Дж. Р. - "Семь баз данных за семь недель: руководство по современным базам данных и движению NoSQL" - Pragmatic Bookshelf - 2012 - 352с.
8. Меркель Д. - "Docker: легковесные контейнеры Linux для согласованной разработки и развертывания" - Linux Journal - 2014 - 100с.
9. Паль К., & Броги А. - "Технологии облачных контейнеров: обзор современных технологий" - Journal of Cloud Computing: Advances, Systems and Applications - 2019 - 20с.
10. Джоши С. - "Redis на практике" - Packt Publishing - 2013 - 124с.
11. Карлос С., & Чинчилла, Дж. - "Redis для чайников" - Wiley - 2019 - 256с.
12. Бёрнс Б., Беда Дж., & Хайтауэр К. - "Kubernetes: в действии" - O'Reilly Media - 2017 - 250с.
13. Копленд М. - "Книга о Docker: контейнеризация — это новая виртуализация" - Self-published - 2015 - 260с.

References

1. Fowler, M. - "Patterns of enterprise application architecture" - Addison-Wesley Professional - 2015 - p.560
 2. Donovan, A. A., & Kernighan, B. V. - "The Go Programming Language" - Addison-Wesley Professional - 2015 - p.400
 3. Balbaert, I. - "Go web programming" - Manning Publications - 2016 - p.256
 4. Newman, S. - "Creating microservices: designing fine-grained systems" - O'Reilly Media - 2021 – p. 616
 5. Banks, A., Porcello, E. - "Studying React: modern templates for developing applications on React" - O'Reilly Media - 2020 - p.350
 6. Vieruch, R. - "The road to React: your path to mastering clean and practical React.js" - Self-published - 2018 - pp.200
 7. Redmond, E., & Wilson, J. R. - "Seven Databases in seven Weeks: a guide to Modern databases and the NoSQL Movement" - Pragmatic Bookshelf - 2012 - p. 352
 8. Merkel, D. - "Docker: Lightweight Linux containers for coordinated development and deployment" - Linux Journal - 2014 – p.100
 9. Pal, K., & Brogi, A. - "Cloud Container technologies: an overview of modern technologies" - Journal of Cloud Computing: Advances, Systems and Applications - 2019 - p .20
 10. Joshi, S. - "Redis in practice" - Packt Publishing - 2013 - p.124
 11. Carlos, S., & Chinchilla, J. - "Redis for dummies" - Wiley - 2019 - p.256
 12. Burns, B., Bede, J., & Hightower, K. - "Kubernetes: in Action" - O'Reilly Media - 2017 - p.250
 13. Copland, M. - "The book about Docker: containerization is the new virtualization" — Self-published - 2015 - 260 p.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.942.2

МЕТОД ПОЛУЧЕНИЯ КАРТ ВЫСОТ НА ОСНОВЕ ГЕНЕРАТИВНО-СОСТАВЛЯТЕЛЬНОЙ СЕТИ

Любченко Э.М.

ФГБОУ ВО "УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", Ульяновск, Россия,
(432017, Ульяновская область, город Ульяновск, ул. Льва Толстого, д. 42), e-mail:
nighop@yandex.ru

Географическая информация представляется в виде двухмерных карт местности. Для получения сведений о рельефе местности к двумерной карте прилагается шкала высот и глубин. Она приводится в виде цветовой диаграммы с обозначением отметок относительно уровня моря. В статье представлен подход, позволяющий извлекать информацию о рельефе и высотах в условиях, когда шкала высот у карты отсутствует. Указанный подход позволяет генерировать карты высот на основе генеративно-сопоставительной сети. Сеть состоит из двух разных противопоставленных сетей - генерирующей сети, которая берёт входные данные и максимально изменяет их для получения новых данных, и дискриминирующей сети, которая пытается предсказать, являются ли выходные данные, полученные от генерирующей сети, оригинальными.

Ключевые слова: Географическая карта; карты высот; генеративно-сопоставительные сети.

METHOD OF GENERATING HEIGHTMAPS BASED ON GENERATIVE ADVERSARIAL NETWORK

Lyubchenko E.M.

ULYANOVSK STATE UNIVERSITY, Ulyanovsk, Russia, (432017, Ulyanovsk region, Ulyanovsk city,
Lva Tolstoy str., 42), e-mail: nighop@yandex.ru

Most of the time topological data is previewed as a two dimensional map. To describe specific height maps include a scale that represents each height with specific color value.

This article provides an approach that allows to extract topological and height information in cases where heightmap is missing. This approach allows to generate height maps based on conditional generative adversarial network (cGAN), which consist of two different networks - generator network, that generates a new data by taking an input and modifying it, and discriminator network, that determines whether the generated data is fake or real.

Keywords: Maps; height maps; conditional generative adversarial network (cGAN).

Введение

Географические карты являются обобщенным изображением поверхности местности. Для изображения информации о рельефе местности используется цветовое кодирование регионов карты, где каждому цвету соответствует конкретная величина высоты над уровнем моря. В случае, когда используется цветовое кодирование, к карте прилагается шкала высот, которая сопоставляет высоту (или глубину) с цветом на карте.

Однако, возможны случаи, когда шкала высот отсутствует или её невозможно корректно обработать средствами компьютерного зрения. В статье предложен способ, который на основе генеративно-сопоставительной сети позволяет построить карту высот [1] на основе оригинальной географической карты.

Карты высот

Вместо шкалы высот и кодировки высот на карте при помощи цветов могут использоваться карты высот. Карты высот - это изображение местности, представленное двумерным массивом, где каждый его элемент содержит информацию о высоте каждой точки местности [1, 2]. Пример карты высот и соответствующая ей карта местности представлена на Рисунке 1.

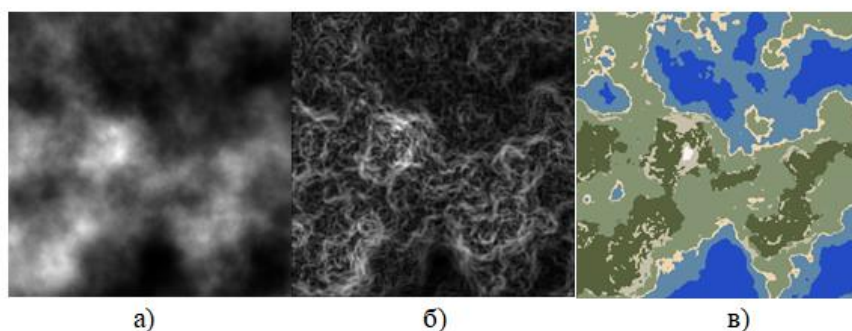


Рисунок 1. - Карта высот и соответствующие ей карта склонов и цветная карта местности. а) Карта высот. б) Карта склонов. в) Карта местности.

Карту высот можно представить как матрицу (1), а карта склонов необходима для того, чтобы отобразить наклон и спуск/подъем рельефа при помощи градиентов (Рисунок 1б) или чисел (2).

$$HMap = \begin{pmatrix} H_{1,1} & \cdots & H_{N,1} \\ \vdots & \ddots & \vdots \\ H_{1,M} & \cdots & H_{N,M} \end{pmatrix} \quad (1)$$

Карта склонов представляется матрицей, у которой каждый элемент получен на основе матрицы высот и каждый элемент является средним арифметическим значений высот для соседних элементов матрицы.

$$SMap = \begin{pmatrix} \frac{|3 * HMap_{1,1} - HMap_{1,2} - HMap_{2,1} - HMap_{2,2}|}{3} & \cdots & \cdots \\ \vdots & \ddots & \vdots \\ \frac{|3 * HMap_{1,M} - HMap_{1,M-1} - HMap_{2,M-1} - HMap_{2,M}|}{3} & \cdots & \cdots \end{pmatrix} \quad (2)$$

Двухмерная цветная карта местности может быть получена функцией преобразования числовой величины карты высот и склонов в соответствующий данной величине цвет. Данная функция получает на вход два параметра – высоту (h) и величину склона (s) в конкретной точке карты (элементе матрицы) и возвращает соответствующее значение в цветовой схеме RGB [3], которое является вектором из трех элементов, где каждый из элементов соответствует значению цвета в определенном канале RGB. Пример данной функции представлен в формуле (3).

$$color(h, s) = \begin{cases} (200, 192, 170), & 0.2 < h < 0.9 \text{ and } s > 0.45 \\ (35, 75, 195), & h \leq 0.1 \\ (94, 145, 168), & 0.2 < h \leq 0.225 \\ (238, 214, 175), & 0.225 < h \leq 0.45 \\ (132, 147, 114), & 0.45 < h \leq 0.85 \\ \dots & \end{cases} \quad (3)$$

Генеративно-состязательные сети

В качестве инструмента для преобразования двухмерной карты в карту высот предлагается использовать модель генеративно-состязательной сети [4, 5].

Генеративно-состязательная сеть это модель, которая в данном случае обучается преобразованию изображения x с вектором шума z в y , где y – фотореалистическое изображение, близкое к реальному (4). Генератор G обучается созданию изображений, которые дискриминатор D не может отличить от «реальных». Дискриминатор D в данном случае обучается как можно лучше выявлять все изображения далекие от реальных, которые сгенерировал генератор G . [1]

$$G: f(x, z) \rightarrow y \quad (4)$$

Пусть математическое ожидание – E , Тогда задачу, поставленную перед генеративно-состязательной сетью можно представить в виде (5).

$$GAN(G, D) = E_{x,y}[\log D(x, y)] + E_{x,z}[\log (1 - D(x, G(x, z)))] \quad (5)$$

В (5) основная задача генератора G – попытаться как можно сильнее снизить влияние дискриминатора D .

Конкретно для решения задачи преобразования изображения в другое изображение (двухмерную карту в карту высот) предлагается использовать подвид генеративно-состязательных сетей – pix2pix [6]. Данная модель специально спроектирована для сопоставления входных изображений с выходными.

Генератор, используемый в pix2pix [6] является модификацией U-Net [7], который состоит из кодера и декодера. Структура слоев генератора представлена в Таблице 1.

Таблица 1. - Список слоев генеративной сети

Тип слоя	Размер ядра слоя	Параметры слоя, (Н, W, С)
InputLayer		(256, 256, 3)
Sequential	4 * 4	(128, 128, 64)
Sequential	4 * 4	(64, 64, 128)
Sequential	4 * 4	(32, 32, 256)
Sequential	4 * 4	(16, 16, 512)
Sequential	4 * 4	(8, 8, 512)
Sequential	4 * 4	(4, 4, 512)
Sequential	4 * 4	(2, 2, 512)
Sequential	4 * 4	(1, 1, 512)

Тип слоя	Размер ядра слоя	Параметры слоя, (H, W, C)
Sequential	4 * 4	(2, 2, 512)
Concatenate	4 * 4	(2, 2, 1024)
Sequential	4 * 4	(4, 4, 512)
Concatenate	4 * 4	(4, 4, 1024)
Sequential	4 * 4	(8, 8, 512)
Concatenate	4 * 4	(8, 8, 1024)
Sequential	4 * 4	(16, 16, 512)
Concatenate	4 * 4	(16, 16, 1024)
Sequential	4 * 4	(32, 32, 256)
Concatenate	4 * 4	(32, 32, 512)
Sequential	4 * 4	(64, 64, 128)
Concatenate	4 * 4	(64, 64, 256)
Sequential	4 * 4	(128, 128, 64)
Concatenate	4 * 4	(128, 128, 128)
Conv2DTranspose	4 * 4	(256, 256, 3)

Дискриминатор D является классификатором PatchGAN (Markovian discriminator) [8] – он пытается выяснить, является ли каждый фрагмент изображения реальным или нет. Дискриминатор получает на вход 2 изображения – входное изображение, которое является реальным и сгенерированное изображение, полученное на выходе генератора G, которое дискриминатор D должен классифицировать как подделку.

Структура слоев дискриминатора D представлена в Таблице 2.

Таблица 2. - Список слоев дискриминирующей сети

Тип слоя	Размер ядра слоя	Параметры слоя, (H, W, C)
InputLayer		(256, 256, 3)
Concatenate	4 * 4	(256, 256, 6)
Sequential	4 * 4	(128, 128, 64)
Sequential	4 * 4	(64, 64, 128)
Sequential	4 * 4	(32, 32, 256)
ZeroPadding2D	4 * 4	(34, 34, 256)
Conv2D	4 * 4	(31, 31, 512)
BatchNormalization	4 * 4	(31, 31, 512)
LeakyReLU	4 * 4	(31, 31, 512)
ZeroPadding2D	4 * 4	(33, 33, 512)
Conv2D	4 * 4	(30, 30, 1)

Общий вид данной сети представлен на Рисунке 2.

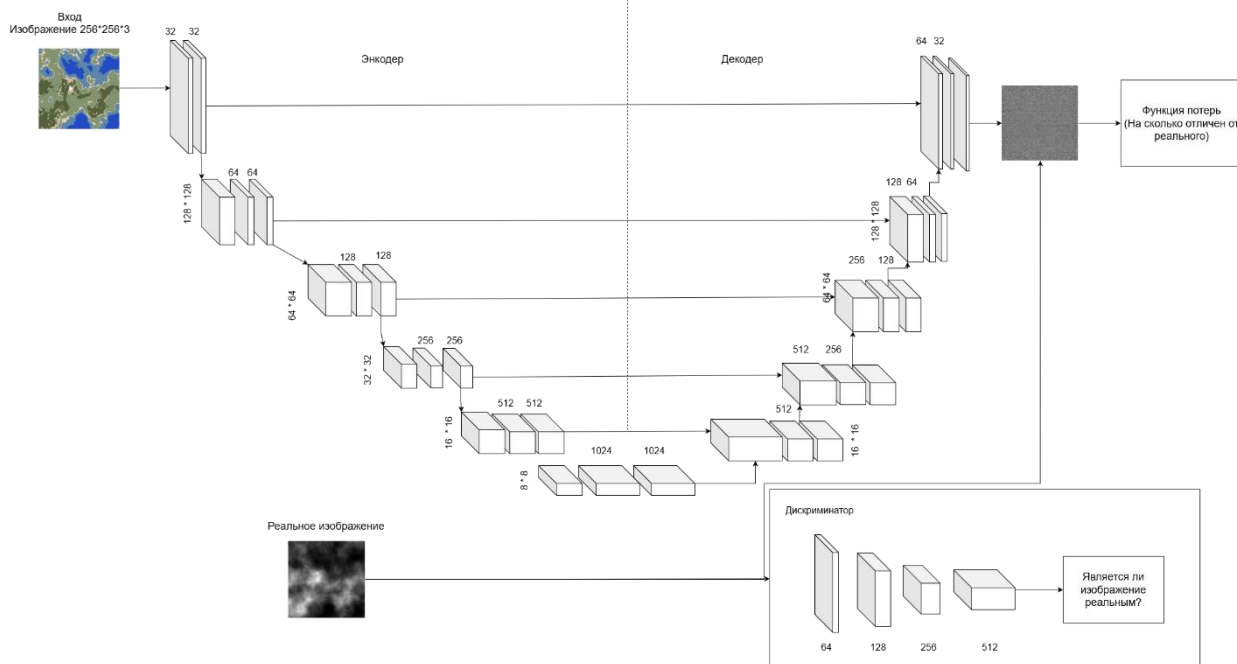


Рисунок 2. - Общая схема построенной сети.

Подготовка данных для обучения сети

В качестве набора данных для сети был выбран метод по генерации набора карт с одинаковой шкалой высот на основе симплексного шума [9], таким образом можно сгенерировать неограниченное количество карт местности и соответствующих им карт высот.

Метод получает на вход оригинальную цветную двухмерную карту местности. Затем необходимо извлечь информацию о шкале высот, которая соответствует карте местности. Для решения данной задачи предлагается использовать метод k-средних [10], который позволяет извлечь весь набор цветов, представленный на карте.

После того как была получена информация о карте высот можно переходить к созданию набора данных. При помощи функции симплексного шума можно создать набор карты высот.

Пусть $snoise$ - это функция генерации симплексного шума, тогда карту высот с шириной N и высотой M по формуле (1) можно представить как матрицу (6).

$$HMap_{snoise} = \begin{pmatrix} snoise_{1,1} & \cdots & snoise_{N,1} \\ \vdots & \ddots & \vdots \\ snoise_{1,M} & \cdots & snoise_{N,M} \end{pmatrix} \quad (6)$$

$$SMap_{snoise} = \begin{pmatrix} \frac{|3 * HMap_{snoise_{1,1}} - HMap_{snoise_{1,2}} - \cdots|}{3} & \cdots & \cdots \\ \vdots & \ddots & \vdots \\ \frac{|3 * HMap_{snoise_{1,M}} - HMap_{snoise_{1,M-1}} - \cdots|}{3} & \cdots & \cdots \end{pmatrix} \quad (7)$$

$$Map_{snoise} = \begin{pmatrix} color(HMap_{snoise_{1,1}}, SMap_{snoise_{1,1}}) & \cdots & \cdots \\ \vdots & \ddots & \vdots \\ color(HMap_{snoise_{1,M}}, SMap_{snoise_{N,M}}) & \cdots & \cdots \end{pmatrix} \quad (8)$$

На основе полученной карты высот по формуле (2) необходимо построить карту склонов (7) и сгенерировать карту местности используя заранее выбранную формулу (3). Полученная карта местности (8) и карта высот (6) – являются входными данными для генеративно-состязательной сети, где (8) – это данные для генератора, а (6) – реальное изображение (эталон) для проведения сравнения с результатом работы генератора.

Результат работы

Сгенерированный набор данных это множество изображений, где каждое изображение имеет размер 256 x 512 пикселей, и является склейкой двух изображений (обычной карты местности и соответствующей ей картой высот) размером 256 x 256.

Как описано в [4] для составления тестового набора необходимо провести последующую постобработку изображений. Постобработка состоит из следующих шагов:

1. Провести изменение размера изображения 256 x 256 на большую высоту и ширину – 286 x 286.
2. Произвольно обрезать изображение обратно до 256 x 256.
3. Провести произвольное зеркальное отражение изображения (слева направо).

По ходу обучения сети была сгенерирована модель с результатами, представленными на Рисунке 3.

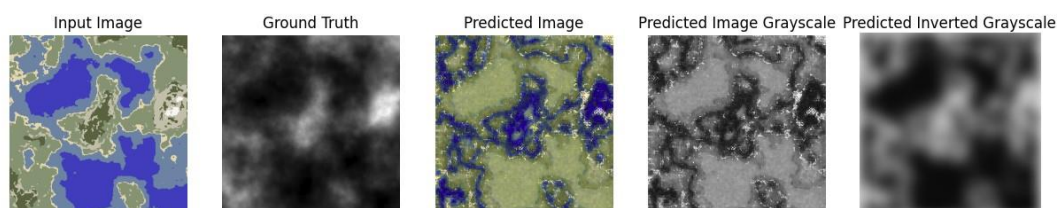


Рисунок 3. - Процесс преобразования генеративно-состязательной сетью карты местности в карту высот.

Заключение

Представленный в статье метод позволяет для заданной карты местности сгенерировать соответствующую ей карту высот. Данную карту высот в последующем можно использовать для проектирования трехмерной модели местности.

Модель, полученная в результате обучения сети, всё ещё содержит несколько недочетов – после преобразования в карту высот её необходимо привести в черно-белый вид и нормировать цвета по самому светлому и темному оттенку. Также необходимо дополнить существующий набор данных фотореалистичными изображениями карт с разными картами высот и наборами цветов у шкалы высот, что сделает модель более точной в предсказании карт высот и позволит использовать с ней больший набор карт местности.

Список литературы

1. Ивсон, Пауло и Толедо, Родриго и Гаттасс, Марсело. (2008). Наборы сплошных карт высот: моделирование и визуализация. 359-365. 10.1145/1364901.1364953.

2. Алонсо, Хесус Алонсо и Роберт Жоан-Ариньо. “Обоснованное дерево карт высот - новая структура данных для представления рельефа”. Международная конференция по теории и приложениям компьютерной графики (2008).
3. Желязко, А. "Цветовая модель RGB". Британская энциклопедия, 19 июля 2024 г. URL: <https://www.britannica.com/science/RGB-colour-model>.
4. Аланкрита Аггарвал, Мамта Миттал, Гопи Баттинени, Генеративная состязательная сеть: обзор теории и приложений, Международный журнал управления информацией Data Insights, Том 1, выпуск 1, 2021, 100004, ISSN 2667-0968.
5. Гудфеллоу И.-Дж., Пуже-Абади Дж. и Мирза М., э.э. Порождающие состязательные сети, 2014. URL: <https://arxiv.org/abs/1406.2661>
6. Изола П. Преобразование изображения в изображение с помощью условных состязательных сетей, Джун И.-З., Чжоу Т., Алексей Е. // CoRR // DOI: abs/1611.07004. URL: <https://doi.org/10.48550/arXiv.1611.07004>
7. Роннебергер О., Фишер П., Брокс Т. (2015). U-Net: Сверточные сети для сегментации биомедицинских изображений. В книге: Наваб, Н., Хорнеггер, Дж., Уэллс, У., Франджи, А. (ред.) Обработка медицинских изображений и компьютерное вмешательство - MICCAI, 2015. MICCAI, 2015. Конспекты лекций по информатике (), том 9351. Спрингер, Чам. https://doi.org/10.1007/978-3-319-24574-4_28
8. Демир, Угур и Гезде Б. Юнал. “Создание изображений на основе исправлений с помощью генеративных состязательных сетей”. arXiv abs/1803.07422 (2018).
9. Густавсон Стефан. Симплексный шум раскрыт. Линчепингский университет, Швеция. (2005). URL: https://www.researchgate.net/publication/216813608_Simplex_noise_demystified
10. Абиодун М. Икотун, Авессалом Э. Эзугву, Лейт Абуалига, Белал Абухайя, Цзя Хеминг, Алгоритмы кластеризации с помощью К-средних: всесторонний обзор, анализ вариантов и достижения в эпоху больших данных, Информационные науки, том 622, 2023, С 178-210, ISSN 0020-0255. URL: <https://www.sciencedirect.com/science/article/pii/S0020025522014633>

References

1. Ivson, Paulo & Toledo, Rodrigo & Gattass, Marcelo. (2008). Solid height-map sets: modeling and visualization. 359-365. 10.1145/1364901.1364953.
2. Alonso, Jesus Alonso and Robert Joan-Arinyo. “The Grounded Heightmap Tree - A New Data Structure for Terrain Representation.” International Conference on Computer Graphics Theory and Applications (2008).
3. Zelazko, A.. "RGB colour model." Encyclopedia Britannica, July 19, 2024. URL: <https://www.britannica.com/science/RGB-colour-model>.
4. Alankrita Aggarwal, Mamta Mittal, Gopi Battineni, Generative adversarial network: An overview of theory and applications, International Journal of Information Management Data Insights, Volume 1, Issue 1, 2021, 100004, ISSN 2667-0968.
5. Goodfellow I-J, Pouget-Abadie J. and Mirza M. e.c. Generative Adversarial Networks, 2014. URL: <https://arxiv.org/abs/1406.2661>

6. Isola, P. Image-to-Image Translation with Conditional Adversarial Networks, Jun Y-Z., Zhou T., Alexei E. // CoRR // DOI: abs/1611.07004. URL: <https://doi.org/10.48550/arXiv.1611.07004>
 7. Ronneberger, O., Fischer, P., Brox, T. (2015). U-Net: Convolutional Networks for Biomedical Image Segmentation. In: Navab, N., Hornegger, J., Wells, W., Frangi, A. (eds) Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015. MICCAI 2015. Lecture Notes in Computer Science(), vol 9351. Springer, Cham. https://doi.org/10.1007/978-3-319-24574-4_28
 8. Demir, Ugur and Gözde B. Ünal. “Patch-Based Image Inpainting with Generative Adversarial Networks.” ArXiv abs/1803.07422 (2018).
 9. Gustavson, Stefan. Simplex noise demystified. Linköping University, Swede. (2005). URL: https://www.researchgate.net/publication/216813608_Simplex_noise_demystified
 10. Abiodun M. Ikotun, Absalom E. Ezugwu, Laith Abualigah, Belal Abuhaija, Jia Heming, K-means clustering algorithms: A comprehensive review, variants analysis, and advances in the era of big data, Information Sciences, Volume 622, 2023, Pages 178-210, ISSN 0020-0255. URL: <https://www.sciencedirect.com/science/article/pii/S0020025522014633>
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.942

МОДЕЛЬ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ «ПОЧТИ-ТОЧНО-В-СРОК»

Подгорнов М.Д.

ФГБОУ ВО "УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", Ульяновск, Россия,
(432017, Ульяновская область, город Ульяновск, ул. Льва Толстого, д. 42), e-mail:
maksimka_7373@mail.ru

В работе развивается семимартингалный (траекторный) подход к математическому описанию и моделированию систем массового обслуживания (СМО) «почти-точно-в-срок». Рассмотрена модель СМО «почти-точно-в-срок». Предложена стратегия по выбору количества обслуживающих каналов. Показан переход от математической модели к итерационным формулам, по которым проводится имитационное моделирование.

Ключевые слова: Система массового обслуживания, семимартингалное описание, точно-в-срок, точечный процесс, компенсатор, имитационное моделирование.

THE QUEUING SYSTEM «ALMOST-JUST-IN-TIME» MODEL

Podgornov M.D.

ULYANOVSK STATE UNIVERSITY, Ulyanovsk, Russia, (432017, Ulyanovsk region, Ulyanovsk city,
Lva Tolstoy str., 42), e-mail: maksimka_7373@mail.ru

The paper develops a semi-martingale (trajectory) approach to the mathematical description and modeling of closed queuing systems "almost-just-in-time". The queuing systems model "almost-just-in-time" is considered. A strategy for choosing the number of service channels is proposed. The transition from a mathematical model to iterative formulas, which are used for simulation, is shown.

Keywords: Queuing System, semi-martingale description, just-in-time, point process, compensator, simulation modeling.

Введение

В работе рассматривается достаточно новая для теории массового обслуживания система *почти-точно-в-срок*.

На сегодняшний день концепция организации процессов выполнения в системах *точно-в-срок* достаточно хорошо известна и применяется во различных областях. В пример можно привести производственные системы *точно-в-срок*, также известные как *JIT* (just-in-time), методы компиляции *точно-в-срок* в программировании, а также образовательные стратегии организации обучения *точно-в-срок* (см., например, работы [1-2]).

Как правило, для описания производственных систем используются детерминистические модели, так как в подобных системах методы *точно-в-срок* рассматриваются для решения логистических задач. Однако, данные методы не подходят для других (отличных от логистики) областей применения, в частности, в моделировании систем массового обслуживания (СМО). Учитывая крайне высокую частоту случайных событий в таких системах и соответствующих им процессах, формальное описание и моделирование

СМО по принципу *точно-в-срок* представляют крайне высокий интерес, в особенности, если обратить внимание на их производственную актуальность и отсутствие соответствующих стохастических моделей. Стоит отметить, что, из-за своей специфики, СМО не может справиться с задачей *точно-в-срок*. Поэтому, в данном контексте, будет корректнее использовать термин «почти-точно-в-срок».

На сегодняшний день математические модели для систем массового обслуживания *точно-в-срок*, в частности стохастические, развиты крайне слабо. Однако, применение таких моделей необходимо при решении задач оптимального управления, так как они позволяют оптимизировать распределения системных ресурсов и реализовать оптимальную стратегию планирования достаточно произвольной стохастической системы. Цель исследования заключается в разработке стохастического описания СМО *почти-точно-в-срок*, которое было бы подходящим как для аналитических методов, так и для компьютерного моделирования.

В работе изучается модель простой СМО *почти-точно-в-срок*, в семимартингальных терминах для точечных процессов [3-5]. Управление осуществляется посредством изменения числа обслуживающих каналов. Здесь же допускаются некоторые предположения о процессах, присущих реальным системам.

1. Постановка задачи

Рассмотрим СМО, в которой имеется стартовый пул заявок в количестве $n > 0$ (Рисунок 1). Помимо изначального набора заявок, в процессе работы в систему поступают новые того же типа. Интенсивность поступления заявок определяется параметром $\lambda > 0$. Отметим, что момент их поступление ограничен во времени параметром $T > 0$. Данный параметр определяет момент времени, к которому система должна стремиться обработать все находящиеся в ней заявки.

Как было отмечено ранее, управление системой осуществляется изменением количества каналов обслуживания, которое определяется параметром $r \geq 0$. Каждый из операторов имеет одинаковую квалификацию со средней интенсивностью обслуживания $\mu > 0$.

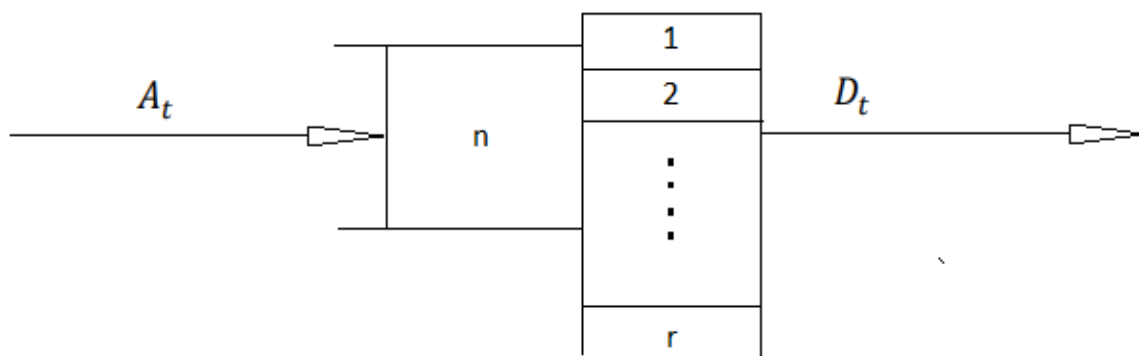


Рисунок 1. - Схема СМО.

2. Математическая модель

Для описания работы системы введем считающие процессы A, D , где $A = (A_t)_{t \geq 0}$ – число заявок, поступивших в СМО за время $t \geq 0$, $A_0 = 0$, $D = (D_t)_{t \geq 0}$ – число

обслуженных заявок в СМО за время $t \geq 0$, $D_0 = 0$. Точечные процессы A и D определяются своими компенсаторами $\tilde{A} = (\tilde{A}_t)_{t \geq 0}$ и $\tilde{D} = (\tilde{D}_t)_{t \geq 0}$ [4]:

$$A_t = \tilde{A}_t + m_t^A, \quad (1)$$

$$D_t = \tilde{D}_t + m_t^D, \quad (2)$$

где \tilde{A} и \tilde{D} – неубывающие предсказуемые процессы, m_t^A и m_t^D – мартингалы.

Для рассматриваемой в данной работе системы компенсатор процесса $A = (A_t)_{t \geq 0}$ имеет следующий вид:

$$\tilde{A}_t = \int_0^t \lambda \cdot I(s < T) ds, \quad (3)$$

где $\lambda > 0$, $I(\cdot)$ – индикаторная функция.

Компенсатор для процесса $D = (D_t)_{t \geq 0}$ определяется соотношением:

$$\tilde{D}_t = \int_0^t \mu \cdot r_s ds. \quad (4)$$

Обозначим ξ_t – число заявок в СМО в момент времени $t \geq 0$, r_t – количество обслуживающих каналов в СМО в момент времени $t \geq 0$.

Для ξ_t в момент времени $t \geq 0$ можно написать следующее основное балансовое соотношение:

$$\xi_t = n + A_t - D_t. \quad (5)$$

Для выбора количества каналов обслуживания r_t в СМО в момент времени $t \geq 0$ выбрана следующая стратегия:

$$r_t = \min(r_t^m, \xi_t) \cdot I(t < T) + \xi_t \cdot I(t \geq T), \quad (6)$$

где r_t^m – оптимальное количество каналов, при котором СМО стремиться завершить свою работу в момент времени T . Определять его будем соотношением, которое имеет следующий вид:

$$r_t^m = \left\lfloor \frac{\xi_t}{\mu \cdot (T-t)} \right\rfloor. \quad (7)$$

Логика управления системой такова. В начале определяется оптимальное количество каналов r_t^m по формуле (7). Однако, следует отметить, что количество операторов не может превышать количества заявок в системе ξ_t , поэтому необходимо найти минимум между этими значениями. Так же очевидно, что если система преодолела момент времени T , к которому стремилась, то максимально быстро она завершит свою работу, если количество обслуживающих каналов r_t будет равняться количеству заявок, оставшихся в системе.

3. Итерационные формулы

Из формул (1)-(7) можно получить следующие инфинитезимальные соотношения:

$$P\{A_{t+\Delta} - A_t = 1 | \mathcal{F}_t\} = \lambda \cdot \Delta \cdot I(t < T) + o(\Delta), \quad (8)$$

$$P\{D_{t+\Delta} - D_t = 1 | \mathcal{F}_t\} = r_t \cdot \mu \cdot \Delta + o(\Delta). \quad (9)$$

Введя дискретизацию (шаг по времени) Δ из условия $\lambda \cdot \Delta \ll 1$, $\mu \cdot \Delta \ll 1$, получим следующие итерационные формулы:

$$A_{t+\Delta} = A_t + \delta(\lambda \cdot I(t < T)), \quad (10)$$

$$D_{t+\Delta} = D_t + \delta(r_t \cdot \mu), \quad (11)$$

где $\delta(\gamma) = \begin{cases} 1, & \text{с вероятностью } \gamma \cdot \Delta, \\ 0, & \text{с вероятностью } 1 - \gamma \cdot \Delta. \end{cases}$

Далее пересчитывается число заявок в СМО в момент $t + \Delta$: $\xi_{t+\Delta} = n + A_{t+\Delta} - D_{t+\Delta}$. Затем применяем найденное значение $\xi_{t+\Delta}$ к формулам (6),(7) и находим значение

$r_{t+\Delta}$ – количество обслуживающих каналов в СМО в момент времени $t + \Delta$. После происходит переход к следующей итерации (шаг от $t + \Delta$ к $t + 2\Delta$).

4. Результаты компьютерного моделирования

Практическая реализация СМО осуществлена с помощью языка программирования высокого уровня C# в среде разработки Visual Studio 2019.

На рисунке 2 представлен результат моделирования 1000 траекторий при следующих заданных значениях: $T = 10, n = 100, \lambda = 5, \mu = 5$.

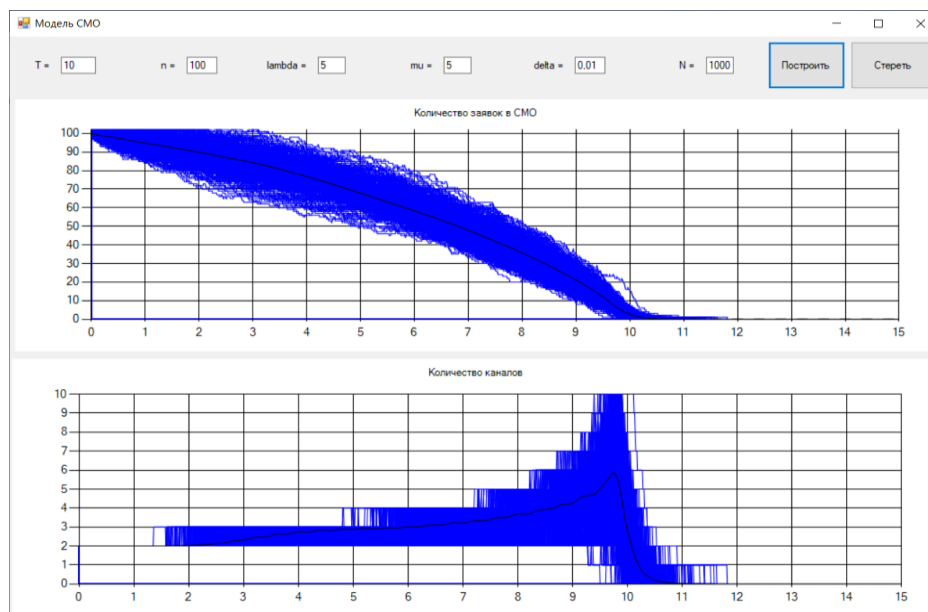


Рисунок 2. - Результат моделирования

Результат моделирования показывает, что система корректно справляется со своими функциями и стремится закончить свою работу в момент времени T . Количество каналов изменяется в соответствии с нагрузкой.

Для сравнительного анализа проведем второе моделирование, в котором увеличим в двое стартовый пул заявок в количестве n (Рисунок 3).

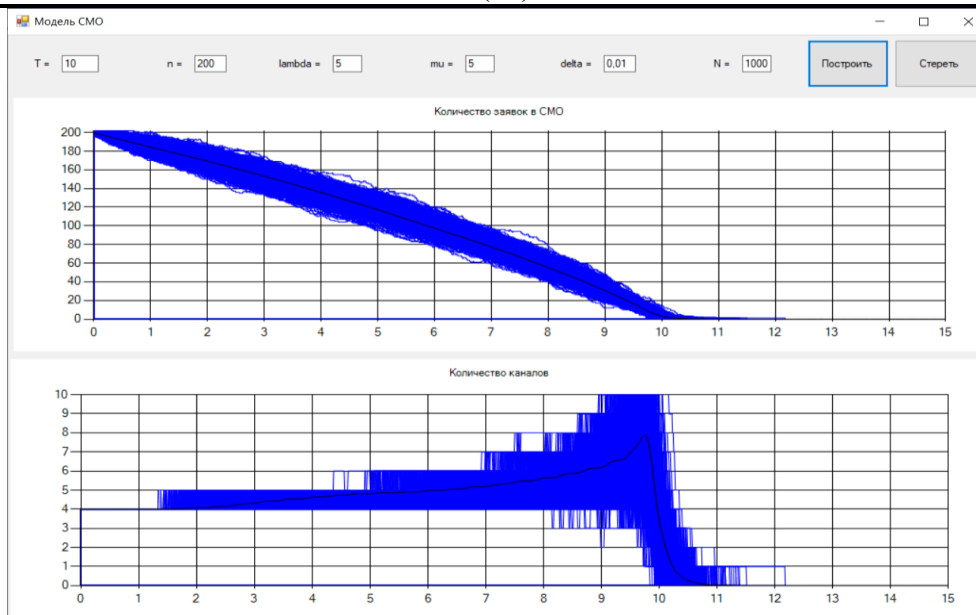


Рисунок 3. - Результат моделирования при увеличении n

Серия экспериментов показывает, что модель справляется с поставленными задачами не зависимо от стартовых значений.

Заключение

В результате выполнения данной работы была построена математическая модель системы массового обслуживания *почти-точно-в-срок* в семимартингальных терминах. Показан переход от математической модели к итерационным формулам. Проведено имитационное моделирование, показывающее возможность оценки отклонения реального времени остановки системы от заданного.

Список литературы

1. Butov A.A., Kovalenko A.A. Stochastic models of simple controlled systems just-in-time // Вестник Самарского государственного технического университета. Серия: Физикоматематические науки. 2018, т. 22, №. 3, с. 518-531.
2. Бутов А.А. Оценивание параметров распределенных продуктивных систем, работающих по принципу «точно в срок» // Автомат. и телемех. 2020, № 3, с.14–27.
3. Бородин А.Н. Случайные процессы: Учебник. Спб.: Изд-во «Лань», 2013.
4. Бутов, А.А. Теория случайных процессов: учеб. пособие / А.А. Бутов, К.О. Раводин. Ульяновск: УлГУ, 2009. 62 с.
5. Бутов, А.А. Теория случайных процессов и её дополнительные главы: учеб. пособие. Ч. 1. Введение в стохастическое исчисление. Ульяновск : УлГУ, 2016. – 48 с

References

1. Butov A.A., Kovalenko A.A. Stochastic models of simple controlled systems just-in-time // Bulletin of the Samara State Technical University. Series: Physical and Mathematical Sciences. 2018, vol. 22, No. 3, pp. 518-531.

2. Butov A.A. Estimation of parameters of distributed productive systems operating on the principle of "just in time" // Automaton. and telemech. 2020, No. 3, pp.14-27.
 3. Borodin A.N. Random processes: Textbook. St. Petersburg: Publishing house "Lan", 2013.
 4. Butov, A.A. Theory of random processes : textbook. the manual / A.A. Butov, K.O. Ravodin. Ulyanovsk: UISU, 2009. 62 p.
 5. Butov, A.A. Theory of random processes and its additional chapters: textbook. manual. Part 1. Introduction to stochastic calculus. Ulyanovsk : UISU, 2016. – 48 p.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.65

ПРИМЕНЕНИЕ VLAN В СЕТЯХ CISCO: ЭФФЕКТИВНОСТЬ И НАСТРОЙКА

Овсянников Р.Я.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: rovsyannikov23@gmail.com

Развитие сетевых технологий требует глубокого понимания способов коммутации пакетов. Эта статья рассматривает применение технологии VLAN в сетях Cisco. Мы исследуем основные преимущества использования VLAN, такие как повышение безопасности, улучшение производительности и оптимизация управления сетью. Кроме того, обсуждаются методы настройки VLAN в устройствах Cisco, включая конфигурацию интерфейсов, создание VLAN и присвоение портов VLAN.

Ключевые слова: VLAN, сети CISCO, безопасность сети, оптимизация производительности, настройка VLAN.

USING VLANS IN CISCO NETWORKS: EFFICIENCY AND CONFIGURATION

Ovsyannikov R.Ya.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: rovsyannikov23@gmail.com

The advancement of networking technologies demands a deep understanding of packet switching methods. This article explores the application of VLAN technology in Cisco networks. We delve into the key benefits of VLAN implementation, such as enhanced security, improved performance, and network management optimization. Additionally, methods for configuring VLANs on Cisco devices are discussed, including interface configuration, VLAN creation, and port assignment.

Keywords: VLAN, CISCO networks, network security, performance optimization, VLAN configuration.

Введение

В современном мире, где информация является основным ресурсом, сети становятся жизненно важной составляющей бизнес-инфраструктуры. Однако с ростом объема данных и разнообразия сетевых устройств возникают новые вызовы, связанные с эффективным управлением трафиком и обеспечением безопасности.

Виртуальные локальные сети (VLAN) являются одним из инструментов, которые помогают решить эти проблемы. VLAN позволяют разбить сеть на логические сегменты, что обеспечивает более гибкое управление трафиком и повышает безопасность путем изоляции групп устройств.

В этой статье мы сосредоточимся на роли и применении VLAN в сетях Cisco. Мы рассмотрим, как VLAN могут помочь в повышении эффективности сети, улучшении безопасности и обеспечении более простого управления ресурсами сети. Кроме того, мы рассмотрим методы настройки и управления VLAN на оборудовании Cisco, чтобы

предоставить читателям практические знания, необходимые для эффективного использования этой технологии.

Глубокое понимание концепций VLAN и их применение в контексте сетей Cisco поможет сетевым администраторам и инженерам создать более надежные и безопасные сетевые инфраструктуры, которые соответствуют требованиям современного бизнеса.

Основные концепции VLAN в сетях Cisco: Исследование и применение

Сетевые технологии продолжают эволюционировать, и виртуальные локальные сети (VLAN) остаются одним из ключевых инструментов для эффективного управления сетевым трафиком и обеспечения безопасности. В этой статье мы глубже погрузимся в основные концепции VLAN в контексте сетей Cisco, рассмотрим их принцип работы, преимущества и ограничения.

1. Определение VLAN (Virtual LAN):

Виртуальные локальные сети (VLAN) представляют собой метод логического разбиения физической сети на отдельные виртуальные сегменты. Это позволяет группировать устройства на основе различных критериев, таких как функциональная принадлежность или безопасность.

2. Принцип работы VLAN:

В сетях Cisco VLAN создаются программным образом на коммутаторах. Каждая VLAN имеет свой уникальный идентификатор (VLAN ID), который указывает коммутатору, к какой VLAN принадлежит каждый порт. Трафик в пределах одной VLAN остается внутри этой VLAN, что обеспечивает изоляцию и безопасность.

3. Преимущества VLAN:

Повышение безопасности: VLAN позволяют изолировать трафик между различными сегментами сети, снижая риск несанкционированного доступа.

Оптимизация производительности: Группировка устройств схожей функциональности в одну VLAN помогает оптимизировать трафик и управлять его потоками более эффективно.

Улучшение управления ресурсами: Администраторы могут легко управлять и настраивать трафик в каждой VLAN, облегчая администрирование сети.

4. Недостатки и ограничения VLAN:

Ограничение размера сети: Большие сети могут столкнуться с ограничением на количество доступных VLAN или максимальное количество устройств в одной VLAN.

Сложность конфигурации: Неправильная настройка VLAN может привести к непредсказуемому поведению сети или потере связности.

Несовместимость устройств: Некоторые старые или дешевые устройства могут не поддерживать работу с VLAN, что усложняет интеграцию сетевого оборудования.

Понимание основных концепций VLAN помогает сетевым администраторам создавать более безопасные, эффективные и управляемые сетевые инфраструктуры в сетях Cisco.

Применение VLAN в сетях Cisco: Преимущества и особенности настройки

Применение виртуальных локальных сетей (VLAN) в сетях Cisco предоставляет ряд значимых преимуществ и представляет собой ключевой аспект сетевой архитектуры. В этом разделе мы подробнее рассмотрим, как VLAN могут быть эффективно использованы в сетях Cisco, а также обсудим особенности и методы их настройки.

1. Улучшение безопасности сети:

Применение VLAN позволяет физически разделить сеть на логические сегменты. Это способствует повышению безопасности, так как трафик между VLAN может быть ограничен, что затрудняет несанкционированный доступ к данным.

2. Оптимизация производительности:

Группировка устройств схожей функциональности в одну VLAN позволяет оптимизировать трафик. Это улучшает производительность сети, так как трафик может быть направлен более эффективно, а нагрузка на сетевое оборудование распределяется равномерно.

3. Управление трафиком и ресурсами сети:

Настройка VLAN на оборудовании Cisco обеспечивает гибкость управления трафиком и ресурсами. Администраторы могут легко изменять конфигурацию VLAN, добавлять или удалять устройства из VLAN, а также применять политики безопасности и качества обслуживания (QoS) для каждой VLAN.

4. Методы настройки VLAN на оборудовании Cisco:

Конфигурация интерфейсов для VLAN: Администраторы могут назначать определенные порты коммутатора определенной VLAN, определяя их членство в VLAN.

Создание VLAN и присвоение портов: С помощью командной строки или графического интерфейса администраторы могут создавать новые VLAN и назначать им порты коммутатора.

Применение методов маршрутизации между VLAN: Для обеспечения связности между VLAN может потребоваться настройка маршрутизатора или многоуровневого коммутатора.

Внимательное понимание этих аспектов позволяет сетевым специалистам эффективно использовать и настраивать VLAN в сетях Cisco, обеспечивая оптимальную производительность, безопасность и управляемость сети.

Примеры использования VLAN в реальных сценариях

В данном разделе мы рассмотрим конкретные сценарии применения виртуальных локальных сетей (VLAN) в реальных сетевых средах. Эти примеры помогут наглядно продемонстрировать, как VLAN могут быть использованы для решения различных задач и повышения эффективности сети.

1. Сегментация сети в офисной среде:

Предприятия могут использовать VLAN для сегментации офисной сети на отдельные логические группы в зависимости от отделов или функциональных областей. Например, отдел маркетинга, отдел продаж и отдел разработки могут быть помещены в разные VLAN, что обеспечит изоляцию и безопасность данных каждого отдела.

2. Разграничение трафика в центрах обработки данных:

В центрах обработки данных (ЦОД) VLAN используются для разграничения трафика между серверами, хранилищами данных и другими устройствами. Например, разные типы трафика, такие как трафик пользователей, трафик приложений и трафик хранилищ, могут быть помещены в разные VLAN для упрощения управления и обеспечения высокой производительности.

3. Развитие гибридных сетей с использованием VLAN:

В сетях общего пользования, таких как университетские сети или открытые Wi-Fi сети, VLAN могут использоваться для разделения трафика различных пользователей или групп

пользователей. Например, гостевой трафик может быть помещен в отдельную VLAN с ограниченным доступом к ресурсам основной сети, обеспечивая безопасность и соблюдение политик безопасности.

Эти примеры иллюстрируют широкий спектр сценариев использования VLAN в реальных сетевых средах. Понимание и умение применять VLAN в соответствии с конкретными потребностями и требованиями бизнеса позволяют создавать гибкие, безопасные и высокопроизводительные сетевые инфраструктуры.

Итоги и перспективы

В данной статье мы рассмотрели ключевые аспекты применения виртуальных локальных сетей (VLAN) в сетях Cisco. От определения VLAN и принципов их работы до конкретных примеров использования в реальных сценариях, мы обсудили, как VLAN могут быть эффективно использованы для повышения безопасности, оптимизации производительности и управления ресурсами сети.

Важно понимать, что VLAN - это не просто технология разделения сети, но и мощный инструмент для организации и управления сетевой инфраструктурой. Правильное применение VLAN позволяет создавать гибкие, масштабируемые и безопасные сети, соответствующие потребностям современного бизнеса.

Надеемся, что данная статья помогла вам лучше понять концепцию VLAN и их применение в сетях Cisco. С учетом быстрого развития сетевых технологий, понимание VLAN становится все более важным для сетевых администраторов и инженеров.

Список литературы

1. Зимин А. Е., Косов Н. А. Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). – 2017. – С. 343-348.
2. Кибирев М. П., Миняев А. А., Скорых М. А. СРАВНИТЕЛЬНЫЙ АНАЛИЗ УТИЛИТ ДЛЯ ПРОВЕДЕНИЯ АТАКИ РТН //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 710-715.
3. Ковцур М. М. и др. Исследование способов удаленного перехвата трафика в корпоративных сетях //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия. – 2021. – Т. 1. – С. 68-75.
4. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.5.
5. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.

References

1. Zimin A. Ye., Kosov N. A. "Ensuring information security in the process of creating and using software for computers" //Actual Problems of Infocommunications in Science and Education (APINO 2017). – 2017. – pp. 343-348.

2. Kibirev M. P., Minyaev A. A., Skorikh M. A. "Comparative analysis of utilities for conducting PTH attack" //Actual Problems of Infocommunications in Science and Education (APINO 2023). – 2023. – pp. 710-715.
 3. Kovtsur M. M. et al. "Research on ways to remotely intercept traffic in corporate networks" //Bulletin of St. Petersburg State University of Technology and Design. Series. – 2021. – Vol. 1. – pp. 68-75.
 4. Krasov A. V. et al. "Packet switching methods in CISCO networks" //Materials of the All-Russian scientific and practical conference "National Security of Russia: Current Aspects" GNI "National Development". July 2018. – 2018. – pp. 31-35.
 5. Petrova T. V. et al. "Approaches to detecting a malicious wireless access point in a local computing network" //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.6

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ФИНИТНО-ВРЕМЕННОГО С ОБРАТНОЙ СВЯЗЬЮ И СПЕКТРАЛЬНО-ФИНИТНОГО БЕЗ ОБРАТНОЙ СВЯЗИ МЕТОДОВ ОБРАБОТКИ ИЗМЕРИТЕЛЬНОЙ ИНФОРМАЦИИ

Иванов Ю.П., ¹Красненков Н.С.

ФГАОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ", Санкт-Петербург, Россия (190000, город Санкт-Петербург, Большая Морская ул., д.67 лит. а), e-mail: ¹nikita.krasnenkov@gmail.com

В настоящей статье проводится сравнительный анализ двух альтернативных методов фильтрации Калмана: оптимальной финитно-временной фильтрации с обратной связью и спектрально-финитной фильтрации без обратной связи. Анализ охватывает оценку точности, робастности и помехозащищенности каждого метода с целью определения наиболее рационального подхода к обработке сигналов в контексте заданной модели измерения.

Ключевые слова: Финитно-временная обработка, спектрально-финитная обработка, обратная связь, робастность, помехозащищенность, точность.

COMPARATIVE ANALYSIS OF FINITE-TIME FEEDBACK AND SPECTRAL-FINITE NON-FEEDBACK MEASUREMENT PROCESSING METHODS

Ivanov Yu.P., ¹Krasnenkov N.S.

ST. PETERSBURG STATE UNIVERSITY OF AEROSPACE INSTRUMENTATION, St. Petersburg, Russia (190000, St. Petersburg, Bolshaya Morskaya str., 67 lit. a), e-mail: ¹nikita.krasnenkov@gmail.com

This paper presents a comparative analysis of two alternative Kalman filtering methods: optimal finite-time filtering with feedback and spectral-finite filtering without feedback. The analysis covers the assessment of the accuracy, robustness and noise immunity of each method in order to determine the most rational approach to signal processing in the context of a given measurement model.

Keywords: Finite-time processing, spectral-finite processing, feedback, robustness, noise immunity, accuracy.

Введение

В настоящее время существуют различные методы обработки сигналов, являющиеся альтернативами фильтрации Калмана, традиционно считающейся наилучшей обработкой в классе линейных оценок [1, 2]. Такие методы нацелены на устранение ряда недостатков, присущих Калмановской фильтрации [3].

В данной статье рассмотрим такие альтернативные методы фильтрации, как новый финитно-временной с обратной связью метод оптимальной оценки измерительной информации на основе теоремы ортогонального проецирования и спектрально-финитный метод обработки без обратной связи.

Оба метода обладают рядом преимуществ и особенностей, вследствие чего возникает необходимость проведения сравнительного анализа альтернативных способов фильтрации сигналов.

Финитно-временной метод фильтрации с обратной связью

Финитно-временной метод обработки сигналов с обратной связью, обладает универсальностью по отношению к коррелированным и некоррелированным ошибкам моделей измерения [4]. Данный метод обеспечивает оптимальную оценку по среднеквадратичной ошибки на заданном временном отрезке. Он характеризуется простотой реализации алгоритмов, не требует представления сигналов в пространстве состояний и демонстрирует точность, эквивалентную фильтру Калмана.

Оптимальная финитно-временная обработка с обратной связью определяется из следующих соотношений [4]:

1. Модель измерения, которая подается на вход фильтра финитно-временной обработки с обратной связью:

$$Y_i = X_i + N_i, i=1,2,...,n, \quad (1)$$

где Y_i – результат измерений в момент времени i ; X_i – оцениваемый дискретный сигнал.

2. Вектор полезного сигнала, размерности $r \times 1$:

$$X1_i = [X_i, X_{i-1}, \dots, X_{i-r+1}]^T, \quad (2)$$

3. Вектор оценки полезного сигнала, размерности $r \times 1$:

$$Z1_i = [Y_i, \hat{X}_{i-1}^*, \dots, \hat{X}_{i-r+1}^*]^T, \quad (3)$$

где $Y_i, i=1,2,...,n$ – текущий результат измерений; $\hat{X}_p^*, p=i-1, i-2, \dots, i-r+1$ – оптимальные оценки сигнала, полученные в $r-1$ моменты времени.

4. Оптимальные оценки полезного сигнала:

$$\hat{X}1_i^* = A_i^* \cdot Z1_i + \hat{X}n1_i, \quad (4)$$

где $\hat{X}n1_i$ – вектор несмещенных оценок.

5. Вектор оптимальных оценок, размерности $r \times 1$:

$$\hat{X}1_i^* = [\hat{X}_i^*, \hat{X}1_{i-1}^*, \dots, \hat{X}_{i-r+1}^*]^T, \quad (5)$$

6. Корреляционная матрица A_i размерностью $r \times r$ преобразующая вектор результатов измерения в вектор оценок $\hat{X}1_i^*$:

$$A_i^* = Kx1_i z1_i \times Kz1_i^{-1}, \quad (6)$$

где $Kx1_i z1_i$ – матрица взаимных корреляционных моментов для векторных сигналов $X1_i$ и выходного сигнала $Z1_i$ размерности $r \times r$; $Kz1_i$ – матрица корреляционных моментов входного сигнала $Z1_i$, размерности $r \times r$.

7. Вектор несмещенных оценок:

$$\begin{aligned} \hat{X}n1_i &= [I - A_i^*] \cdot M[X1_i] - A_i^* \cdot M[H1_i], \\ i &= r, r+1, \dots, n. \end{aligned} \quad (7)$$

где $M[X1_i]^T = \{M[X_i], M[X_{i-1}], \dots, M[X_{i-r+1}]\}$ – математическое ожидание вектора $X1_i$; $M[H1_i]^T = [M[H_i], M[E_{i-1}^*], \dots, M[E_{i-r+1}^*]]$ – математическое ожидание, состоящие из помехи $H1_i$ и ошибки оптимальной оценки $M[E_k^*], k=i-1, i-2, \dots, i-r+1$.

Спектрально-финитный метод фильтрации без обратной связью

Спектрально-финитная линейная оптимальная фильтрация дискретных сигналов характеризуется универсальностью применения [5]. Она применима для обработки как стационарных, так и нестационарных сигналов, как марковских, так и немарковских процессов, не зависит от наличия или отсутствия коррелированной помехи измерения. Данный алгоритм отличается повышенной устойчивостью благодаря отсутствию обратной связи, а также простотой реализации. Несмотря на это, спектрально-финитная фильтрация уступает по точности фильтрации Калмана.

Спектрально-финитная обработка без обратной связью определяется из следующих соотношений [5]:

1. Спектральное представление наблюдаемого сигнала сигнал $Y1_i$ в спектральном виде на i -ом интервале, размерности $d_i \times 1$, учитывая величину значения спектральных компонент d_i , записывается в следующем виде:

$$CY1d_i = BB1_i^T * Y1_i, i = k, k + 1, \dots, N, \quad (8)$$

где $BB1_i$ – матрица собственных векторов матрицы $Kx1_i$ на i -ом шаге оценки сигнала.

2. Корреляционная матрица $Kx1_i$ на i -ом интервале в спектральном представлении, размерности $d_i \times d_i$ определяется следующим образом:

$$CKx1d_i = BB1_i^T * Kx1_i * BB1_i, \quad (9)$$

3. Корреляционная матрица $Ky1_i$ в спектральном представлении, размерности $d_i \times d_i$ определяется в следующем виде:

$$CKy1d_i = BB1_i^T * Ky1_i * BB1_i, \quad (10)$$

4. Корреляционная матрица $Kx1y1_i$ векторов $X1_i$ и $Y1_i$ в спектральном представлении, размерности $d_i \times d_i$, которая учитывает величину значения спектральных компонент d_i :

$$CKx1y1d_i = BB1_i^T * Kx1y1_i * BB1_i, \quad (11)$$

5. Матрица оптимальных коэффициентов полезного сигнала $X1_i$ в i -ый момент времени, размерности $d_i \times d_i$, при спектральном представлении имеет следующий вид:

$$CA d_i^* = CKx1y1d_i \times CKy1d_i^{-1}, \quad (12)$$

6. Матрица, которая определяет во временной области оператор оптимального оценивания вектора $X1_i$ в i -ый момент времени, размерность которого $k \times k$, и с учетом величины значения спектральных компонент d_i :

$$Ad_r^* = BB1_i * CA d_i^* * BB1_i^T, \quad (13)$$

Сравнительный анализ финитно-временного метода обработки с обратной связью и спектрально-финитного метода обработки без обратной связи

Сравнительный анализ рассмотрим на примере следующей модели измерения, как частного случая: $Y_i = X_i + N_i$, $i = 1, 2, \dots, n$, где Y_i , X_i и N_i – стационарные, гауссовские, эргодические, центрированные, случайные процессы.

Моделирование проводилось по следящим исходным данным:

- Корреляционная функция полезного сигнала первого порядка марковости:

$$KX(\tau) = \sigma X^2 \cdot e^{-\alpha X \cdot |\tau|};$$

- Вид погрешности – коррелированный случайный процесс;

- Среднеквадратическое отклонение: $\sigma = 1$;
- Параметры робастности и помехозащищенности: $\alpha = \alpha_1 = 0,01 \frac{1}{c}$, $\beta_2 = \beta_{21} = 0,1 \frac{M}{c}$;
- СКО помехи и полезного сигнала для робастности и помехозащищенности:
 $SIG0 = SIG1 = SIG00 = SIG11 = 1$;
- Используемая память фильтра финитно-временной обработки: $r = 4$
- Дискрет, определяемый по теореме Котельникова: $d = 4$ с;
- Объем выборки: $N = 2000$.

Моделирование проводилось в компьютерном математическом пакете MathCad [6].

В ходе моделирования методов обработки информации, после завершения переходных процессов, были получены статистические оценки дисперсии, которые характеризуют точность финитно-временного метода обработки с обратной связью (ФВОсОС) и спектрально-финитного метода обработки без обратной связи (СФО).

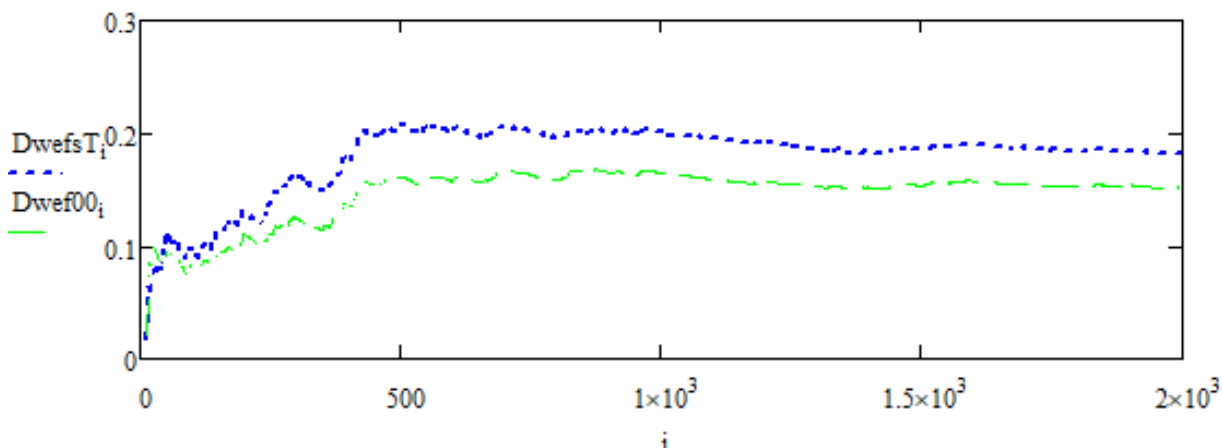


Рисунок 1. - График зависимости дисперсий ошибок оценок исследуемых методов обработки полезного сигнала от выборки. Dwef00 – дисперсия ошибки оценки полезного сигнала ФВОсОС; Dwefts – дисперсия ошибки оценки полезного сигнала СФО.

Источник: анализ автора

Определим точность и времена переходных процессов исследуемых методов обработки в численном виде на конце интервала.

Таблица 1. - Значения точности и времени переходного процесса исследуемых методов обработки.

	ФВОсОС	СФО
Точность	0,152	0,182
Время ПП, с	974	1001

Источник: анализ автора

Сравнение на робастность будем проводить по следующим параметрам: r , d , α , β_2 , $SIG0$, $SIG1$. Ниже представим числовые данные робастности при отклонении заданного параметра

робастности на $\pm 10\%$. Где Rob00 – значение робастности финитно-временной обработки с обратной связью, RobsT – значение робастности спектрально-финитной обработки без обратной связи. Будем называть систему робастной, когда хотя бы один коэффициент робастности окажется меньше определенного значения, равного 0,3 [7].

Определим робастность финитно-временной обработки с обратной связью и спектрально-финитной обработки без обратной связи по:

Параметру памяти фильтра – r:

$$\text{Rob00}(-) = 0,112; \text{Rob00}(+) = 0,266$$

$$\text{RobsT}(-) = 0,188; \text{RobsT}(+) = 0,013$$

По параметру дискрета – d:

$$\text{Rob00}(-) = 0,195; \text{Rob00}(+) = 0,035$$

$$\text{RobsT}(-) = 0,047; \text{RobsT}(+) = 0,138$$

По параметру – α :

$$\text{Rob00}(-) = 0,121; \text{Rob00}(+) = 0,316$$

$$\text{RobsT}(-) = 0,249; \text{RobsT}(+) = 0,337$$

По параметру – β_2 :

$$\text{Rob00}(-) = 0,058; \text{Rob00}(+) = 0,079$$

$$\text{RobsT}(-) = 0,075; \text{RobsT}(+) = 0,045$$

По параметру СКО ошибки – SIG0:

$$\text{Rob00}(-) = 0,811; \text{Rob00}(+) = 0,909$$

$$\text{RobsT}(-) = 0,786; \text{RobsT}(+) = 0,742$$

По параметру СКО полезного сигнала – SIG1:

$$\text{Rob00}(-) = 0,336; \text{Rob00}(+) = 0,06$$

$$\text{RobsT}(-) = 0,159; \text{RobsT}(+) = 0,147$$

Сравнение на помехозащищенность будем проводить по следующим параметрам: α_1 , β_2 , SIG00, SIG11. Ниже представим числовые данные помехозащищенности при отклонении заданного параметра помехи на $\pm 10\%$. Где Pom00 – значение помехозащищенности финитно-временной обработки с обратной связью, PomsT – значение помехозащищенности спектрально-финитной обработки без обратной связи. Будем называть систему помехозащищенной, когда хотя бы один коэффициент помехозащищенности окажется меньше определенного значения, равного 0,3 [7].

Определим помехозащищенность финитно-временной обработки с обратной связью и спектрально-финитной обработки без обратной связи по:

По параметру – α_1 :

$$\text{Pom00}(-) = 0,59; \text{Pom00}(+) = 0,188$$

$$\text{PomsT}(-) = 0,673; \text{PomsT}(+) = 0,31$$

По параметру – β_2 :

$$\text{Rob00}(-) = 0,093; \text{Rob00}(+) = 0,25$$

$$\text{PomsT}(-) = 0,187; \text{PomsT}(+) = 0,153$$

По параметру СКО ошибки – SIG00:

$$\text{Pom00}(-) = 1,392; \text{Pom00}(+) = 2,538$$

$$\text{PomsT}(-) = 1,379; \text{PomsT}(+) = 2,489$$

По параметру СКО полезного сигнала – SIG11:

$$\text{Pom00}(-) = 0,778; \text{Pom00}(+) = 1,439$$

$$\text{PomsT}(-) = 0,928; \text{PomsT}(+) = 1,721$$

Заключение

В данной работе был проведен сравнительный анализ линейных оптимальных методов фильтрации, являющихся альтернативами Калмановской фильтрации: финитно-временного метода с обратной связью и спектрально-финитного метода без обратной связи, по показателям точности, робастности и помехозащищенности.

По показателю точности финитно-временная фильтрация с обратной связью оказалась точнее, а время ее переходного процесса меньше.

По показателю робастности финитно-временная фильтрация с обратной связью обладает робастностью по параметрам: g , d , α , β_2 , $SIG1$. Спектрально-финитная фильтрация без обратной связи обладает робастностью по параметрам: g , d , α , β_2 , $SIG1$.

По показателю помехозащищенности финитно-временная фильтрация с обратной связью обладает помехозащищенностью по параметрам: α , β_2 . Спектрально-финитная фильтрация без обратной связи обладает помехозащищенностью по параметру: β_2 .

Таким образом, можно сделать вывод, что из двух альтернативных методов фильтрации Калмана наиболее точным оказался финитно-временной фильтр с обратной связью. По показателю робастности оба фильтра являются робастны. По показателю помехозащищенности финитно-временной фильтр более помехоустойчив.

Список литературы

1. Э. Сейдж, Дж. Мелс. Теория оценивания и ее применение в связи и управления. Связь. М. 1976, 495 с.
2. Медич Дж. Статистически оптимальные линейные оценки и управление. М. 1973, Энергия, 440 с.
3. Иванов Ю. П. Рекуррентный оптимальный метод фильтрации произвольных дискретных сигналов на фоне коррелированных помех измерения. Моделирование и ситуационное управление качеством сложных систем // Сборник докладов Третьей Всероссийской научной конференции. Санкт-Петербург. 2022. С. 27-32
4. Иванов Ю. П. Финитно-временной и спектрально-финитный методы оптимальной фильтрации дискретных сигналов // Морские интеллектуальные технологии. 2021. №3-1 (53). С. 154-160.
5. Иванов Ю. П. Спектрально-финитный метод оптимальной линейной фильтрации сигналов / Ю. П. Иванов. – Текст : электронный // Аэрокосмическое приборостроение и эксплуатационные технологии. – Сборник докладов Первой Международной научной конференции. – Санкт-Петербург, 2020. – С. 35-41.
6. Новиковский, Е. А. Учебное пособие «Работа в системе MathCAD» [Текст] / Е. А. Новиковский. – Барнаул: Типография АлтГТУ, 2013. – 114 с.
7. Иванов Ю. П., Никитин В. Г. Информационно-статистическая теория измерений. Методы оптимального синтеза информационно-измерительных, критерии оптимизации и свойства оценок. Учебное пособие. СПГУАП, С П. 2011. 102 с.

References

1. E. Sage, J. Mels. Evaluation theory and its application in communication and management. Svyaz. M. 1976, p. 495
2. Medich J. Statistically optimal linear estimates and control. M. 1973, Energiya, 440 p.
3. Ivanov Yu. P. Recurrent optimal method of filtering arbitrary discrete signals against the background of correlated measurement interference. Modeling and situational quality management of complex systems // Collection of reports of the Third All-Russian Scientific Conference. St. Petersburg. 2022. C. 27-32
4. Ivanov Yu. P. Finite-time and spectral-finite methods of optimal filtering of discrete signals // Marine intelligent technologies. 2021. No.3-1 (53). pp. 154-160.

5. Ivanov Yu. P. Spectral-finite method of optimal linear signal filtering / Yu. P. Ivanov. – Text : electronic // Aerospace instrumentation and operational technologies. – Collection of reports of the First International Scientific Conference. – St. Petersburg, 2020. – pp. 35-41.
 6. Novikov, E. A. Textbook "Work in the MathCAD system" [Text] / E. A. Novikov. Barnaul: Printing house of AltSTU, 2013. p.114
 7. Ivanov Yu. P., Nikitin V. G. Information and statistical theory of measurements. Methods of optimal synthesis of information and measurement, optimization criteria and evaluation properties. A study guide. SPGUAP, From p. 2011. p. 102
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.6

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СПЕКТРАЛЬНО-ФИНИТНОГО БЕЗ ОБРАТНОЙ СВЯЗИ МЕТОДА ОБРАБОТКИ ИЗМЕРИТЕЛЬНОЙ ИНФОРМАЦИИ И ФИЛЬТРА КАЛМАНА

Иванов Ю.П., ¹Красненков Н.С.

ФГАОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ", Санкт-Петербург, Россия (190000, город Санкт-Петербург, Большая Морская ул., д.67 лит. а), e-mail: ¹nikita.krasnenkov@gmail.com

В данном исследовании проводится сравнительный анализ характеристик спектрально-финитной фильтрации без обратной связи и фильтра Калмана для дискретных сигналов по точности, робастности и помехозащищенности. Цель сравнительного анализа сводится к установлению более точного и оптимального метода фильтрации измерительной информации относительно выбранной модели измерения.

Ключевые слова: Спектрально-финитная обработка, фильтр Калмана, фильтрация, робастность, помехозащищенность, точность.

COMPARATIVE ANALYSIS OF THE SPECTRAL-FINITE METHOD OF PROCESSING MEASUREMENT INFORMATION WITHOUT FEEDBACK AND THE KALMAN FILTER

Ivanov Yu.P., ¹Krasnenkov N.S.

ST. PETERSBURG STATE UNIVERSITY OF AEROSPACE INSTRUMENTATION, St. Petersburg, Russia (190000, St. Petersburg, Bolshaya Morskaya str., 67 lit. a), e-mail: ¹nikita.krasnenkov@gmail.com

In this study, a comparative analysis of the characteristics of spectral-finite filtering without feedback and the Kalman filter for discrete signals in terms of accuracy, robustness and noise immunity is carried out. The purpose of the comparative analysis is to establish a more accurate and optimal method for filtering measurement information relative to the selected measurement model.

Keywords: Spectral-finite processing, Kalman filter, filtration, robustness, noise immunity, accuracy.

Введение

В мире достаточно часто применяют в качестве метода обработки сигналов фильтр Калмана. Такое частое применение обуславливается целым рядом особенностей и преимуществ Калмановской фильтрации перед другими методами обработки [1, 2]. Как бы там ни было, фильтр Калмана так же имеет и ряд недостатков [3].

В качестве альтернативы Калмановской фильтрации, для устранения его недостатков, были придуманы новые методы обработки. К одному из таких методов относится спектрально-финитная обработка без обратной связи.

Оба метода являются линейными, таким образом, возникает необходимость проведения сравнительного анализа по точности, робастности и помехозащищенности с целью установления наиболее рационального метода обработки.

Спектрально-финитный метод фильтрации без обратной связью

Спектрально-финитная линейная оптимальная фильтрация дискретных сигналов характеризуется универсальностью применения [5]. Она применима для обработки как стационарных, так и нестационарных сигналов, как марковских, так и немарковских, не зависит от наличия или отсутствия коррелированной помехи измерения. Данный алгоритм отличается повышенной устойчивостью благодаря отсутствию обратной связи, а также простотой реализации.

Спектрально-финитная обработка без обратной связью определяется из следующих соотношений [5]:

1. Спектральное представление наблюдаемого сигнала сигнал $Y1_i$ в спектральном виде на i -ом интервале, размерности $d_i \times 1$, учитывая величину значения спектральных компонент d_i , записывается в следующем виде:

$$CY1d_i = BB1_i^T * Y1_i, i = k, k + 1, \dots, N, \quad (8)$$

где $BB1_i$ – матрица собственных векторов матрицы $Kx1_i$ на i -ом шаге оценки сигнала.

2. Корреляционная матрица $Kx1_i$ на i -ом интервале в спектральном представлении, размерности $d_i \times d_i$ определяется следующим образом:

$$CKx1d_i = BB1_i^T * Kx1_i * BB1_i, \quad (9)$$

3. Корреляционная матрица $Ky1_i$ в спектральном представлении, размерности $d_i \times d_i$ определяется в следующем виде:

$$CKy1d_i = BB1_i^T * Ky1_i * BB1_i, \quad (10)$$

4. Корреляционная матрица $Kx1y1_i$ векторов $X1_i$ и $Y1_i$ в спектральном представлении, размерности $d_i \times d_i$, которая учитывает величину значения спектральных компонент d_i :

$$CKx1y1d_i = BB1_i^T * Kx1y1_i * BB1_i, \quad (11)$$

5. Матрица оптимальных коэффициентов полезного сигнала $X1_i$ в i -ый момент времени, размерности $d_i \times d_i$, при спектральном представлении имеет следующий вид:

$$CA d_i^* = CKx1y1d_i \times CKy1d_i^{-1}, \quad (12)$$

6. Матрица, которая определяет во временной области оператор оптимального оценивания вектора $X1_i$ в i -ый момент времени, размерность которого $k \times k$, и с учетом величины значения спектральных компонент d_i :

$$Ad_r^* = BB1_i * CA d_i^* * BB1_i^T, \quad (13)$$

Сравнительный анализ спектрально-финитного метода обработки без обратной связи и фильтра Калмана

Сравнительный анализ рассмотрим на примере следующей модели измерения: $Y_i = X_i + N_i$, $i=1,2,\dots,n$, где Y_i , X_i и N_i – стационарные, гауссовские, эргодические, центрированные, случайные процессы.

Моделирование проводилось по следящим исходным данным:

1. Корреляционная функция полезного сигнала второго порядка марковости:

$$KX(\tau) = \sigma X^2 * e^{-\alpha X|\tau|} * (\cos(\beta X|\tau|) + \frac{\alpha}{\beta} * \sin(\beta X|\tau|))$$

2. Вид погрешности – коррелированный случайный процесс;
3. Среднеквадратическое отклонение: $\sigma = 1$;
4. Параметры робастности и помехозащищенности: $\alpha = \alpha_1 = \beta = \beta_1 = 0,01 \frac{1}{c}$,
 $\beta_2 = \beta_{21} = 0,1 \frac{m}{c}$;
5. СКО помехи и полезного сигнала для робастности и помехозащищенности:
 $SIG0 = SIG1 = SIG00 = SIG11 = 1$;
6. Используемая память фильтра финитно-временной обработки: $r = 4$;
7. Дискрет, определяемый по теореме Котельникова: $d = 4$ с;
8. Объем выборки: $N = 2000$.

Моделирование проводилось в компьютерном математическом пакете MathCad [6].

В ходе моделирования методов обработки информации, после завершения переходных процессов, были получены статистические оценки дисперсии, которые характеризуют точность спектрально-финитного метода обработки без обратной связи (СФО) и фильтра Калмана (ФК).

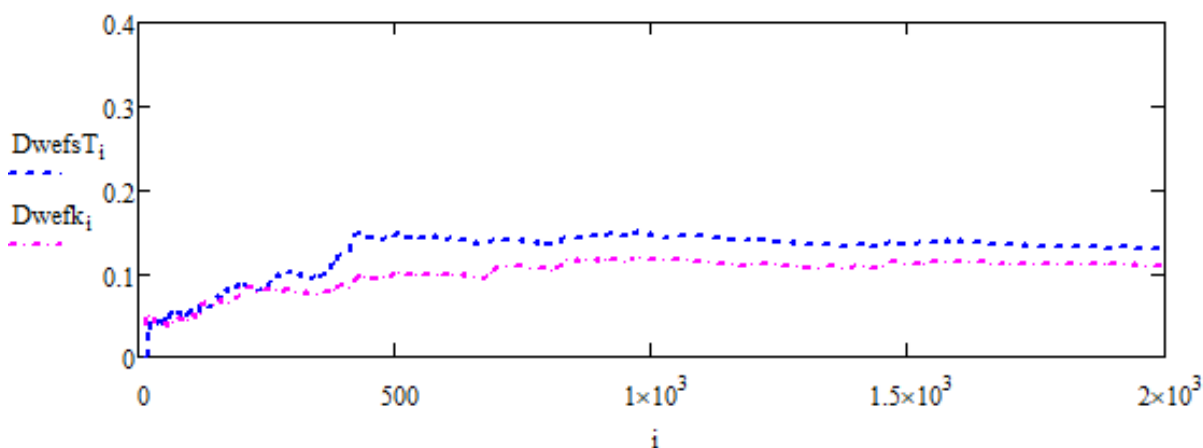


Рисунок 1. - График зависимости дисперсий ошибок оценок исследуемых методов обработки полезного сигнала от выборки. DweftsT – дисперсия ошибки оценки полезного сигнала СФО;
 Dwefk – дисперсия ошибки оценки полезного сигнала ФК.

Источник: анализ автора

Определим точность и времена переходных процессов исследуемых методов обработки в численном виде на конце интервала.

Таблица 1. - Значения точности и времени переходного процесса исследуемых методов обработки.

	СФО	ФК
Точность	0,131	0,111
Время ПП, с	1087	684

Источник: анализ автора

Сравнение на робастность будем проводить по следующим параметрам: r , d , α , β , β_2 , SIG0, SIG1. Ниже представим числовые данные робастности при отклонении заданного параметра робастности на $\pm 10\%$. Где RobsT – значение робастности спектрально-финитной обработки без обратной связи, Robk – значение робастности фильтра Калмана. Будем называть систему робастной, когда хотя бы один коэффициент робастности окажется меньше определенного значения, равного 0,3 [7].

Определим робастность спектрально-финитной обработки без обратной связи и фильтра Калмана по:

Параметру памяти фильтра – r :

RobsT(-) = 0,533; RobsT(+) = 0,276 Robk(-) = 0,313; Robk(+) = 0,569

По параметру дискрета – d :

RobsT(-) = 0,699; RobsT(+) = 0,146 Robk(-) = 0,553; Robk(+) = 0,052

По параметру – α :

RobsT(-) = 0,099; RobsT(+) = 0,064 Robk(-) = 0,048; Robk(+) = 0,048

По параметру – β :

RobsT(-) = 0,04; RobsT(+) = 0,014 Robk(-) = 0,182; Robk(+) = 0,165

По параметру – β_2 :

RobsT(-) = 0,694; RobsT(+) = 0,525 Robk(-) = 0,736; Robk(+) = 0,474

По параметру СКО ошибки – SIG0:

RobsT(-) = 0,599; RobsT(+) = 0,907 Robk(-) = 0,171; Robk(+) = 0,62

По параметру СКО полезного сигнала – SIG1:

RobsT(-) = 0,15; RobsT(+) = 0,254 Robk(-) = 0,104; Robk(+) = 0,208

Сравнение на помехозащищенность будем проводить по следующим параметрам: α_1 , β_1 , β_{21} , SIG00, SIG11. Ниже представим числовые данные робастности при отклонении заданного параметра помехи на $\pm 10\%$. Где PomsT – значение помехозащищенности спектрально-финитной обработки без обратной связи, Pomk – значение помехозащищенности фильтра Калмана. Будем называть систему помехозащищенной, когда хотя бы один коэффициент помехозащищенности окажется меньше определенного значения, равного 0,3 [7].

Определим помехозащищенность спектрально-финитной обработки без обратной связи и фильтра Калмана по:

По параметру – α_1 :

PomsT(-) = 0,346; PomsT00(+) = 0,415 Pomk(-) = 0,468; Pomk(+) = 0,161

По параметру – β_1 :

PomsT(-) = 0,083; PomsT(+) = 0,158 Pomk(-) = 0,041; Pomk(+) = 0,054

По параметру – β_{21} :

PomsT(-) = 0,627; PomsT(+) = 0,653 Pomk(-) = 0,599; Pomk(+) = 0,423

По параметру СКО ошибки – SIG00:

PomsT(-) = 1,529; PomsT00(+) = 2,499 Pomk(-) = 1,539; Pomk(+) = 2,529

По параметру СКО полезного сигнала – SIG11:

PomsT(-) = 1,533; PomsT00(+) = 1,194 Pomk(-) = 0,911; Pomk(+) = 1,234

Заключение

В данной работе был проведен сравнительный анализ линейных оптимальных методов фильтрации: спектрально-финитного метода без обратной связи, являющегося альтернативой Калмановской фильтрации, и самого фильтра Калмана, по показателям точности, робастности и помехозащищенности.

По показателю точности фильтрация Калмана оказалась немного точнее спектрально-финитной фильтрации без обратной связи, при этом время переходного процесса лучше у Калмановской фильтрации.

По показателю робастности спектрально-финитная фильтрация без обратной связи обладает робастностью по параметрам: r , d , α , β , $SIG0$. Калмановская фильтрация обладает робастностью по параметрам: d , α , β , $SIG0$, $SIG1$.

По показателю помехозащищенности спектрально-финитная фильтрация без обратной связи обладает помехозащищенностью по параметру: β_1 . Фильтр Калмана обладает помехозащищенностью по параметрам: α_1 , β_1 .

Таким образом, можно сделать вывод, что из двух методов фильтрации сигналов, фильтрация Калмана оказалась наиболее точна. По показателю робастности оба фильтра являются робастны в равной степени. По показателю помехозащищенности фильтр Калмана является более помехоустойчив.

Список литературы

1. Э. Сейдж, Дж. Мелс. Теория оценивания и ее применение в связи и управления. Связь. М. 1976, 495 с.
2. Медич Дж. Статистически оптимальные линейные оценки и управление. М. 1973, Энергия, 440 с.
3. Иванов Ю. П. Рекуррентный оптимальный метод фильтрации произвольных дискретных сигналов на фоне коррелированных помех измерения. Моделирование и ситуационное управление качеством сложных систем // Сборник докладов Третьей Всероссийской научной конференции. Санкт-Петербург. 2022. С. 27-32
4. Иванов Ю. П. Финитно-временной и спектрально-финитный методы оптимальной фильтрации дискретных сигналов // Морские интеллектуальные технологии. 2021. №3-1 (53). С. 154-160.
5. Иванов Ю. П. Спектрально-финитный метод оптимальной линейной фильтрации сигналов / Ю. П. Иванов. – Текст : электронный // Аэрокосмическое приборостроение и эксплуатационные технологии. – Сборник докладов Первой Международной научной конференции. – Санкт-Петербург, 2020. – С. 35-41.
6. Новиковский, Е. А. Учебное пособие «Работа в системе MathCAD» [Текст] / Е. А. Новиковский. – Барнаул: Типография АлтГТУ, 2013. – 114 с.
7. Иванов Ю. П., Никитин В. Г. Информационно-статистическая теория измерений. Методы оптимального синтеза информационно-измерительных, критерии оптимизации и свойства оценок. Учебное пособие. СПбУАП, С П. 2011. 102 с.

References

1. E. Sage, J. Mels. Evaluation theory and its application in communication and management. Svyaz. M. 1976, p. 495
2. Medich J. Statistically optimal linear estimates and control. M. 1973, Energiya, 440 p.

3. Ivanov Yu. P. Recurrent optimal method of filtering arbitrary discrete signals against the background of correlated measurement interference. Modeling and situational quality management of complex systems // Collection of reports of the Third All-Russian Scientific Conference. St. Petersburg. 2022. С. 27-32
 4. Ivanov Yu. P. Finite-time and spectral-finite methods of optimal filtering of discrete signals // Marine intelligent technologies. 2021. No.3-1 (53). pp. 154-160.
 5. Ivanov Yu. P. Spectral-finite method of optimal linear signal filtering / Yu. P. Ivanov. – Text : electronic // Aerospace instrumentation and operational technologies. – Collection of reports of the First International Scientific Conference. – St. Petersburg, 2020. – pp. 35-41.
 6. Novikov, E. A. Textbook "Work in the MathCAD system" [Text] / E. A. Novikov. Barnaul: Printing house of AltSTU, 2013. p.114
 7. Ivanov Yu. P., Nikitin V. G. Information and statistical theory of measurements. Methods of optimal synthesis of information and measurement, optimization criteria and evaluation properties. A study guide. SPGUAP, From p. 2011. p. 102
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.438.31

РЕАЛИЗАЦИЯ ПРОТОКОЛА АУТЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ С ИСПОЛЬЗОВАНИЕМ МЕТОК

Туртыгин А.А.

*ФГБОУ ВО "УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", Ульяновск, Россия,
(432017, Ульяновская область, город Ульяновск, ул. Льва Толстого, д. 42), e-mail:
alex.mad.turt@gmail.com*

Целью статьи является исследование протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамала. Протокол аутентификации, основанный на асимметричном шифровании с дополнительным свойством нулевого разглашения, позволяет проверяющей стороне убедиться в достоверности некоторого высказывания доказывающей стороны, не допуская при этом утечки информации о секрете. Для обеспечения взаимной аутентификации применяется механизм меток, добавляемых в проверочное сообщение перед его зашифрованием. Использование меток в протоколе аутентификации позволяет снизить нагрузку на вычислительные ресурсы вследствие отказа от традиционно применяемых хеш-функций.

Ключевые слова: Протокол аутентификации; нулевое разглашение; алгоритм Эль-Гамала; серверная аутентификация; клиент-серверное приложение.

IMPLEMENTATION OF ZERO-KNOWLEDGE AUTHENTICATION PROTOCOL USING LABELS

Turtygin A.A.

*ULYANOVSK STATE UNIVERSITY, Ulyanovsk, Russia, (432017, Ulyanovsk region, Ulyanovsk city,
Lva Tolstoy str., 42), e-mail: alex.mad.turt@gmail.com*

The purpose of the paper is to study the zero-knowledge authentication protocol based on the ElGamal cipher. The authentication protocol, based on asymmetric encryption with an additional zero-knowledge property, allows the verifier to check the authenticity of some statement of the prover, while preventing leakage of secret. To ensure mutual authentication, a mechanism of tags is used, which are added to the verification message before its encryption. The use of tags in the authentication protocol reduces the load on computing resources due to the abandonment of traditionally used hash functions.

Keywords: Authentication protocol; zero-knowledge proof; ElGamal algorithm; server authentication; client-server application.

Метки в протоколах аутентификации

В последнее время набирают популярность протоколы аутентификации с нулевым разглашением на основе асимметричного шифрования. В данном случае «нулевое разглашение» говорит об отсутствии утечки какой-либо информации о секретном ключе в процессе обмена сообщениями типа «запрос-ответ» в процессе аутентификации [1]. Причём допускается возможная первоначальная утечка информации о секретном ключе в случае, если злоумышленник предложит владельцу открытого ключа расшифровать поддельное проверочное сообщение M [2].

Такие протоколы должны обеспечивать взаимную аутентификацию, т.е. оба участника по результатам обмена сообщениями в процессе аутентификации получают информацию о возможности доверия к противоположной стороне-участнику.

Односторонние протоколы аутентификации построены на методах зашифрования некоторых сообщений проверяющим, их последующей расшифровке и передаче обратно доказывающей стороной. Такой подход позволяет проверяющей стороне убедиться в подлинности доказывающей, но не наоборот. Проблема возникает в случае, когда вместо проверяющей стороны окажется злоумышленник – он сможет получить информацию о секрете.

Для решения проблемы взаимной аутентификации к зашифрованным сообщениям добавляют хеш-код, полученный в результате работы хеширующей функции от этих сообщений [3], тем самым предотвращая возможность выбора злоумышленником случайного запроса в качестве проверочного. Корректно сформированный запрос от проверяющего участника представляется в виде пары значений: зашифрованного на открытом ключе сообщения и его хеша. При получении этой пары значений в качестве запроса, доказывающий расшифровывает сообщение и вычисляет его хеш. Затем он сравнивает полученный и вычисленный хеши, и убеждается в том, что расшифрованное им сообщение уже было известно проверяющему.

Но применение хеш-функций не является единственным способом каждой из сторон убедиться в правдивости утверждения противоположной стороны. В качестве доказательства того, что переданное сообщение было известно проверяющему до процесса зашифрования, может применяться механизм меток μ , встраиваемых в сообщение [1]. Наличие метки в расшифрованном сообщении позволяет убедиться в том, что проверяющая сторона изначально владела информацией об исходном сообщении. На роль метки при использовании асимметричного шифрования хорошо подходит некоторая часть открытого ключа доказывающей стороны. На практике длина метки ($|\mu|$) в двоичном представлении выбирается от 80 до 512 бит, что позволяет значительно снизить вероятность расшифрования случайного запроса злоумышленника в сообщение с корректной меткой ($P = 2^{-|\mu|}$) [1].

Протокол Эль-Гамала

Схема Эль-Гамала – это криптосистема с открытым ключом, основанная на сложности вычисления дискретных логарифмов в конечном поле [4]. Шифрование в ней – вероятностное, т.е. одинаковое сообщение может быть зашифровано в различные криптограммы, при расшифровании которых всегда получается одно и то же изначальное сообщение.

Рассмотрим протокол аутентификации с нулевым разглашением, использующий асимметричный шифр Эль-Гамала и метку в качестве механизма взаимной аутентификации (Рис. 1). В нашем случае меткой будут являться младшие 160 бит открытого ключа, что говорит о крайне низкой вероятности совпадения меток для случайного запроса ($P = 2^{-160}$).

В качестве открытых (известных обоим участникам) параметров протокола используются p – большое простое число, где $p-1$ содержит простой делитель длиной не менее 160 бит в двоичном исчислении, g – первообразный корень по модулю p , y – открытый ключ доказывающей стороны и μ – метка, где $\mu = y \pmod{2^{160}}$.

Секретный ключ x доказывающая сторона будет хранить в тайне.

Шаги протокола аутентификации можно записать следующим образом:

1. Проверяющая сторона генерирует случайным образом разовый секретный ключ отправителя k и сообщение M со следующим ограничением его длины: $|M| < |p| - |2 * \mu|$.
2. Далее вычисляет разовый открытый ключ отправителя R и разовый общий секретный ключ Q , где $R = g^k \pmod{p}$ и $Q = y^k \pmod{p}$.
3. Затем осуществляет зашифрование битовой строки $M||\mu$, состоящей из сообщения M и метки μ , в число C , где $C = Q * (M||\mu) \pmod{p}$.
4. Проверяющая сторона передаёт доказывающей полученную в предыдущих шагах пару чисел (R, C) .
5. Доказывающая сторона получает значения (R, C) и приступает к вычислению общего секретного ключа $Q = R^x \pmod{p}$ и Q^{-1} (обратного к нему числа по модулю p), используя расширенный алгоритм Эвклида [5].
6. Далее расшифровывает полученную криптограмму C и получает некоторую битовую строку, содержащую в себе сообщение и метку, следующим образом: $M' || \mu' = C * Q^{-1} \pmod{p}$.
7. Затем проверяет равенство вычисленной ранее и расшифрованной меток, если равенство выполняется, то доказывающая сторона отправляет проверяющей значение M' , а в противном случае объявляет запрос некорректным.
8. Проверяющая сторона принимает решение о легитимности доказывающей на основе равенства исходного и полученного сообщений.

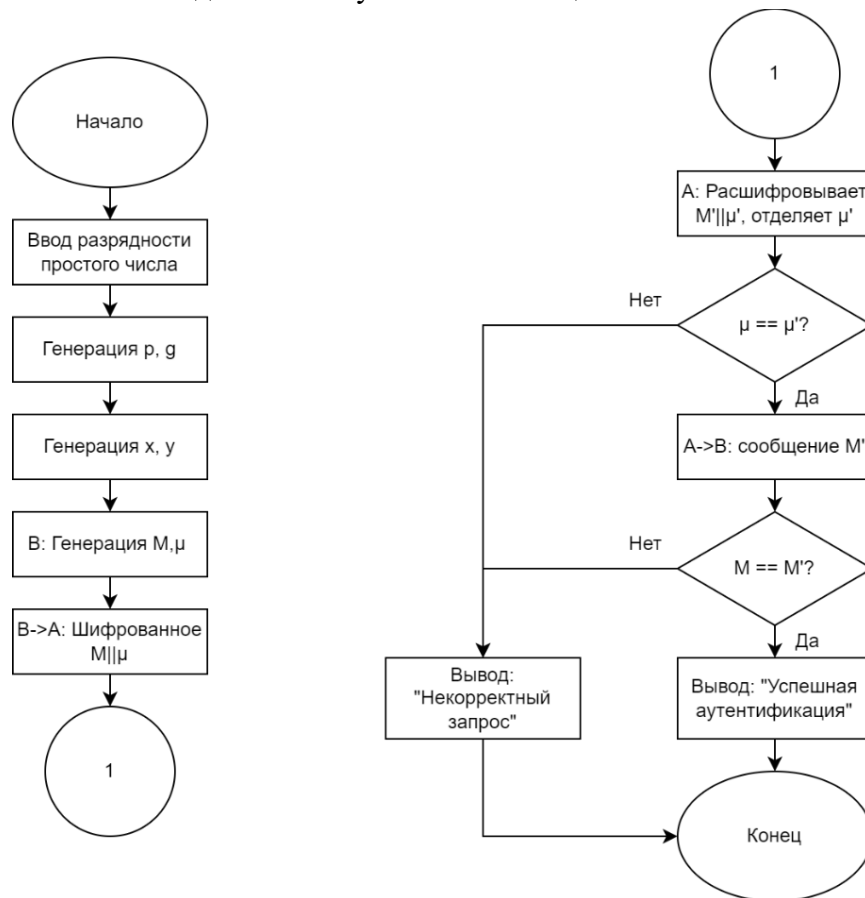


Рисунок 1. - Схема протокола аутентификации

Источник: анализ автора

Реализация протокола

Протокол аутентификации был реализован в виде исполняемого файла для операционных систем семейства Windows на языке программирования Visual C# (.Net Framework 4.7.2). Поскольку размеры стандартных числовых типов в данном языке ограничены 64 битами, а для криптостойкости необходима работа с числами размером, превышающим 1024 бита, было решено использовать тип данных BigInteger.

Все основные методы и функции работают в нескольких потоках, поскольку приложение содержит в себе клиентскую и серверную части – выполнение всех функций обеих частей в одном потоке невозможно по причине постоянных его блокировок. Пример запуска серверных функций во вспомогательных потоках:

```
private void awaitConnectButton_Click(object sender,
EventArgs e)
{
    new Thread(MainServerThread).Start();
}
private void MainServerThread()
{
    Invoke(() => { consoleRichTextBox.Text = "*** Создан
именованный канал ***\n"; });
    Invoke(() => { consoleRichTextBox.Text += "Ожидание
подключения клиентов...\n"; });
    new Thread(ServerThread).Start();
    Thread.Sleep(250);
}

private void newClientWindowOpenButton_Click(object
sender, EventArgs e)
{
    Thread cfT = new Thread(ClientStart);
    cfT.Start();
}
}
```

Основное окно серверной части программы позволяет задать размер числа p , запустить протокол аутентификации и открыть клиентскую часть. Клиентское приложение содержит строку установления связи с сервером и выступает в роли доказывающей стороны.

Межпроцессный обмен информацией в процессе аутентификации происходит посредством именованных каналов. По этим каналам информация передаётся в виде некоторой последовательности байт. Для восстановления чисел из данных последовательностей предложено следующее представление числа:

“длина массива длины” [“массив длины”] [“массив числа”]

Это позволяет передавать числа размерами до $255 \cdot 255 \cdot 8 = 520200$ бит, что достаточно для современных криптосистем. Ниже представлен фрагмент программы, отвечающий за восстановление числа из последовательности байт:

```
private BigInteger GetFromPipe(NamedPipeServerStream
pipe)
{
    // [length of length] [...length...] [...number...]
    int lengthOfLength = pipe.ReadByte();

    byte[] lengthBytes = new byte[4] { 0, 0, 0, 0 };
    for (int i = 0; i < lengthOfLength; i++)
    {
        lengthBytes[i] = (byte)pipe.ReadByte();
    }
    int length = BitConverter.ToInt32(lengthBytes, 0);
    byte[] number = new byte[length];
    pipe.Read(number, 0, number.Length);

    return new BigInteger(number);
}
private void SendToPipe(NamedPipeServerStream pipe,
BigInteger bigInt)
{
    byte[] number = bigInt.ToByteArray();
    byte[] length =
BitConverter.GetBytes(number.Length);
    // [length of length] [...length...] [...number...]
    pipe.WriteByte((byte)length.Length);
    pipe.Write(length);
    pipe.Write(number);
}
```

Именованный канал создаётся при запуске аутентификации либо на сервере, либо на клиенте, и выбранная сторона начинает следить за поступающей в канале информацией. Фрагмент программы, отвечающий за создание именованного канала:

```
private void ServerThread(object? data)
{
    try
    {
        // Pipe initialization
        NamedPipeServerStream pipeServer =
        new NamedPipeServerStream("authpipe",
PipeDirection.InOut);

        // Wait for a client to connect
        pipeServer.WaitForConnection();
    }
}
```

```
Invoke() => { consoleRichTextBox.Text +=  
$"Клиент успешно подключен.\n"; });  
}  
}
```

После того, как сервер и клиент запустят процесс аутентификации, происходит обмен «приветствием» друг с другом для того, чтобы убедиться в идентичности выбранного протокола:

```
// Get greeting <---  
BigInteger hello = new BigInteger(78858074867485);  
if (hello == GetFromPipe(pipeServer))  
{  
    Invoke() => {  
        consoleRichTextBox.Text += $"Получено  
приветствие от клиента!\n\n";  
    };  
}
```

После утверждения типа протокола между клиентом и сервером начинается обмен параметрами и криптограммами в соответствии с блок-схемой алгоритма (Рис. 1). По результатам выводится отчёт об успешности аутентификации (Рис. 2).

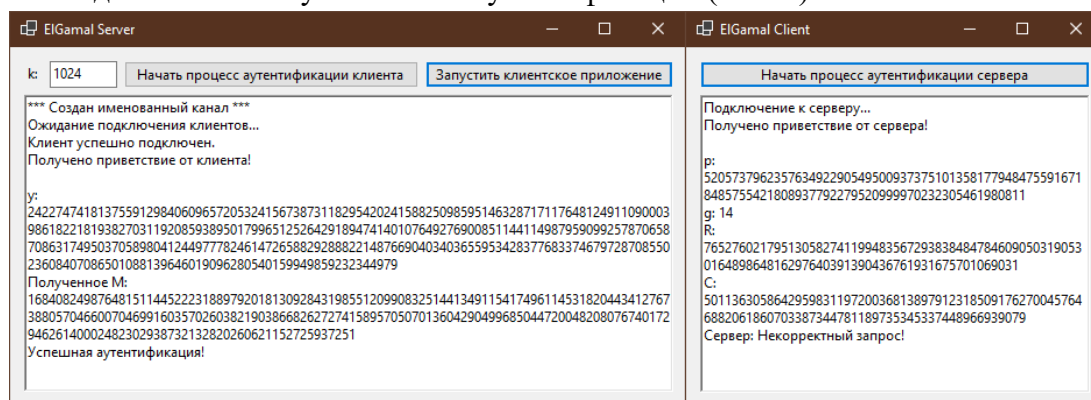


Рисунок 2. - Примеры отчётов программы

Источник: анализ автора

Заключение

Протоколы аутентификации с нулевым разглашением часто применяются в системах защиты информации. С их помощью одна из сторон-участников убеждается в том, что некоторый секрет уже известен второй стороне без необходимости раскрытия самого секрета.

В статье приводится программная реализация протокола аутентификации на основе асимметричного шифра Эль-Гамалия с использованием меток, который позволяет снизить нагрузку на вычислительные ресурсы путём отказа от традиционно используемых хеш-функций. Также приведён способ решения возникающих проблем при обработке больших чисел в процессе разработки.

Список литературы

1. Молдовян, А. А. Протоколы аутентификации с нулевым разглашением секрета / А. А. Молдовян, Д. Н. Молдовян, А. Б. Левина. – Санкт-Петербург : Университет ИТМО, 2016. – 55 с. – EDN XFXBRL.
2. Рацеев, С. М. Математические методы защиты информации / С. М. Рацеев. – Санкт-Петербург : Издательство "Лань", 2022. – 544 с. – ISBN 978-5-8114-8589-5. – EDN QZANSJ.
3. Рацеев, С. М. О протоколах аутентификации с нулевым разглашением знания / С. М. Рацеев, М. А. Ростов // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. – 2019. – Т. 19, № 1. – С. 114-121. – DOI 10.18500/1816-9791-2019-19-1-114-121. – EDN ULRWTX.
4. T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985, doi: 10.1109/TIT.1985.1057074.
5. Сикорская, Г. А. Мультипликативно обратный элемент для вычета по модулю m / Г. А. Сикорская // Инновационная наука. – 2016. – № 4-4. – С. 37-39. – EDN VSUOND.

References

1. Moldovyan, A. A. Authentication protocols with zero-knowledge of a secret / A. A. Moldovyan, D. N. Moldovyan, A. B. Levina. – St. Petersburg : ITMO University, 2016. – p.55 – EDN XFXBRL.
 2. Ratseev, S. M. Mathematical methods of information protection / S. M. Ratseev. – St. Petersburg : Lan Publishing House, 2022. – p. 544– ISBN 978-5-8114-8589-5. – EDN QZANSJ.
 3. Ratseev, S. M. On authentication protocols with zero knowledge disclosure / S. M. Ratseev, M. A. Rostov // Izvestiya Saratov University. A new series. Series: Mathematics. Mechanics. Computer science. - 2019. – Vol. 19, No. 1. – pp. 114-121. – DOI 10.18500/1816-9791-2019-19-1-114-121. – EDN ULRWTX.
 4. T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985, doi: 10.1109/TIT.1985.1057074.
 5. Sikorskaya, G. A. Multiplicatively inverse element for deduction modulo m / G. A. Sikorskaya // Innovative science. - 2016. – No. 4-4. – pp. 37-39. – EDN VSUOND.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

БЕЗОПАСНОСТЬ И ПРИВАТНОСТЬ В БЛОКЧЕЙН СЕТЯХ. МЕТОДЫ И ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ

Марква Т.Д.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большеви́ков, 22, корп. 1), e-mail: norm_staffchik@mail.ru

В данной статье рассматриваются ключевые аспекты обеспечения безопасности блокчейн-сетей. Обсуждаются криптографические основы, консенсусные механизмы и многоуровневый подход к защите, охватывающий уровни узлов, сети, приложений и пользователей. Особое внимание уделяется перспективным направлениям исследований, таким как гомоморфное шифрование, блокчейн с нулевым разглашением информации, применение искусственного интеллекта и противодействие угрозам квантовых вычислений. Подчеркивается важность государственного регулирования, отраслевых стандартов и международного сотрудничества для создания безопасной и надежной блокчейн-экосистемы. В заключении отмечается, что обеспечение безопасности является фундаментальным требованием для массового внедрения блокчейна и реализации его революционного потенциала.

Ключевые слова: Блокчейн, безопасность, криптография, консенсус, смарт-контракты, кибербезопасность, гомоморфное шифрование, нулевое разглашение информации, искусственный интеллект, квантовые вычисления, регулирование, стандарты, международное сотрудничество.

SECURITY AND PRIVACY IN BLOCKCHAIN NETWORKS. DATA PROTECTION METHODS AND TECHNOLOGIES

Markva T.D.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: norm_staffchik@mail.ru

This article discusses the key aspects of ensuring the security of blockchain networks. Cryptographic foundations, consensus mechanisms, and a multi-layered approach to protection covering node, network, application, and user levels are discussed. Special attention is paid to promising areas of research, such as homomorphic encryption, zero-disclosure blockchain, the use of artificial intelligence and countering the threats of quantum computing. The importance of government regulation, industry standards and international cooperation to create a secure and reliable blockchain ecosystem is emphasized. In conclusion, it is noted that ensuring security is a fundamental requirement for the mass adoption of blockchain and the realization of its revolutionary potential.

Keywords: Blockchain, security, cryptography, consensus, smart contracts, cybersecurity, homomorphic encryption, zero disclosure of information, artificial intelligence, quantum computing, regulation, standards, international cooperation.

Введение

Технология блокчейна, лежащая в основе криптовалют, получила широкое распространение и признание в качестве революционной инновации, способной трансформировать различные отрасли за пределами финансовой сферы. Одним из ключевых преимуществ блокчейна является его децентрализованная природа, обеспечивающая высокую

степень прозрачности, неизменности и отказоустойчивости данных. Однако вместе с этими преимуществами возникают серьезные вопросы безопасности и защиты конфиденциальности информации, циркулирующей в блокчейн-сетях. Поскольку все транзакции и данные распределены и доступны для просмотра всеми участниками, существует риск раскрытия конфиденциальной информации, подверженности атакам и злонамеренному использованию данных. Обеспечение надлежащего уровня безопасности и конфиденциальности является критически важным для широкого принятия и доверия к технологии блокчейна, особенно в таких чувствительных областях, как финансы, здравоохранение, управление цепочками поставок и защита интеллектуальной собственности.

Криптографические основы блокчейна

Безопасность и неизменность данных в блокчейн-сетях обеспечивается с помощью криптографических алгоритмов и протоколов. В основе технологии блокчейна лежат асимметричное шифрование на базе криптосистем с открытым ключом и цифровые подписи. Каждый участник блокчейна имеет пару ключей: открытый (публичный) ключ, который используется для получения криптовалюты и проверки подписей, и закрытый (приватный) ключ для подписания транзакций и доступа к средствам. Транзакции подписываются отправителем с помощью приватного ключа, гарантируя их подлинность и неизменность. Открытые ключи участников распределяются по сети для проверки подписей. [1, с.262]

Другой важной криптографической техникой в блокчейне является хеширование – применение криптографических хеш-функций для получения цифрового отпечатка или дайджеста данных. Каждый блок в цепочке содержит хеш предыдущего блока, образуя связанную структуру. Изменение любых данных в предыдущих блоках приведет к нарушению последовательности хешей, что легко обнаружить. Помимо хеширования, используются другие криптографические примитивы, такие как деревья Меркла для эффективной проверки транзакций.

Распределенный консенсус между узлами сети является ключевым компонентом блокчейна, обеспечивающим согласованное состояние реестра. Популярными алгоритмами консенсуса являются Proof-of-Work (PoW) и Proof-of-Stake (PoS), основанные на криптографических вычислениях. Распределенная архитектура и согласование данных между множеством узлов делает блокчейн устойчивым к отказам и атакам, поскольку для успешной атаки требуется скомпрометировать значительную часть сети.

Методы защиты конфиденциальности данных

Одной из главных проблем безопасности в блокчейн-сетях является защита конфиденциальности персональных данных и деталей транзакций. Поскольку все операции в блокчейне распределены и потенциально видны всем участникам, существует риск раскрытия конфиденциальной информации, такой как суммы переводов, состояния счетов и связи между адресами. [5, с.267]

Для решения этой проблемы были разработаны различные криптографические методы и технологии, направленные на сохранение приватности пользователей и анонимности транзакций в блокчейне. Одним из базовых подходов является использование псевдонимов и анонимных адресов вместо реальных идентификаторов пользователей. Однако этот метод не

обеспечивает полной конфиденциальности, так как транзакции все равно видны, а адреса могут быть связаны с реальными личностями путем анализа блокчейна.

Для более надежной защиты конфиденциальности применяются технологии обфускации и микширования (mixers), которые объединяют множество транзакций от разных источников, затрудняя отслеживание связей между адресами отправителей и получателей. Также используются кольцевые подписи, позволяющие скрыть отправителя транзакции в группе из нескольких возможных подписантов.

Одной из наиболее перспективных технологий являются криптографические доказательства с нулевым разглашением информации (zk-SNARKs), которые позволяют проверить корректность транзакций, не раскрывая их содержимого. Эта технология лежит в основе таких проектов, как Zcash и конфиденциальный вариант Ethereum, обеспечивая полную конфиденциальность и невозможность отслеживания транзакций. [3, с.77]

Кроме того, существуют специализированные конфиденциальные блокчейны, например, Monero, которые изначально ориентированы на повышенную приватность за счет использования кольцевых подписей, технологии взаимного сокрытия (stealth addressing) и других методов.

Важно отметить, что обеспечение приватности в блокчейне часто имеет компромиссы, такие как снижение производительности или увеличение размера данных. Поэтому выбор и внедрение соответствующих методов защиты конфиденциальности должны учитывать требования конкретных случаев использования и находить баланс между безопасностью, производительностью и масштабируемостью.

Многоуровневая безопасность блокчейн-сетей

Обеспечение всесторонней безопасности в блокчейн-экосистеме требует принятия многоуровневого подхода, охватывающего различные компоненты и слои системы. Меры защиты должны распространяться на уровни отдельных узлов, сети в целом, уровень приложений и смарт-контрактов, а также учитывать безопасность конечных пользователей.

На уровне отдельных узлов необходимо применять традиционные методы защиты, такие как антивирусное программное обеспечение, брандмауэры, регулярное обновление программного обеспечения и операционных систем. В блокчейнах, использующих алгоритм консенсуса Proof-of-Work, важно обеспечить достаточную вычислительную мощность для защиты от потенциальных атак 51%. Также необходимо тщательно защищать закрытые ключи узлов с помощью надежных средств хранения и резервного копирования.

На уровне сети безопасность обеспечивается распределенной архитектурой блокчейна и консенсусными механизмами. Тем не менее, существуют угрозы, такие как DDoS-атаки, направленные на перегрузку и дестабилизацию сети. Для противодействия этим атакам применяются специальные протоколы и методы обнаружения аномального трафика, а также повышение производительности и пропускной способности сети. [2, с.92]

На уровне приложений и смарт-контрактов крайне важен тщательный аудит исходного кода на предмет уязвимостей и ошибок, которые могут привести к потере средств или раскрытию данных. Технологии, такие как формальная верификация и изоляция смарт-контрактов, помогают снизить риски. Кроме того, необходимо постоянно отслеживать появление новых угроз и своевременно выпускать обновления безопасности.

Наконец, безопасность конечных пользователей является важным фактором. Необходимо обеспечить надежную защиту кошельков и приватных ключей, а также повышать осведомленность пользователей о потенциальных угрозах, таких как фишинг и мошеннические схемы. Кроме того, следует предоставлять простые в использовании инструменты для резервного копирования и восстановления средств в случае потери доступа.

Новые технологии и исследования в области безопасности блокчейна

Область безопасности и приватности в блокчейн-сетях является активно развивающейся и привлекает значительные усилия исследователей и разработчиков. Помимо совершенствования существующих методов, ведутся работы по созданию принципиально новых технологий для повышения уровня защиты данных в этой экосистеме.

Одним из перспективных направлений является применение гомоморфного шифрования, позволяющего выполнять вычисления над зашифрованными данными без их расшифровки. Это открывает возможность для создания приватных смарт-контрактов и конфиденциальных вычислений в блокчейне без раскрытия входных данных. Компании, такие как Microsoft, IBM и другие ведущие технологические гиганты, активно исследуют применение гомоморфного шифрования в блокчейн-средах.

Другим многообещающим подходом являются так называемые "блокчейны с нулевым разглашением информации" (zk-Rollups), которые используют современные криптографические доказательства с нулевым разглашением для масштабирования и повышения конфиденциальности транзакций. Этот метод позволяет проверять корректность транзакций, не раскрывая их содержимого, и агрегировать большое количество операций в одну, снижая нагрузку на основную блокчейн-сеть. Проекты вроде Starkware и ZCash работают над внедрением этой технологии.

В сфере кибербезопасности активно изучается применение методов искусственного интеллекта, таких как машинное обучение, для выявления аномалий, мошеннических схем и потенциальных атак на блокчейн-системы. Возможность анализировать огромные объемы данных о транзакциях и поведении узлов позволит своевременно обнаруживать подозрительную активность и принимать соответствующие меры защиты.

Важным направлением исследований является разработка методов защиты блокчейнов от угроз, связанных с квантовыми вычислениями. Поскольку квантовые компьютеры могут нарушить многие современные криптографические алгоритмы, необходимо заранее подготовить постквантовые криптосистемы, устойчивые к атакам с использованием квантовых вычислений.

Кроме технологических инноваций, важную роль играет стандартизация и создание передовых практик в области безопасности блокчейна. Различные отраслевые организации и консорциумы, такие как Всемирный экономический форум и Институт стандартов IEEE, работают над разработкой стандартов и рекомендаций по обеспечению кибербезопасности в блокчейн-экосистеме.

Регулирование, стандартизация и сотрудничество

Обеспечение надлежащего уровня безопасности и конфиденциальности в блокчейн-экосистеме невозможно без соответствующих регуляторных мер, отраслевых стандартов и тесного сотрудничества между различными заинтересованными сторонами.

Регулирующие органы играют важную роль в создании нормативно-правовой базы для безопасного и ответственного внедрения блокчейн-технологий. Необходимо разработать четкие требования и руководящие принципы в области кибербезопасности, защиты данных, соблюдения конфиденциальности и противодействия финансовым преступлениям, связанным с блокчейном. Своевременное регулирование поможет устранить правовую неопределенность и создаст благоприятные условия для развития инноваций в этой сфере.

Наряду с государственным регулированием, крайне важна разработка отраслевых стандартов и передовых практик безопасности блокчейнов. Такие организации, как Институт инженеров по электротехнике и электронике (IEEE), Международная организация по стандартизации (ISO) и Консорциум распределенных реестров (Decentralized Identity Foundation), работают над созданием всеобъемлющих стандартов, охватывающих различные аспекты блокчейн-безопасности, включая криптографию, управление идентификационными данными, смарт-контракты и многое другое.

Кроме того, необходимо тесное сотрудничество и координация усилий между различными участниками блокчейн-экосистемы, включая разработчиков, владельцев узлов, поставщиков услуг, регуляторов и исследовательские организации. Обмен информацией об актуальных угрозах, уязвимостях и передовых методах защиты имеет решающее значение для повышения общего уровня безопасности.

На международном уровне важную роль играют такие инициативы, как Глобальная платформа по управлению киберпространством Всемирного экономического форума, которая объединяет правительства, компании и экспертов для координации усилий по обеспечению безопасности новых технологий, включая блокчейн. [4, с.149]

Заключение

В заключение следует отметить, что безопасность является фундаментальным требованием для массового внедрения блокчейна в различных областях человеческой деятельности. Только путем объединения усилий разработчиков, исследователей, регуляторов и всех заинтересованных сторон мы сможем создать надежную и защищенную блокчейн-экосистему, способную реализовать весь революционный потенциал этой технологии.

Безопасность блокчейна – это непрерывный процесс, требующий постоянного внимания и совершенствования. Будущее этой технологии во многом зависит от нашей способности эффективно противостоять новым угрозам и вызовам, которые неизбежно возникнут. Только тогда мы сможем в полной мере воспользоваться преимуществами открытой, прозрачной и децентрализованной среды, создаваемой блокчейнами.

Список литературы

1. Волкогон В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019.
2. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8.

3. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4.
4. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018.
5. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019.

References

1. Volkogonov V. N., Gelfand A.M., Derevyanko V. S. Relevance of automated control systems //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019.
 2. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – №. 8.
 3. Orlov G. A., Krasov A.V., Gelfand A.M. Application of Big Data in the analysis of big data in computer networks //High-tech technologies in space exploration of the Earth. – 2020. – Vol. 12. – No. 4.
 4. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics" RI-2018". – 2018.
 5. Volkogonov V. N., Gelfand A.M., Karamova M. R. Ensuring the security of personal data during their processing in personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.942.2

БЛОКЧЕЙН И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ. ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ СОВМЕСТНОГО ИСПОЛЬЗОВАНИЯ

Марквa Т.Д.

*ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большеви́ков, 22, корп. 1), e-mail:
norm_staffchik@mail.ru*

В данной статье рассматривается перспективная область интеграции двух революционных технологий – блокчейна и искусственного интеллекта (ИИ). Анализируются ключевые направления и преимущества их совместного применения, такие как повышение прозрачности, безопасности и эффективности различных систем и процессов. Обсуждается использование блокчейна для обеспечения подотчетности И-решений, а также применение ИИ для оптимизации блокчейн-сетей и смарт-контрактов. Рассматриваются существующие проблемы и риски, включая масштабируемость, конфиденциальность данных, энергопотребление и регулирование. Наконец, представлены перспективные направления дальнейшего развития, такие как децентрализованные платформы И, федеративное обучение, самоуправляемые DAO и решения для Интернета вещей. Статья демонстрирует огромный потенциал синергии блокчейна и ИИ для трансформации различных отраслей.

Ключевые слова: Блокчейн, искусственный интеллект, интеграция технологий, децентрализация, прозрачность, безопасность, смарт-контракты, проблемы масштабируемости, конфиденциальность данных, перспективные направления.

BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE. OPPORTUNITIES AND PROSPECTS FOR SHARING

Markva T.D.

*ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: norm_staffchik@mail.ru*

This article examines a promising area of integration of two revolutionary technologies – blockchain and artificial intelligence (AI). The key areas and advantages of their joint application are analyzed, such as increasing transparency, security and efficiency of various systems and processes. The use of blockchain to ensure accountability of I-solutions is discussed, as well as the use of AI to optimize blockchain networks and smart contracts. The existing problems and risks are considered, including scalability, data privacy, energy consumption and regulation. Finally, promising areas for further development are presented, such as decentralized platforms and federated learning, self-managed DAOs and solutions for the Internet of Things. The article demonstrates the huge potential of blockchain and AI synergy for the transformation of various industries.

Keywords: Blockchain, artificial intelligence, technology integration, decentralization, transparency, security, smart contracts, scalability issues, data privacy, promising areas.

Введение

Блокчейн и искусственный интеллект (ИИ) являются двумя из наиболее перспективных и революционных технологий современности, оказывающих глубокое влияние на различные сферы человеческой деятельности. Блокчейн представляет собой распределенную базу

данных или реестр, записи в котором объединены в неизменяемые цепочки блоков и репликируются на множество узлов в одноранговой сети. Ключевыми свойствами блокчейна являются децентрализация, прозрачность, неизменность данных и отсутствие единой точки отказа или контроля.

В свою очередь, искусственный интеллект - это область информатики и компьютерных наук, занимающаяся разработкой интеллектуальных систем и алгоритмов, способных имитировать когнитивные функции, характерные для человеческого разума. ИИ лежит в основе таких технологий, как машинное обучение, обработка естественного языка, компьютерное зрение и многих других. Совместное использование этих двух прорывных технологий открывает огромные возможности для создания принципиально новых решений в самых разных областях, начиная от финансов и логистики и заканчивая здравоохранением и образованием. Объединение децентрализованной архитектуры блокчейна и вычислительной мощности искусственного интеллекта может способствовать повышению безопасности, прозрачности, эффективности и масштабируемости различных систем и процессов. В данной статье мы рассмотрим текущее состояние интеграции технологий блокчейна и ИИ, проанализируем ключевые области их совместного применения, оценим риски и проблемы, а также обсудим перспективные пути дальнейшего развития этого многообещающего междисциплинарного направления.

Блокчейн для ИИ

Помимо использования искусственного интеллекта для развития и оптимизации самой блокчейн-технологии, распределенные реестры данных обладают колоссальным потенциалом для повышения эффективности, безопасности, прозрачности и доверия к системам на базе ИИ. Блокчейн может стать ключевым связующим звеном, обеспечивающим прозрачность, подотчетность и надежную защиту данных для приложений искусственного интеллекта.

Одной из основных и наиболее острых проблем современных ИИ-систем является так называемая "черный ящик" - отсутствие прозрачности в процессах принятия решений сложными моделями машинного обучения. Алгоритмы, особенно глубокие нейронные сети, зачастую представляют собой настоящие "черные коробки", внутренняя логика работы которых скрыта от конечных пользователей. Блокчейн способен преодолеть эту фундаментальную проблему, предоставляя неизменяемый, полностью прозрачный и проверяемый реестр для записи всех входных данных, обучающих наборов, параметров моделей, промежуточных вычислений, обоснований и окончательных результатов работы ИИ-алгоритмов. Такая прозрачность существенно повысит подотчетность искусственного интеллекта, его объяснимость и, как следствие, доверие к принимаемым им решениям.

Качество, достоверность и полнота данных, используемых для обучения и работы моделей искусственного интеллекта, имеет критически важное значение. Однако централизованные хранилища данных, применяемые в настоящее время крупными технологическими компаниями, уязвимы для манипуляций, утечек и внесения искажений, что может приводить к существенным систематическим ошибкам (смещениям) и снижению производительности ИИ-систем. Децентрализованные блокчейн-реестры, построенные по принципу распределенного консенсуса, способны обеспечить единый достоверный, неизменяемый и полностью прозрачный источник обучающих данных для ИИ, доступный для

проверки и аудита всеми заинтересованными сторонами. Это повысит качество и надежность самих моделей ИИ.

Кроме того, революционная идея технологии смарт-контрактов, реализуемой в блокчейнах, открывает новые беспрецедентные способы для практического внедрения и коммерциализации решений на базе искусственного интеллекта. ИИ-модели могут быть напрямую интегрированы в смарт-контракты, размещаемые и исполняемые в децентрализованной блокчейн-среде, что позволит полностью автоматизировать и обезопасить выполнение сложных условных сделок, договоров и транзакций, основываясь на выходных данных и предсказаниях интеллектуальных алгоритмов без какого-либо вмешательства третьих лиц. Кроме того, блокчейн может использоваться как распределенный реестр для отслеживания авторства, подтверждения происхождения и защиты прав интеллектуальной собственности на ИИ-модели, алгоритмы и наборы данных.

ИИ для развития блокчейна

Искусственный интеллект также играет критически важную роль в дальнейшем развитии и совершенствовании самой технологии блокчейна. Благодаря своей колоссальной вычислительной мощности и способности обрабатывать гигантские объемы структурированных и неструктурированных данных, алгоритмы искусственного интеллекта могут применяться для решения широкого круга задач по оптимизации и модернизации различных аспектов блокчейн-систем.

Одной из ключевых областей является использование ИИ для совершенствования консенсусных алгоритмов, лежащих в основе большинства блокчейн-сетей. Существующие алгоритмы консенсуса, такие как доказательство выполнения работы (Proof-of-Work, PoW) и доказательство владения долей (Proof-of-Stake, PoS), обеспечивающие согласованность и безопасность распределенных реестров данных, часто сталкиваются с серьезными проблемами масштабируемости, энергоэффективности и гибкости. Искусственный интеллект может помочь в разработке принципиально новых более эффективных и адаптивных консенсусных протоколов, способных динамически подстраиваться под изменяющиеся условия нагрузки и состава сети. К примеру, методы машинного обучения могут использоваться для оптимального распределения вычислительных ресурсов между узлами сети, прогнозирования будущих пиковых нагрузок и своевременного масштабирования инфраструктуры. ИИ-алгоритмы также могут применяться для выявления и предотвращения различных типов атак на консенсусные механизмы, таких как атаки большинства или атаки с использованием вредоносных смарт-контрактов. [2, с.2]

Другой важной областью является применение искусственного интеллекта для всестороннего анализа, моделирования и изучения сложного системного поведения блокчейн-сетей. Ввиду высокой сложности взаимодействия многокомпонентных блокчейн-систем, традиционные аналитические методы часто оказываются недостаточно эффективными. Передовые технологии ИИ, такие как глубокие нейронные сети, генетические и эволюционные алгоритмы, позволяют создавать высокоточные модели для исследования свойств блокчейн-экосистем на системном уровне. Это дает возможность лучше понимать фундаментальные характеристики распределенных реестров данных, выявлять их уязвимости и узкие места, а также разрабатывать более эффективные и совершенные архитектуры

блокчейнов. ИИ-модели также могут использоваться для прогнозирования дальнейшего развития блокчейн-технологий и оценки влияния новых технических улучшений и инноваций.

Наконец, искусственный интеллект находит все более широкое применение в области выявления мошеннической активности, отмывания денег и других видов финансовых преступлений в блокчейн-сетях. Алгоритмы машинного обучения способны анализировать огромные массивы данных транзакций и выявлять сложные закономерности, а также распознавать аномалии и подозрительные паттерны поведения, указывающие на незаконную деятельность. ИИ-системы могут использоваться для автоматического мониторинга и контроля соответствия транзакций нормативным требованиям в области комплаенса, а также для повышения общей безопасности блокчейн-решений и противодействия кибератакам на них.

Проблемы и риски в сочетании блокчейна и ИИ

Несмотря на огромные преимущества и перспективы использования блокчейна и искусственного интеллекта в рамках единой технологической экосистемы, существует целый ряд серьезных проблем и рисков, которые необходимо тщательно учитывать и решать при практической реализации этой интеграции.

Одной из наиболее острых проблем является масштабируемость и производительность совместных блокчейн-ИИ решений. Уже на текущем этапе многие блокчейн-сети, такие как биткойн и эфириум, сталкиваются с фундаментальными ограничениями в виде низкой пропускной способности, высоких задержек при обработке транзакций и консенсусе. Интеграция вычислительно сложных моделей и алгоритмов искусственного интеллекта может еще больше снизить производительность и создать критическую нагрузку на инфраструктуру распределенных сетей. Требуются масштабные дальнейшие исследования и разработки для создания новых высокопроизводительных архитектур и протоколов, способных эффективно объединять возможности блокчейна и ИИ.

Другой существенной проблемой является обеспечение безопасности и сохранение неизменности самих ИИ-моделей в блокчейн-средах. Одним из фундаментальных свойств блокчейна является криптографическая неизменность данных после их внесения в реестр. Однако в случае с моделями машинного обучения неизменность может стать серьезным ограничением, поскольку эти модели нередко требуют обновления, доработки и переобучения по мере поступления новых данных. Необходимо найти разумный баланс между требованиями неизменности и гибкости для эффективной интеграции ИИ-технологий с блокчейн-инфраструктурой. [5, с.33]

Еще одним вызовом является обеспечение конфиденциальности и безопасности данных в гибридной блокчейн-ИИ среде. С одной стороны, прозрачность и отслеживаемость транзакций в блокчейн-системах является безусловным преимуществом для многих приложений. Однако в таких чувствительных областях, как здравоохранение, финансы или оборона, требования по неприкосновенности частной информации являются критически важными. Хотя блокчейн позволяет шифровать и сохранять конфиденциальность данных, обработка зашифрованного контента моделями ИИ представляет собой сложнейшую техническую задачу. Для решения этой проблемы необходимы принципиально новые криптографические методы и протоколы, обеспечивающие безопасность данных на всех этапах цикла в гибридных блокчейн-ИИ системах.

Серьезные опасения вызывают также вопросы ответственности и аудита ИИ-решений, работающих в рамках децентрализованной блокчейн-среды. Использование распределенных реестров может повысить прозрачность работы алгоритмов ИИ, однако в то же время возникают сложные юридические коллизии – кто будет нести ответственность за ошибочные или наносящие ущерб действия таких систем, если их логика выполняется автономно на сотнях или тысячах узлов? Необходима разработка четких правовых норм, процедур аудита и определения ответственных сторон для предотвращения злоупотреблений. [1, с.31]

В целом, текущая правовая и регуляторная неопределенность в отношении блокчейна и ИИ является одним из главных сдерживающих факторов для их интеграции и широкого внедрения. Поскольку эти технологии являются относительно новыми, во многих юрисдикциях отсутствуют полноценные законодательные акты и нормативно-правовая база для их регулирования в комплексе. Необходимо тесное сотрудничество между разработчиками, регуляторами и экспертами для создания всеобъемлющих стандартов и правил игры.

Не стоит также недооценивать риски централизации и монополизации блокчейн-сетей и ИИ-решений крупными технологическими игроками, обладающими значительными ресурсами данных и вычислительными мощностями. Это идет вразрез с фундаментальными принципами децентрализации и распределенности, лежащими в основе этих технологий. Важно создавать стимулы и защитные механизмы для сохранения действительно открытого и инклюзивного характера будущих блокчейн-ИИ экосистем.

И наконец, крайне важной проблемой является высокое энергопотребление и вопросы экологической устойчивости интегрированных ИИ-блокчейн решений. Добавление вычислительно интенсивных задач искусственного интеллекта к уже ресурсоемким блокчейн-сетям может создать колоссальную нагрузку на энергосистемы. Поэтому необходимо уделять первостепенное внимание энергоэффективности при разработке архитектур и протоколов для совместного использования этих технологий.

Будущие направления и перспективы

Интеграция блокчейна и искусственного интеллекта представляет собой одно из наиболее многообещающих и активно развивающихся направлений на передовой технологического прогресса. Открывая практически безграничные возможности для инноваций и трансформации различных отраслей, это междисциплинарное поле уже демонстрирует впечатляющую динамику исследований и разработок.

Одним из ключевых векторов развития является создание децентрализованных платформ и инфраструктуры для разработки, обучения, развертывания и монетизации моделей и приложений искусственного интеллекта. Такие платформы, построенные на базе технологий распределенных реестров и смарт-контрактов, позволят различным участникам (разработчикам ИИ, исследователям, поставщикам данных, потребителям) безопасно и прозрачно взаимодействовать, обмениваться ресурсами и монетизировать свои вклады в рамках единой экосистемы. Пионерами в этом направлении выступают такие проекты, как SingularityNET, Ocean Protocol, Fetch.ai и другие, стремящиеся создать подлинно глобальные децентрализованные рынки и сообщества для ИИ-приложений, наборов данных, обучающих примеров и вычислительных мощностей.

Еще одной перспективной областью является разработка передовых методов федеративного или совместного обучения моделей искусственного интеллекта на распределенных данных без необходимости их физической централизации. Данные подходы в сочетании с новейшими технологиями сохранения конфиденциальности на блокчейне, такими как доказательства с нулевым разглашением, гомоморфное шифрование, секретные контракты и др., позволят создавать сверхмощные ИИ-модели с беспрецедентными возможностями при сохранении полной приватности данных всех задействованных сторон. Над решениями для федеративного ИИ активно работают технологические гиганты вроде IBM, Microsoft и Google, а также многочисленные стартапы и исследовательские группы.

Объединение возможностей блокчейна, смарт-контрактов и искусственного интеллекта открывает путь к созданию полностью автономных и самоуправляемых децентрализованных организаций и сообществ (DAO). В таких организациях ИИ-системы смогут выполнять функции принятия решений и управления на основе заранее заданных целей, правил и ограничений, кодифицированных в виде смарт-контрактов и исполняемых в блокчейн-среде без какого-либо централизованного управления. Децентрализованные автономные организации на стыке ИИ и блокчейна могут применяться в самых разных областях - от управления сообществами и ресурсами до координации сложных производственных процессов, логистических цепочек поставок и многого другого. Первыми ласточками в этом направлении стали такие проекты, как DAO.casino, Aragon и ряд других.

Помимо этого, симбиоз искусственного интеллекта и блокчейна открывает огромные возможности для повышения безопасности, эффективности и масштабируемости систем Интернета вещей (IoT). Распределенные реестры данных способны обеспечить надежную децентрализованную инфраструктуру для безопасной передачи данных между устройствами. В то же время, ИИ-алгоритмы могут использоваться для интеллектуального управления IoT-сетями, оптимизации рабочих процессов, предиктивного обслуживания, выявления аномалий и предотвращения кибератак на подключенные устройства. Уже сейчас компании вроде Xage, Hdac и другие активно работают над созданием инновационных блокчейн-ИИ решений для безопасного подключения и управления IoT на принципах децентрализации и искусственного интеллекта. [4, с.68]

Хотя многие из этих направлений все еще находятся на ранней стадии, они демонстрируют поистине революционный потенциал объединения блокчейна и ИИ для трансформации существующих и создания принципиально новых отраслей и рынков. По мере дальнейшего развития и преодоления нынешних ограничений, синергия этих передовых технологий будет только возрастать, открывая новые парадигмы для повышения эффективности, безопасности, масштабируемости и уровня автоматизации самых разных систем и процессов.

Будущее, в котором распределенные неизменяемые реестры данных и сверхмощные алгоритмы искусственного интеллекта гармонично дополняют друг друга, обещает стать более прозрачным, рациональным, безопасным и в конечном счете более ориентированным на истинные человеческие потребности и ценности. Однако для воплощения этого грандиозного видения необходимы объединенные усилия учёных, инженеров, предпринимателей, политиков и всего глобального сообщества.

Заключение

Интеграция технологий блокчейна и искусственного интеллекта открывает широкие перспективы для создания инновационных и трансформационных решений в самых разных сферах человеческой деятельности. Объединение децентрализованной архитектуры распределенных реестров и вычислительной мощи ИИ позволяет повысить эффективность, безопасность, прозрачность и масштабируемость различных систем и процессов.

Хотя на пути практической реализации этого многообещающего симбиоза существуют значительные проблемы и вызовы, быстрое развитие исследований и разработок в данной области внушает оптимизм. Создание децентрализованных ИИ-платформ, методов федеративного обучения, самоуправляемых DAO и решений для безопасности Интернета вещей – лишь некоторые из перспективных направлений, демонстрирующих огромный потенциал объединения блокчейна и ИИ.

Однако для полной реализации этого потенциала необходимы дальнейшие усилия по преодолению существующих ограничений в плане масштабируемости, энергоэффективности, конфиденциальности данных и регулирования. Кроме того, крайне важно обеспечить ответственное и этическое внедрение этих передовых технологий, учитывая их серьезные последствия для общества и индустрий.

Требуется тесное сотрудничество между учеными, разработчиками, регуляторами и другими заинтересованными сторонами для разработки всеобъемлющих стандартов, норм и законодательных актов, способствующих безопасному и устойчивому развитию экосистемы, объединяющей блокчейн и искусственный интеллект. [3, с.508]

В целом, интеграция блокчейна и ИИ представляет собой один из наиболее многообещающих технологических фронтиров с огромным трансформационным потенциалом. По мере дальнейшего прогресса в этой области мы можем ожидать появления принципиально новых бизнес-моделей, продуктов и услуг, повышающих эффективность, безопасность и инновационность различных отраслей. Будущее, в котором распределенные реестры и искусственный интеллект гармонично работают вместе, обещает стать более прозрачным, подотчетным и ориентированным на человека.

Список литературы

1. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018.
2. Krasov A., Vitkova L., Pestov I. Behavioral analysis of resource allocation systems in cloud infrastructure //2019 International Russian Automation Conference (RusAutoCon). – IEEE, 2019.
3. Гераськина В. С. и др. Методы и стратегии оповещения населения об угрозах возникновения кризисных ситуаций //Информационная безопасность регионов России (ИБРР-2017). – 2017.
4. Шемякин С. Н. и др. Теоретическая оценка использования математических методов прогнозирования загрузки виртуальной инфраструктуры //Наукоемкие технологии в космических исследованиях Земли. – 2021. – Т. 13. – №. 4.
5. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2021.

References

1. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018.
 2. Krasov A., Vitkova L., Pestov I. Behavioral analysis of resource allocation systems in cloud infrastructure //2019 International Russian Automation Conference (RusAutoCon). – IEEE, 2019.
 3. Geraskina V. S. et al. Methods and strategies for notifying the public about the threats of crisis situations //Information security of Russian regions (IBRD-2017). – 2017.
 4. Shemyakin S. N. et al. Theoretical assessment of the use of mathematical methods for predicting the load of virtual infrastructure //High-tech technologies in space exploration of the Earth. - 2021. – Vol. 13. – No. 4.
 5. Shemyakin S. N. et al. Using graph theory to model the security of cloud systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2021.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.942.2

ЦИФРОВЫЕ ДВОЙНИКИ: ТЕХНОЛОГИЯ, ФОРМИРУЮЩАЯ БУДУЩЕЕ

¹Вирясов А.Р., ²Мелькин М.В., ³Левкин Н.Е.

ФГБОУ ВО «ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ», г. Самара, Россия (443010, г. Самара ул. Льва
Толстого, 23), e-mail: ¹mirrrorsedge2020@mail.ru, ²soultrxter@gmail.com,
³levkin.nikita@inbox.ru

Цифровые двойники (digital twins сокр. DT) — это виртуальные копии физических объектов, систем или процессов, созданные для мониторинга, анализа и оптимизации их работы. В статье рассматриваются основные аспекты применения цифровых двойников в различных отраслях. Описываются принципы работы технологии, ее возможности для моделирования и прогнозирования. В заключении обсуждаются перспективы развития технологии цифровых двойников и ее влияние на цифровую трансформацию бизнеса и общества.

Ключевые слова: Цифровой двойник, технология моделирования, визуализация данных, прогресс.

DIGITAL TWINS: THE TECHNOLOGY SHAPING THE FUTURE

¹ Viryasov A.R., ² Melkin M.V., ³ Levkin N.E.

VOLGA REGION STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS,
Samara, Russia (443010, Samara st. Lev Tolstoy, 23), e-mail: ¹mirrrorsedge2020@mail.ru,
²soultrxter@gmail.com, ³levkin.nikita@inbox.ru

Digital twins are virtual copies of physical objects, systems, or processes created to monitor, analyze, and optimize their operation. The article discusses the main aspects of the use of digital twins in various industries. The principles of the technology, its capabilities for modeling and forecasting are described. In conclusion, the prospects for the development of digital twin technology and its impact on the digital transformation of business and society are discussed.

Keywords: Digital twin, modeling technology, data visualization, progress.

1. Понятие цифрового двойника

1.1 Определение

Цифровой двойник — это виртуальная модель физического объекта, процесса или системы, которая непрерывно обновляется данными, собираемыми с объекта в режиме реального времени. Эта модель использует технологии интернета вещей (IoT), машинного обучения и искусственного интеллекта для создания точной модели реального объекта или процесса.[1]

DT могут моделировать поведение сложных промышленных систем, отдельных машин и продуктов, а также человеческих органов.

1.2 История и развитие

Идея цифровых двойников возникла в 2002 году в исследовательской работе Майкла Грейвза и начала активно развиваться с развитием IoT и технологий обработки больших данных. [2] Изначально DT применялись в аэрокосмической отрасли для мониторинга и управления сложными техническими системами, такими как самолеты и спутники. Следует отметить, что концепция цифровых двойников впервые была провозглашена как важная часть четвертой промышленной революции (Industry 4.0), основанный на массовом внедрении информационных технологий в промышленность, масштабной автоматизации бизнес-процессов и распространении искусственного интеллекта [6,с.30]

2. Архитектура и принципы работы цифровых двойников

2.1 Структурные элементы

DT состоит из нескольких ключевых компонентов, которые позволяют ему эффективно моделировать физический объект и взаимодействовать с ним:[3]

- Физический объект: это реальный объект или система, данные которого собираются и передаются в цифровую среду.
- Датчики и устройства IoT: устройства, установленные на физическом объекте, которые собирают данные о его состоянии и передают их в цифровую модель.
- Цифровая модель: это виртуальная копия физического объекта, которая отражает его структуру, динамику работы и поведение в различных условиях.[4]

2.2 Принципы работы

Работа DT основана на постоянном взаимодействии между физическими и виртуальными объектами. Датчики, установленные на реальном объекте, собирают данные о его состоянии (например, температуру, вибрацию, износ деталей), передавая их в цифровую модель для дальнейшего анализа. Эта модель анализирует данные, сравнивает их с прогнозами и сценариями, а затем предоставляет пользователю информацию для принятия решений или автоматически оптимизирует работу системы.

Принципы работы цифрового двойника можно разбить на несколько ключевых этапов:

1. Сбор данных: Датчики собирают данные с физического объекта и передают их в облачное хранилище или локальный сервер.
2. Анализ данных: Алгоритмы машинного обучения и ИИ анализируют собранные данные, выявляют аномалии и предсказывают возможные сбои.
3. Визуализация: Операторы могут отслеживать состояние объекта через визуальные интерфейсы в режиме реального времени.

3. Применение цифровых двойников в различных отраслях

3.1 Промышленное производство

DT позволяют мониторить работу оборудования, предсказывать поломки и оптимизировать процессы производства. [5] Примером может служить их использование на автомобильных заводах, где симуляции позволяют не только следить за состоянием оборудования, но и моделировать различные сценарии его работы.

3.2 Строительство и недвижимость

В строительстве DT помогают моделировать эксплуатацию зданий и инженерных сооружений. Они могут использоваться для проектирования, контроля за строительством и управления объектами недвижимости. Например, цифровой двойник здания может отслеживать его энергопотребление, состояние инфраструктуры и планировать профилактические работы.[6]

3.3 Здоровоохранение

DT находят применение в медицине, где они используются для симуляции работы человеческих органов и систем. Это помогает врачам диагностировать заболевания, прогнозировать их развитие и разрабатывать индивидуальные планы лечения.

4. Преимущества и недостатки использования цифровых двойников

4.1 Преимущества

Использование цифровых двойников предоставляет ряд ключевых преимуществ для бизнеса:[7]

- **Повышение эффективности:** DT позволяют оптимизировать процессы, сокращать затраты и повышать производительность.
- **Улучшение качества продукции:** симуляции позволяют выявлять дефекты на ранних стадиях и корректировать процессы.
- **Прогнозирование и управление рисками:** DT позволяют предсказывать возможные риски и предотвращать их до того, как они станут проблемой.

4.2 Недостатки и ограничения

Несмотря на значительные преимущества, технология цифровых двойников сталкивается с рядом недостатков:

- **Высокая стоимость внедрения:** разработка и внедрение цифровых двойников требует значительных инвестиций в оборудование, программное обеспечение и обучение персонала.
- **Безопасность данных:** как и любые системы, работающие с большими объемами данных, DT могут быть уязвимы для кибератак.
- **Комплексность управления:** создание и поддержание цифровых двойников для сложных систем требует высококвалифицированных специалистов и постоянного мониторинга.[8]

5. Возможные варианты развития технологии цифровых двойников:

Перспективы развития цифровых двойников связаны с дальнейшим совершенствованием технологий IoT, искусственного интеллекта и больших данных.

Также активно используются технологии виртуальной и дополненной реальности (**VR** и **AR**) в сочетании с цифровыми двойниками уже активно внедряются в промышленное производство, улучшая визуализацию данных и оптимизируя рабочие процессы. Например, компания Control Care, производитель турбомашин, активно использует DT, виртуальную и дополненную реальность для моделирования работы турбин. [9]

VR-прототипирование позволяет значительно сократить цикл разработки. Например, Boeing использует VR для проектирования новых самолетов. Это позволяет инженерам

тестировать эргономику кабины и систем управления в виртуальной среде, что снижает затраты на производство физической модели и время на ее тестирование. [10]

Заключение

ДТ — это мощный инструмент, который меняет подходы к управлению сложными системами и объектами. Они уже сегодня находят широкое применение в промышленности, строительстве, медицине и других отраслях, помогая компаниям повышать эффективность, снижать риски и улучшать качество продукции. Несмотря на вызовы, с которыми сталкивается эта технология, ее потенциал огромен, и в ближайшие годы ДТ станут неотъемлемой частью цифровой трансформации бизнеса и общества.

Список литературы

1. 5 примеров использования: как виртуальная реальность (VR) на производстве обеспечивает реальные результаты. ОПУБЛИКОВАНО 27 ИЮЛЯ 2023 Г. Е.А.А. KUIPERS URL: <https://fectar.com/blog/5-use-cases-how-virtual-reality-vr-in-manufacturing-delivers-real-results/> (дата публикации 10.09.24)
2. Дополненная реальность и цифровой двойник: современное состояние и перспективы кибербезопасности, Фабиан Бом, Маруэтер Дитц, Тобиас Прейндл и Гюнтер Пернул Дж. Кибербезопасность. Приват. 2021, 1(3), 519-538; <https://doi.org/10.3390/jcp1030026> URL: <https://www.mdpi.com/2624-800X/1/3/26> (дата обращения 10.09.24)
3. Менгер Ф.Р., Егоров Ю.: Моделирование турбулентности технических потоков с помощью SAS. В: DLES 6-6 URL: <https://www.ozeninc.com/wp-content/uploads/2021/01/Turbulence-Modeling-for-Engineering-Flows.pdf>
4. ТИТРОВЫЕ ДВОЙНИКИ В системе УПРАВЛЕНИЯ Минзов А. С.1, Невский А. С.2, Баронов О. Р.3, Немчанинова С.В.4 DOI: 10.21681/2311-3456-2024-2- С.29- 35 URL-АДРЕС: <https://cyberrus.info/wp-content/uploads/2024/04/vokib-2024-2-st04-s029-035.pdf?ysclid=m1561tlai0277902124> (дата обращения 10.09.24)
5. Рассел Стюарт, Норвиг Питер. Искусственный интеллект: современный подход. 3-е изд.). Нью-Джерси: Прентис Холл, 2010. 1152 с. URL: https://www.researchgate.net/publication/220546066_S_Russell_P_Norvig_Artificial_Intelligence_A_Modern_Approach_Third_Edition (дата публикации 10.09.24)
6. Здирук К. Б. Применение цифровых двойников в системах управления сложными объектами [Электронный ресурс] // URL-адрес: <https://www.semanticscholar.org/paper/Digital-twins-of-objects-in-the-solution-of-control-Minaev-Mazin/ca62fdb0c64f0b7d66848a8671ab56a2b95e5dae> (дата обращения 10.09.24)
7. Экстремальные технологии и системы URL: <https://www.extansy.com/> (дата обращения: 07.07.2019).
8. Гривз М., Виккерс Дж. - Цифровой двойник: смягчение непредсказуемого, нежелательного поведения сложных систем (2016) URL: https://www.researchgate.net/publication/306223791_Digital_Twin_Mitigating_Unpredictable_Undesirable_Emergent_Behavior_in_Complex_Systems
9. Тао, Ф., Чжан, Х., Лю, А., Ни, А.И.К. - Интеллектуальное производство, управляемое цифровыми близнецами (2019) URL: https://www.researchgate.net/publication/335057699_Digital_Twin-

driven_smart_manufacturing_Connotation_reference_model_applications_and_research_issues (дата обращения 10.09.24)

10. Гривз М., Виккерс Дж. - Цифровой двойник: смягчение непредсказуемого, нежелательного поведения сложных систем (2016) URL: https://www.researchgate.net/publication/306223791_Digital_Twin_Mitigating_Unpredictable_Undesirable_Emergent_Behavior_in_Complex_Systems (дата публикации 10.09.24)

References

1. 5 use cases: how virtual reality (VR) in manufacturing delivers real results POSTED ON 27 JULY 2023 BY E.A.A. KUIPERS URL: <https://fectar.com/blog/5-use-cases-how-virtual-reality-vr-in-manufacturing-delivers-real-results/> (дата обращения 10.09.24)
2. Augmented Reality and the Digital Twin State-of-the-Art and Perspectives for Cybersecurity by Fabian Bohm, Maruetheres Dietz, Tobias Preindl and Gunther Pernul *J. Cybersecur. Priv.* 2021, 1(3), 519-538; <https://doi.org/10.3390/jcp1030026> URL: <https://www.mdpi.com/2624-800X/1/3/26> (дата обращения 10.09.24)
3. Menter, F.R., Egorov, Y.: SAS Turbulence Modelling of Technical Flows. In: DLES 6 - 6th URL: <https://www.izeninc.com/wp-content/uploads/2021/01/Turbulence-Modeling-for-Engineering-Flows.pdf>
4. ЦИФРОВЫЕ ДВОЙНИКИ В СИСТЕМАХ УПРАВЛЕНИЯ Минзов А. С.1, Невский А. Ю.2, Баронов О. Р.3, Немчанинова С.В.4 DOI: 10.21681/2311-3456-2024-2- С.29-35 URL: <https://cyberrus.info/wp-content/uploads/2024/04/vokib-2024-2-st04-s029-035.pdf?ysclid=m1561tlai0277902124> (дата обращения 10.09.24)
5. Russell Stuart, Norvig Peter. Artificial Intelligence: A Modern Approach. 3rd ed). New Jersey: Prentice Hall, 2010. 1152 p.. URL: https://www.researchgate.net/publication/220546066_S_Russell_P_Norvig_Artificial_Intelligence_A_Modern_Approach_Third_Edition (дата обращения 10.09.24)
6. Здирук К. Б. Применение цифровых двойников в системах управления сложными объектами [Электронный ресурс] // URL: <https://www.semanticscholar.org/paper/Digital-twins-of-objects-in-the-solution-of-control-Minaev-Mazin/ca62fdb0c64f0b7d66848a8671ab56a2b95e5dae> (дата обращения 10.09.24)
7. Экстремальные технологии и системы URL: <https://www.extansy.com/> (дата обращения: 07.07.2019).
8. Grieves, M., Vickers, J. - Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems (2016) URL: https://www.researchgate.net/publication/306223791_Digital_Twin_Mitigating_Unpredictable_Undesirable_Emergent_Behavior_in_Complex_Systems
9. Tao, F., Zhang, H., Liu, A., Nee, A.Y.C. - Digital Twin Driven Smart Manufacturing (2019) URL: https://www.researchgate.net/publication/335057699_Digital_Twin-driven_smart_manufacturing_Connotation_reference_model_applications_and_research_issues (дата обращения 10.09.24)
10. Grieves, M., Vickers, J. - Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems (2016) URL: https://www.researchgate.net/publication/306223791_Digital_Twin_Mitigating_Unpredictable_Undesirable_Emergent_Behavior_in_Complex_Systems (дата обращения 10.09.24)

Вирясов А.Р., Мелькин М.В., Левкин Н.Е. Цифровые двойники: технология, формирующая будущее // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 10(48) с. 104–109

10.09.24)Network traffic optimization. Electronic resource. URL:
[<https://www.osp.ru/lan/2014/11/13043730>] (accessed: 15.05.2024).



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.45

ПОДДЕРЖКА ФОНОВОЙ РАБОТЫ: ПРЕРЫВАНИЕ ПРОЦЕССОВ ШИФРОВАНИЯ/ДЕШИФРОВАНИЯ ПРИ ОСТАНОВКЕ РАБОТЫ АРМ

Кондрашов А.С., ¹Куснуяров Р.Э.

ФГАОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА"
Москва, Россия (119296, город Москва, Ленинский пр-кт, д. 65 к. 1) e-mail:
¹mr.kusnuyarov@mail.ru

В ходе данной статьи рассматриваются процессы шифрования и дешифрования с помощью dm-crypt и LUKS на виртуальной машине в среде VirtualBox на базе дистрибутива операционной системы Альт, оценивается производительность шифрования, проводится эксперимент с шифрованием и дешифрованием файла для проверки целостности данных при остановке работы автоматизированного рабочего места.

Ключевые слова: Шифрование, дешифрование, dm-crypt и LUKS, ОС Альт, автоматизированное рабочее место.

SUPPORT FOR BACKGROUND WORK: INTERRUPTION OF ENCRYPTION/DECRYPTION PROCESSES WHEN THE AUTOMATED CONTROL SYSTEM IS STOPPED

Kondrashov A.S., ¹ Khusnuyarova R.E.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH
UNIVERSITY) Moscow, Russia (119296, Moscow, Leninsky prospekt, 65 bldg. 1) e-mail:
¹mr.kusnuyarov@mail.ru

This article examines the processes of encryption and decryption using dm-crypt and LUKS on a virtual machine in a VirtualBox environment based on the Alt operating system distribution, evaluates encryption performance, and conducts an experiment with file encryption and decryption to verify data integrity when an automated workplace is stopped.

Keywords: Encryption, decryption, dm-crypt and LUKS, Alt OS, automated workplace.

С развитием технологий вопрос безопасности данных становится актуальней. Процесс шифрования является одним из главных инструментов для обеспечения конфиденциальности и защиты данных.[1]

Шифрование – это процесс кодирования информации с целью предотвращения несанкционированного доступа (3). Если зашифрованные данные будут украдены, то информация не сможет быть прочитана без соответствующего ключа. Дешифрование – это обратный процесс. С его помощью появляется возможность преобразовать зашифрованную информацию в оригинальный вид.

С развитием облачных технологий, шифрование становится все более важным инструментом. Для защиты информации при хранении в облаке существуют два варианта:

использование специализированного ПО для шифрования данных и последующей загрузка их в облако или выбор облачных хранилищ, которые изначально обеспечивают встроенное шифрование. В настоящее время на рынке существуют различные сервисы, поддерживающие сквозное шифрование: например, ProtonMail, Tresorit, LastPass, Sync и т.д. Все они обеспечивают доступ к данным исключительно авторизованным пользователем, в то время как провайдеры услуг не могут их расшифровать.

Помимо степени защиты информации, многие системы шифрования могут столкнуться с другими трудностями. [2] Примерами таких являются проблемы, возникающие при несанкционированном завершении работы автоматизированных рабочих мест (АРМ) пользователей. В таких ситуациях существует риск потери данных или их повреждения. Поэтому поддержка фоновой работы процессов важна.

Таким образом, объектом исследования в данной статье выступает сервис по шифрованию данных. Предметом же является механизм продолжения процессов шифрования и дешифрования данных в условиях неожиданного отключения АРМ пользователя.[3]

Конкретной целью данного исследования является анализ функциональности и устойчивости выбранного сервиса к прерыванию процессов шифрования и дешифрования при выключении АРМ.

В области поддержки фоновой работы процессов шифрования и дешифрования при отключении АРМ существует недостаток исследований. В основном исследования сосредоточены на алгоритмах шифрования или времени шифрования (8), тогда как вопросы устойчивости этих процессов к прерываниям остаются нераскрытыми. [4]

Для изучения поддержки фоновой работы сервисов в процессе шифрования и дешифрования данных были выбраны методы теоретического анализа, экспериментального моделирования и сравнительного исследования.

Для этого в среде виртуализации была создана виртуальная машина на базе ОС Альт, на которой будет проводиться эксперимент с помощью алгоритма Linux Unified Key Setup-on-disk-format (LUKS). [5] Для этого будет использоваться утилита Cryptsetup, которая позволяет производить шифрование раздела ОС Альт с помощью модуля dm-crypt.

В Linux существует различные методы и инструменты для шифрования данных. Был выбран метод dm-crypt – механизм шифрования блочных устройств, использующий LUKS для управления ключами. Применяется он при шифровании дисков, разделов и устройств.

Поскольку dm-crypt и LUKS являются стандартом для шифрования в Linux, они хорошо поддерживаются в различных дистрибутивах и интегрируются с различными инструментами, такими как системы резервного копирования и восстановления.

dm-crypt – это механизм шифрования на уровне ядра Linux, который позволяет пользователям монтировать зашифрованную файловую систему. Монтирование файловой системы – процесс, при котором файловая система подключается к каталогу, что делает ее доступной для операционной системы. После монтирования все файлы в файловой системе становятся доступны приложениям без какого-либо дополнительного взаимодействия. При хранении на диске эти файлы шифруются. [6]

Взаимосвязь между приложением, файловой системой и dm-crypt представлена на рисунке 1. Dm-crypt находится между физическим диском и файловой системой, и данные, записываемые из операционной системы на диск, шифруются. Приложение не знает о таком шифровании на уровне диска. Приложения используют определенную точку подключения для

хранения и извлечения файлов, и эти файлы шифруются при сохранении на диск. Если диск потерян или украден, данные на нем бесполезны.



Рисунок 1 – Алгоритм работы dm-crypt

Источник: анализ авторов

Для шифрования диска ОС Альт используется модуль ядра dm-crypt. Его использование создает виртуальное блочное устройство в каталоге /dev/mapper с прозрачным шифрованием для файловой системы и пользователя, что делает данные на потерянном или украденном диске бесполезными. При записи данных на виртуальное устройство они шифруются с использованием оптимизированного алгоритма AES и записываются на физический диск. [7] При чтении происходит обратная операция – данные расшифровываются и передаются пользователю в открытом виде. Кроме того, возможно шифрование не только разделов и дисков, но и обычных файлов с созданием файловой системы на них через подключение как loop-устройство.[8]

Интерфейсом командной строки dm-crypt является cryptsetup. Это инструмент для создания и управления зашифрованными блочными устройствами с использованием LUKS. Он позволяет шифровать диски или разделы для защиты данных от несанкционированного доступа.

Сравним время, которое затрачивается на шифрование файлов весом 1, 3 и 5 Гб с помощью dm-crypt, что позволит оценить производительность системы шифрования и ее эффективность при обработке различных объемов данных. Данные результаты помогут лучше понять, как увеличивается временные затраты на шифрование по мере роста размера файла и оценить потенциальные задержки, которые могут возникать при работе с большой информацией.

Замеры будем производить с помощью Bash-скрипта, код которого находится в открытом доступе на GitHub(7). Перед выполнением операции шифрования скрипт фиксирует текущее время. В случае если шифрование завершилось успешно, выводится время, затраченное на шифрование. [9]

Результат эксперимента представлен в Таблице 1.

Таблица 1. - Время шифровании файлов разного размера

Размер	Время	CPU %
1 Гб	18 сек	84,7 us
3 Гб	23 сек	88,6 us
5 Гб	31 сек	89,9 us

Источник: анализ авторов

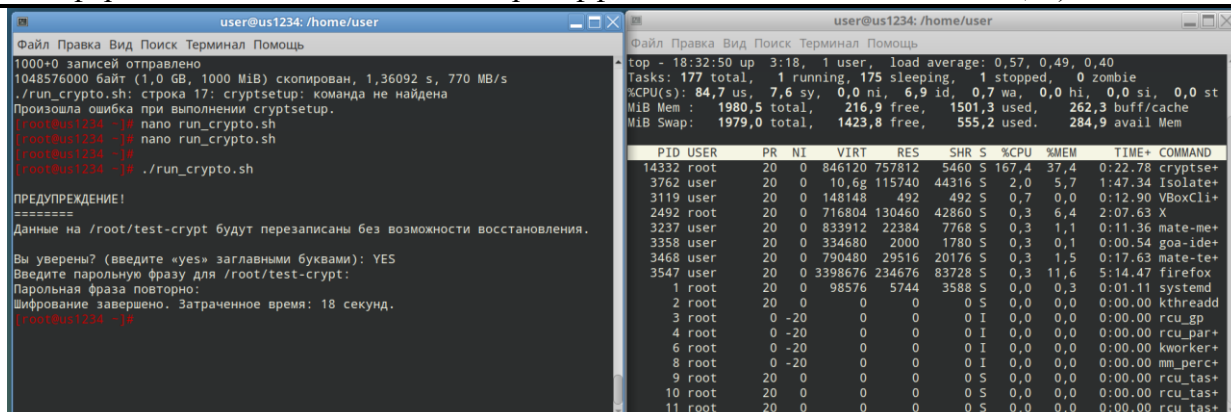


Рисунок 2 – Шифрование файла объемом 1 Гб

Источник: анализ авторов

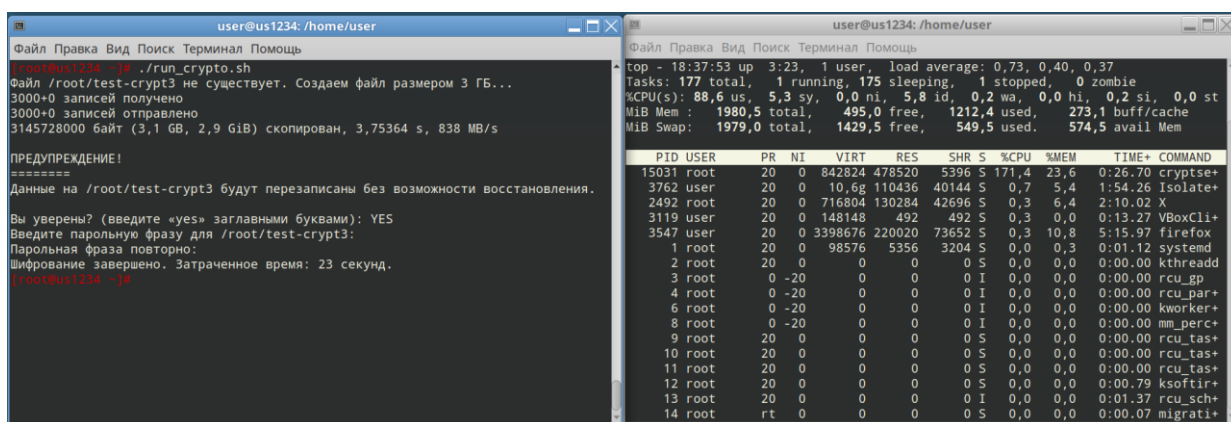


Рисунок 3 – Шифрование файла объемом 3 Гб

Источник: анализ авторов

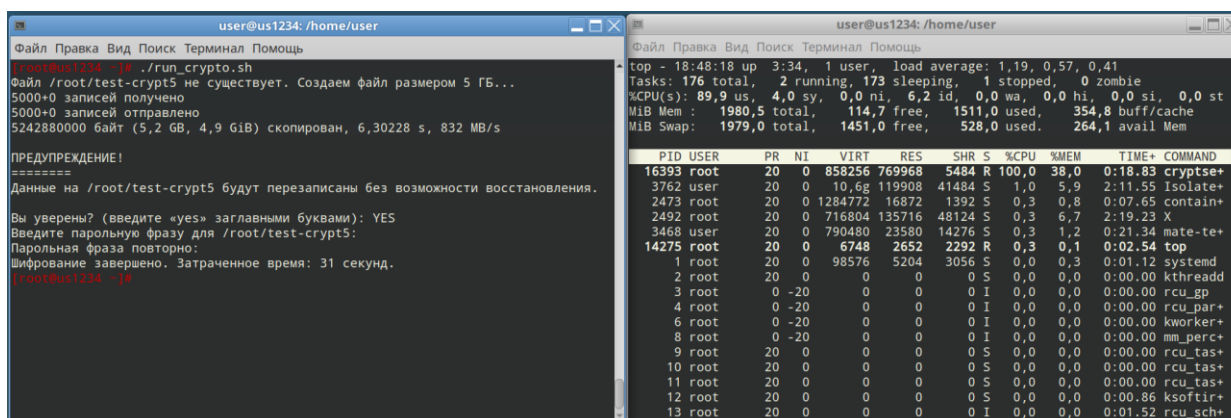


Рисунок 4 – Шифрование файла объемом 5 Гб

Источник: анализ авторов

В результате видно, что в зависимости от размера файла, время его шифрования увеличивалось. Таким образом, можно сделать вывод, что чем больше вес файла, тем больше времени, и тем больше ресурсов требуется процессору.

После выявления данной зависимости, было принято решение шифровать файл весом 10Гб, чтобы иметь больше времени для выключения компьютера в ручном режиме. Далее необходимо выполнить следующий порядок действий.

1. Удалим ранее созданные и зашифрованные файлы;
2. Создадим файл test-crypt3 объемом 10 Гб.
3. Зашифруем файл не прерывая работу АРМ.
4. Проверим, что операция была успешна выполнена.
5. Создадим файл test-crypt2, который шифровать не будем.
6. С помощью команды luksDump выведем информацию о зашифрованном томе.

С помощью luksDump пользователь может просмотреть метаданные, связанные с LUKS-шифрованием, без необходимости монтировать зашифрованный том.

На Рисунке 8 видно, что при попытке вывести информацию о незашифрованном LUKS файле test-crypt2 система выдает ошибку, хотя он сам по себе существует на компьютере. При этом информацию о test-crypt3 выводится. С помощью этой команды будем проверять что произойдет с файлом при выключении компьютера во время процесса шифрования.

```
[root@ust1234 ~]# dd if=/dev/zero of=/root/test-crypt3 bs=1M count=10000
10000+0 записей получено
10000+0 записей отправлено
10485760000 байт (10 GB, 9,8 GiB) скопирован, 9,4458 s, 1,1 GB/s
[root@ust1234 ~]# /sbin/cryptsetup -y luksFormat --batch-mode /root/test-crypt3
Введите парольную фразу для /root/test-crypt3:
Парольная фраза повторно:
[root@ust1234 ~]# ls -l /root/test-crypt2
-rw-r--r-- 1 root root 10485760000 сен  7 23:44 /root/test-crypt2
[root@ust1234 ~]# ls -l /root/test-crypt3
-rw-r--r-- 1 root root 10485760000 сен  7 23:45 /root/test-crypt3
[root@ust1234 ~]# /sbin/cryptsetup luksDump /root/test-crypt2
Устройство /root/test-crypt2 не является корректным устройством LUKS.
[root@ust1234 ~]# /sbin/cryptsetup luksDump /root/test-crypt3
LUKS header information
Version:        2
Epoch:         3
Metadata area:  16384 [bytes]
Keyslots area:  16744448 [bytes]
UUID:          5f100909-bfd0-4d27-9a04-c83b26721505
Label:          (no label)
Subsystem:      (no subsystem)
Flags:          (no flags)
```

Рисунок 5 – Работа с командой luksDump

Источник: анализ авторов

Далее проведем эксперимент с остановкой работы виртуальной машины.

1. Создадим новый файл test-cryp, с которым и будем проводить эксперимент.
2. Запустим процесс шифрования файла test-cryp.
3. Осуществим остановку работы виртуальной машины.

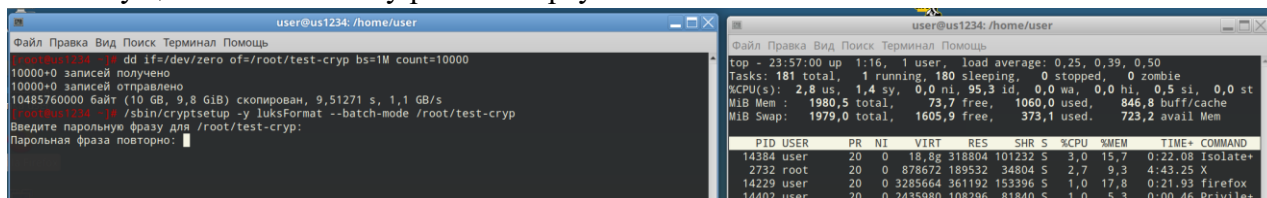


Рисунок 6 – Работа с файлом test-cryp до выключения машины при шифровании

Источник: анализ авторов

После включения машины, проверим его наличие и попытаемся вывести информацию о нем. В результате получим ошибку, что устройство не является корректным устройством LUKS. Чтобы убедиться в корректности работы системы, запросим информацию о test-crypt3, которую система выведет без ошибок.

```
[root@us1234 ~]# ls -l /root/test-cryp
-rw-r--r-- 1 root root 10485760000 сен  7 23:56 /root/test-cryp
[root@us1234 ~]# /sbin/cryptsetup luksDump /root/test-crypt
Устройство /root/test-crypt не существует или отказано в доступе.
[root@us1234 ~]# /sbin/cryptsetup luksDump /root/test-cryp
Устройство /root/test-crypt не является корректным устройством LUKS.
[root@us1234 ~]# /sbin/cryptsetup luksDump /root/test-crypt3
LUKS header information
Version:        2
Epoch:         3
Metadata area:  16384 [bytes]
Keyslots area:  16744448 [bytes]
UUID:           5f100909-bfd0-4d27-9a04-c83b26721505
Label:          (no label)
Subsystem:      (no subsystem)
Flags:          (no flags)
```

Рисунок 7 – Работа с файлом test-cryp после выключения машины при шифровании
Источник: анализ авторов

В результате видно, что файл не зашифровался, но при этом и не повредился.

Перед тем как переходить к процессу дешифрования, для начала проверим как ведет себя система при дешифровании файла без сбоев. Для этого «откроем» зашифрованный контейнер test-crypt3. Так как система дает возможность ввести пароль и не выводит никаких сообщений об ошибке, то файл в порядке, а данные целы.

Для того, чтобы убедиться, что устройство было успешно открыто, выполним команду `ls /dev/mapper/`. Она выводит список всех виртуальных блочных устройств, которые были созданы с помощью `dm-crypt` и которые находятся в каталоге `/dev/mapper/`. Так как `my_encrypted_volume` есть в списке, значит, что контейнер успешно открыт.

```
[root@us1234 ~]# /sbin/cryptsetup luksOpen /root/test-crypt3 my_encrypted_volume
Введите парольную фразу для /root/test-crypt3:
[root@us1234 ~]# cryptsetup luksOpen /root/test-crypt my_encrypted_volume
bash: cryptsetup: команда не найдена
[root@us1234 ~]# ls /dev/mapper/
control my_encrypted_volume
```

Рисунок 8 – Проверка работы команды luksOpen
Источник: анализ авторов

Теперь проверим процесс дешифрования.

1. Зашифруем файл test-cryp
2. Попытаемся открыть файл test-cryp.
3. Во время процесса дешифрования осуществим остановку работы виртуальной машины.

```
[root@us1234 ~]# dd if=/dev/zero of=/root/test-crypt bs=1M count=1000
1000+0 записей получено
1000+0 записей отправлено
1048576000 байт (1,0 GB, 1000 MiB) скопирован, 0,992859 s, 1,1 GB/s
[root@us1234 ~]# /sbin/cryptsetup -y luksFormat --batch-mode /root/test-crypt
Введите парольную фразу для /root/test-crypt:
Парольная фраза повторно:
[root@us1234 ~]# cryptsetup luksOpen /root/test-crypt my_encrypted_volume
bash: cryptsetup: команда не найдена
[root@us1234 ~]# /sbin/cryptsetup luksOpen /root/test-crypt my_encrypted_volume
Устройство my_encrypted_volume уже существует.
[root@us1234 ~]# /sbin/cryptsetup luksOpen /root/test-crypt my_encrypted_volume1
Введите парольную фразу для /root/test-crypt:
```

Рисунок 9 – Работа с файлом test-cryp до выключения машины при дешифровании
Источник: анализ авторов

4. После выключения компьютера проверим наличие файла
5. Выведем список всех виртуальных блочных устройств, которые были созданы с помощью `dm-crypt` и которые находятся в каталоге `/dev/mapper/`.

В результате видно, что блочного устройства под названием `my_encrypted_volume1` нет. Это означает, что файл не дешифровался.

Проверим его наличие и выведем информации о нем в случае, если он до сих пор зашифрован. Обе команды сработали, что означает, что в случае выключения компьютера в процессе дешифрования, работа с файлом не прерывается, но сам файл не повреждается.

Для того, чтобы в этом убедиться, дешифруем файл в нормальном режиме. Команда открытия успешно сработала.

```
root@ruvds:~# su --
Password:
root@ruvds:~# ls /dev/mapper/
control
root@ruvds:~# ls -l /root/test-crypt
-rw-r--r-- 1 root root 1048576000 Sep  8 00:13 /root/test-crypt
root@ruvds:~# /sbin/cryptsetup luksDump /root/test-crypt
LUKS header information
Version:        2
Epoch:         3
Metadata area:  16384 [bytes]
Keyslots area:  16744448 [bytes]
UUID:          e21dd23-90ef-44f4-a759-d840a846d50e
Label:          (no label)
Subsystem:      (no subsystem)
Flags:          (no flags)

Data segments:
0: crypt
   offset: 1677216 [bytes]
   length: (whole device)
   cipher: aes-xts-plain64
   sector: 4096 [bytes]

Keyslots:
0: luks2
   Key:        512 bits
   Priority:    normal
   Cipher:      aes-xts-plain64
   Cipher key: 512 bits
   PBKDF:       argon2id
   Time cost:   4
   Memory:     1014008
   Threads:    2
   Salt:       0a 0c ea 00 70 37 9f 1f b6 46 96 4a e1 c8 91 12
               e0 70 d5 76 56 5d 8c ab 60 b5 50 86 99 fe d5 d1
   AF stripes: 4000
   AF hash:    sha256
   Area offset: 32768 [bytes]
   Area length: 258048 [bytes]
   Digest ID:  0

Tokens:
Digests:
0: pbkdf2
   Hash:      sha256
   Iterations: 131466
   Salt:      68 65 42 3b 64 d5 97 cd e2 44 c2 46 ac 9c 61 2b
               ed 3e 6f 36 a2 f7 c4 6d 82 9e a4 ba b9 34 de 0d
   Digest:    8e 1f cc 1f 64 5b 63 73 64 d6 5d 27 30 1a 7d 6c
               99 1b e0 8a 2c 53 60 39 9d 55 5f df 22 af 2a b3

root@ruvds:~# /sbin/cryptsetup luksOpen /root/test-crypt my_encrypted_volume1Введите парольную фразу для /root/test-crypt:
control my_encrypted_volume1
root@ruvds:~#
```

Рисунок 10 – Работа с файлом test-сгуп после выключения машины при дешифровании

Источник: анализ авторов

Заключение

В результате проведенного эксперимента можно подвести итог, что поддержка фоновой работы в системе `dm-crypt` в контексте прерывания процессов шифрования и дешифрования отсутствует. При выключении компьютера или в случае его неожиданной остановки работы процессы, связанные с шифрованием или дешифрованием данных, обрываются. Это означает, что операции не завершаются корректно, и в памяти могут остаться данные, которые не были зашифрованы или расшифрованы полностью.

Важно упомянуть, что несмотря на прерывание процессов, файлы остаются целостными и не повреждаются. Длительные операции шифрования и дешифрования обрабатываются по блокам, и только полностью завершённые блоки будут корректно записаны на диск.

Список литературы

1. .ruvds Шифрование данных на виртуальном сервере / ruvds [Электронный ресурс] // Хабр : [сайт]. — URL: <https://habr.com/ru/companies/ruvds/articles/535516/> (дата обращения: 07.09.2024).
2. Шифрование дисков в Linux / [Электронный ресурс] // Losst : [сайт]. — URL: <https://losst.pro/shifrovanie-diskov-v-linux?ysclid=m0u0duliz2845471585> (дата обращения: 08.09.2024).

3. Шифрование / [Электронный ресурс] // ESET NOD32 : [сайт]. — URL: <https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/shifrovaniye> (дата обращения: 17.09.2024).
4. Kernel Maintainer Team The Linux Kernel 6.11.0-rc7 dm-crypt / Kernel Maintainer Team [Электронный ресурс] // The Linux Kernel : [сайт]. — URL: <https://www.kernel.org/doc/html/latest/admin-guide/device-mapper/dm-crypt.html> (дата обращения: 08.09.2024).
5. dm-crypt/Encrypting an entire system / [Электронный ресурс] // archlinux : [сайт]. — URL: https://wiki.archlinux.org/title/Dm-crypt/Encrypting_an_entire_system (дата обращения: 08.09.2024).
6. Олег Власенко, Станислав Иевлев, Антон Ионов, Юрий Коновалов, Георгий Курячий, Виталий Липатов, Кирилл Маслинский, Алексей Новодворский, Александр Прокудин, Даниил Смирнов, Илья Трунин, Сергей Турчин, Анатолий Якушин и другие ALT Linux снаружи [Текст] / Олег Власенко, Станислав Иевлев, Антон Ионов, Юрий Коновалов, Георгий Курячий, Виталий Липатов, Кирилл Маслинский, Алексей Новодворский, Александр Прокудин, Даниил Смирнов, Илья Трунин, Сергей Турчин, Анатолий Якушин и другие — 1-е изд. — Москва: ДМК-пресс, 2006 — 196 с.
7. Уймин, А. Г. Периферийные устройства ЭВМ : Практикум / А. Г. Уймин. – Москва : Ай Пи Ар Медиа, 2023. – 429 с. – ISBN 978-5-4497-2079-5. – EDN KQQFAG.
8. Kondra1290 Script / Kondra1290 [Электронный ресурс] // GitHub : [сайт]. — URL: <https://github.com/Kondra1290/Script/blob/main/Script.txt> (дата обращения: 16.09.2024).
9. Потоки фонового шифрования InnoDB / [Электронный ресурс] // runebook : [сайт]. — URL: <https://runebook.dev/ru/docs/mariadb/innodb-background-encryption-threads/index> (дата обращения: 16.09.2024).

References

1. RUVDS Data encryption on a virtual server / ruvs [Electronic resource] // Habr : [website]. - URL: <https://habr.com/ru/companies/ruvs/articles/535516/> (accessed 07.09.2024).
2. Disk encryption in Linux / [Electronic resource] // Losst : [website]. - URL: <https://losst.pro/shifrovanie-diskov-v-linux?ysclid=m0u0duliz2845471585> (accessed 08.09.2024).
3. Encryption / [Electronic resource] // ESET NOD32 : [website]. — URL: <https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/shifrovaniye> (date of request: 09/17/2024).
4. Kernel Maintainer Team The Linux Kernel 6.11.0-rc7 dm-crypt / Kernel Maintainer Team [Electronic resource] // The Linux Kernel : [website]. - URL: <https://www.kernel.org/doc/html/latest/admin-guide/device-mapper/dm-crypt.html> (accessed 08.09.2024).
5. dm-crypt/Encrypting an entire system / [Electronic resource] // archlinux : [website]. - URL: https://wiki.archlinux.org/title/Dm-crypt/Encrypting_an_entire_system (date of application: 09/08/2024).
6. Oleg Vlasenko, Stanislav Ievlev, Anton Ionov, Yuri Konovalov, Georgy Kuryachy, Vitaly Lipatov, Kirill Maslinsky, Alexey Novodvorsky, Alexander Prokudin, Daniil Smirnov, Ilya Trunin, Sergey Turchin, Anatoly Yakushin and other ALT Linux shells [Text] / Oleg Vlasenko,

- Stanislav Ievlev, Anton Ionov, Yuri Konovalov, Georgy Kuryachy, Vitaly Lipatov, Kirill Maslinsky, Alexey Novodvorsky, Alexander Prokudin, Daniil Smirnov, Ilya Trunin, Sergey Turchin, Anatoly Yakushin and others — 1st ed. - Moscow: DMK-press, 2006 — 196 p.
7. Uymin, A. G. Peripheral computer devices : A practical course / A. G. Uymin. - Moscow : Ai Pi Ar Media, 2023. – 429 P. – ISBN 978-5-4497-2079-5. – EDN KQQFAG.
 8. Kondra1290 Script / Kondra1290 [Electronic resource] / / GitHub : [website]. - URL: <https://github.com/Kondra1290/Script/blob/main/Script.txt> (accessed: 16.09).
 9. InnoDB background encryption stream / [Electronic resource] // runebook : [website]. — URL: <https://runebook.dev/ru/docs/mariadb/innodb-background-encryption-threads/index> (date of application: 09/16/2024).
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.942

КЛЮЧЕВАЯ РОЛЬ ИССЛЕДОВАНИЙ В ОБЛАСТИ ДИНАМИКИ ПОЛЕТА, СИСТЕМ УПРАВЛЕНИЯ И МОДЕЛИРОВАНИЯ ДЛЯ РАЗВИТИЯ АВИАЦИОННЫХ НАУК

Кириллов Д.О.

ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА",
Санкт-Петербург, Россия (196210, город Санкт-Петербург, ул. Пилотов, д.38), e-mail:
dimanchik20130@gmail.com

Данная статья призвана собрать в себя краткие результаты исследований в области динамики полета, систем управления и моделирования аэродинамических характеристик летательных аппаратов гражданской авиации. Большое внимание уделяется имитационным моделям, используемым для анализа характеристик самолетов с высокой степенью инноваций с точки зрения архитектуры, систем или силовой установки. Кроме того, разработка и сертификация новых методов аэромеханического анализа и оптимизации, усовершенствованного моделирования, новых способов управления полетом и инструментов анализа динамики полета для различных рабочих процессов проектирования являются весьма важными факторами, которые расширили знания в данной области.

Ключевые слова: Аэродинамика, динамика полета, гражданская авиация, моделирование, системы управления.

THE KEY ROLE OF RESEARCH IN THE FIELD OF FLIGHT DYNAMICS, CONTROL SYSTEMS AND SIMULATION FOR THE DEVELOPMENT OF AVIATION SCIENCES.

Kirillov D.O.

"ST. PETERSBURG STATE UNIVERSITY OF CIVIL AVIATION NAMED AFTER AIR CHIEF
MARSHAL A.A. NOVIKOV", St. Petersburg, Russia (196210, St. Petersburg, ул. Pilotov, д.38), e-
mail: ¹Kvakolka885@gmail.com, ²drots2005@mail.ru, ³borovikovadasha05@mail.ru

This article is intended to collect brief results of research in the field of flight dynamics, control systems and modeling of aerodynamic characteristics of civil aviation aircraft. Much attention is paid to simulation models used to analyze the characteristics of aircraft with a high degree of innovation in terms of architecture, systems or power plant. In addition, the development and certification of new methods of aeromechanical analysis and optimization, advanced modeling, new flight control methods and flight dynamics analysis tools for various design workflows are very important factors that have expanded knowledge in this field.

Keywords: Aerodynamics, flight dynamics, civil aviation, modeling, control systems.

Введение

В развивающейся области исследований гражданской коммерческой авиации изучение динамики полета, систем управления и моделирования имеет ключевое значение для технологического прогресса. Действительно, эти области исследований имеют важное значение для повышения безопасности и экономичности современных воздушных судов, а также для поиска передовых и эффективных решений. Глубокое понимание и характеристика

динамика полета имеют фундаментальное значение для понимания и улучшения летно-технических характеристик воздушных судов. По мере развития авиации от самых простых до более сложных, экономичных и экологичных конструкций [1,2] точное прогнозирование и управление поведением самолета в различных условиях становится все более важным. Это важно не только для оптимизации конфигурации самолетов, но и для обеспечения устойчивости и управляемости, соответствующих строгим требованиям. Инновационные конфигурации, такие как предложенные в работах [3,4,5] требуют тщательной характеристики с точки зрения динамического поведения, прогнозов характеристик и перспектив безопасности.

Системы управления тесно связаны с динамикой полета. Сложные алгоритмы управления позволяют точно управлять все более сложными и автоматизированными системами самолета. Интеграция передовых технологий управления гарантирует, что самолеты могут безопасно и эффективно эксплуатироваться даже в сложных сценариях. Кроме того, взаимодействие между пилотами-людьми и автоматизированными системами становится все более актуальным, и исследования сосредоточены на оптимизации этой взаимосвязи для снижения рабочей нагрузки пилотов и повышения общей надежности. Наконец, моделирование играет ключевую роль в соединении теории и практики. Высокоточное моделирование позволяет исследователям и инженерам тестировать новые концепции, сертифицировать модели и прогнозировать характеристики [6,7]. Поскольку авиационная промышленность сталкивается с необходимостью снижения затрат и повышения безопасности, моделирование обеспечивает важнейшую платформу для тщательного тестирования без рисков и затрат, связанных с реальными испытаниями. Более того, проверенные платформы моделирования позволяют делать надежные прогнозы даже на самой ранней стадии проектирования, ускоряя разработку новых авиационных технологий, таких как новые силовые установки, гибридные электрические [8] или водородные силовые установки [9]. Развитие технологий моделирования позволяет исследовать новые рубежи в конструкции самолетов и эксплуатационных характеристиках, поддерживая стремление к инновациям.

Обзор опубликованных статей

В данной статье представлены 5 научных работ, в которых обсуждаются изучение динамики полета и моделирования, затрагивающие конкретные темы из разных областей. Ниже приводится краткое изложение этих исследований и их основных выводов.

Статья [10] использует специализированные инструменты моделирования для исследования характеристик региональных самолетов, оснащенных гибридными электрическими силовыми установками. В исследовании подчеркивается, что гибридные электрические самолеты демонстрируют отличные эксплуатационные характеристики по сравнению с обычными самолетами с двигателями внутреннего сгорания (ДВС), особенно с точки зрения соотношения полезной нагрузки и дальности полета. Исследование демонстрирует, что гибридная электрическая силовая установка дает значительные преимущества перед ДВС, включая снижение расхода топлива и увеличение дальности полета, особенно для коротких региональных полетов (около 450 километров). Эти результаты подчеркивают потенциал гибридных электрических технологий в снижении воздействия региональной авиации на окружающую среду. Кроме того, в исследовании подчеркивается

важность оптимизации стратегий управления энергопотреблением для дальнейшего повышения производительности.

Статья [11] представляет метод точного определения аэродинамических характеристик на ранней стадии проектирования самолета с использованием виртуальных летных испытаний в аэродинамической трубе. Авторская модель описывает влияние аэродинамических сил на полет, а их метод обеспечивает высокую точность, отличающуюся менее чем на 10% от обычных измерений в аэродинамической трубе. Этот подход позволяет проводить раннюю сертификацию аэродинамических моделей, способствуя сокращению цикла разработки и снижению затрат при проектировании самолетов. Метод особенно полезен для повышения точности динамических испытаний в аэродинамических трубах.

Статья [12] представляет имитационную модель для анализа динамики взлета самолета, подходящую для проектирования как традиционных, так и инновационных конфигураций самолетов. Модель включает в себя экранный эффект земли, который существенно влияет на характеристики самолета при взлете. В исследовании сравнивается обычный самолет с трубчатым крылом и самолет с замкнутой схемой крыла Box Wing, выявляются ключевые различия в их аэродинамическом поведении вблизи взлетно-посадочной полосы. Конструкция прямоугольного крыла демонстрирует преимущества в динамике подъемной силы, лобового сопротивления и тангажа из-за чувствительности к воздействию земли. Универсальность модели и низкие вычислительные затраты делают ее ценным инструментом на ранней стадии проектирования самолетов.

Статья [13] исследует аэродинамические характеристики новой концепции самолета с замкнутой схемой крыла Box Wing и двигателями, установленными сзади, с акцентом на преимущества поглощения пограничного слоя (Boundary-Layer Ingestion - BLI). Испытания в аэродинамической трубе с использованием моделей в масштабе 1:28 показали, что конфигурация BLI повысила эффективность тяги за счет снижения скорости реактивной струи и энергопотребления как минимум на 7,41% по сравнению с традиционными конструкциями. Однако BLI также внесла искажение потока, которое могло повлиять на характеристики. Эти результаты подчеркивают потенциал BLI в повышении эффективности аэродинамических двигателей, хотя необходимы дальнейшие исследования, чтобы полностью понять его влияние на реальные летно-технические характеристики самолета, особенно в полном масштабе и в реальных условиях полета.

Статья [14] представляет платформу виртуальных летных испытаний (Virtual Flight Testing - VFT) для крупномасштабных высокоскоростных аэродинамических труб для решения проблем нелинейного взаимодействия в аэродинамике, динамике полета и управлении при маневрах. VFT объединяет модель с тремя степенями свободы, приборы для измерения аэродинамических параметров, а также виртуальную систему управления, позволяющую реалистично моделировать маневры и проверять законы управления полетом. Платформа эффективно определяет связь тангажа и крена на больших углах атаки и проверяет стратегии управления для разделения этих движений. После сравнения с реальными полетными данными результаты подтверждают надежность VFT и его потенциал для снижения рисков и затрат на летные испытания.

Заключение

Исследования в области транспортной авиации постоянно сталкиваются со сложными и амбициозными новыми задачами. Новые концепции самолетов, типы силовых установок, методы управления самолетами и общие прорывные инновации все чаще изучаются, исследуются и разрабатываются. Изучение динамики полета всегда имело особое значение при исследовании поведения инновационных транспортных самолетов, оценке их характеристик устойчивости и управляемости, а также при оценке их эксплуатационных характеристик. В зависимости от используемого уровня точности, модели, методы и инструменты летного моделирования позволяют охарактеризовать аэромеханическое поведение самолета на любом этапе процесса проектирования, от начальных концептуальных этапов до самого продвинутого детального анализа. Такие модели имеют отношение к достижениям в различных областях транспортной авиации, таким как повышение безопасности полетов, оптимизация выполнения задач, разработка новых концепций эксплуатации воздушных судов и внедрение методов виртуальной сертификации. Эти области имеют решающее значение для авиационной науки, стимулируя разработку новых технологий, которые определяют будущее авиации.

Поскольку отрасль продолжает развиваться, исследования в этих областях должны оставаться приоритетом для обеспечения того, чтобы гражданская и коммерческая авиация могла отвечать требованиям безопасности, эффективности и изобретательности.

Список литературы

1. Платцер М. Ф. Взгляд на актуальность зеленой авиации // Прогресс в аэрокосмических науках. 2023. Т. 141. С. 100932.
2. Фикка А., Маруло Ф., Солло А. Открытое мышление для реализации концепции устойчивой "зеленой" авиации // Прогресс в аэрокосмических науках. 2023. Т. 141. С. 100928.
3. Оконкво П., Смит Х. Обзор развивающихся тенденций в проектировании самолетов со смешанным крылом // Прогресс в аэрокосмических науках. 2016. Т. 82. С. 1-23.
4. Абу Салем К., Чиполла В., Палайя Г., Бинанте В., Дзанетти Д. Основанный на физике междисциплинарный подход к предварительному проектированию и анализу характеристик самолета средней дальности с коробчатой архитектурой крыла // Аэрокосмическая промышленность. 2021. Т. 8. С. 292.
5. Кавалларо Р., Демази Л. Проблемы, идеи и инновации конфигураций со спаренным крылом: концепция из прошлого, возможность для будущего // Прогресс в аэрокосмических науках. 2016. Т. 87. С. 1-93.
6. Тай С., Ван Л., Ван Ю., Бу С., Юэ Т. Моделирование динамики полета и определение аэродинамических параметров при проведении виртуальных летных испытаний с четырьмя степенями свободы // Журнал AIAA. 2023. Т. 61. С. 2652-2665.
7. Томсон Д., Брэдли Р. Обратное моделирование как инструмент исследования динамики полета — принципы и приложения // Прогресс аэрокосмических наук. 2006. Т. 42. С. 174–210.
8. Абу Салем К., Палайя Г., Кварта А. А. Обзор технологий и конструкций гибридно-электрических самолетов: критический анализ и новые решения // Прогресс в аэрокосмических науках. 2023. Т. 141. С. 100924.

9. Адлер Э. Дж., Мартинс Дж. Р. Летательные аппараты на водородном топливе: фундаментальные концепции, ключевые технологии и воздействие на окружающую среду // Прогресс в аэрокосмических науках. 2023. Т. 141. С. 100922.
10. Палайя Г., Абу Салем К. Анализ эффективности полета гибридно-электрического регионального самолета // Аэрокосмическая промышленность. 2023. Т. 10. С. 246.
11. Тай С., Ван Л., Ван Ю., Лу С., Бу С., Юэ Т. Определение поперечно-направленных аэродинамических параметров летательных аппаратов на основе виртуальных летных испытаний в аэродинамической трубе // Аэрокосмическая промышленность. 2023. Т. 10. С. 350.
12. Абу Салем К., Палайя Г., Чиарелли М. Р., Бьянки М. Система моделирования взлета самолета с учетом аэродинамики наземного воздействия при концептуальном проектировании // Аэрокосмическая промышленность. 2023. Т. 10. С. 459.
13. Браво-Москера П. Д., Керон-Муньос Х. Д., Каталано Ф. М. Потенциальные двигательные и аэродинамические преимущества новой концепции самолета: экспериментальное исследование на низкой скорости // Аэрокосмическая промышленность. 2023. № 10. С. 651.
14. Ли Х., Ли Ю., Чжао З., Ван Х., Ян Х., Ма С. Высокоскоростная виртуальная летно-испытательная платформа для оценки эффективности маневров по тангажу // Аэрокосмическая промышленность. 2023. Т. 10. С. 962.

References

1. Platzer M. F. A perspective on the urgency for green aviation // Progress in Aerospace Sciences. 2023. T. 141. p. 100932.
2. Ficca A., Marulo F., Sollo A. An open thinking for a vision on sustainable green aviation // Progress in Aerospace Sciences. 2023. T. 141. p. 100928.
3. Okonkwo P., Smith H. Review of evolving trends in blended wing body aircraft design // Progress in Aerospace Sciences. 2016. T. 82. pp. 1–23.
4. Abu Salem K., Cipolla V., Palaia G., Binante V., Zanetti D. A Physics-Based Multidisciplinary Approach for the Preliminary Design and Performance Analysis of a Medium Range Aircraft with Box-Wing Architecture // Aerospace. 2021. T. 8. pp. 292.
5. Cavallaro R., Demasi L. Challenges, ideas, and innovations of joined-wing configurations: A concept from the past, an opportunity for the future // Progress in Aerospace Sciences. 2016. T. 87. pp. 1–93.
6. Tai S., Wang L., Wang Y., Bu C., Yue T. Flight dynamics modeling and aerodynamic parameter identification of four-degree-of-freedom virtual flight test // AIAA Journal. 2023. T. 61. pp. 2652–2665.
7. Thomson D., Bradley R. Inverse simulation as a tool for flight dynamics research—Principles and applications // Progress in Aerospace Sciences. 2006. T. 42. p. 174–210.
8. Abu Salem K., Palaia G., Quarta A. A. Review of hybrid-electric aircraft technologies and designs: Critical analysis and novel solutions // Progress in Aerospace Sciences. 2023. T. 141. p. 100924.
9. Adler E. J., Martins J. R. Hydrogen-powered aircraft: Fundamental concepts, key technologies, and environmental impacts // Progress in Aerospace Sciences. 2023. T. 141. p. 100922.

10. Palaia G., Abu Salem K. Mission Performance Analysis of Hybrid-Electric Regional Aircraft // Aerospace. 2023. T. 10. p. 246.
 11. Tai S., Wang L., Wang Y., Lu S., Bu C., Yue T. Identification of Lateral-Directional Aerodynamic Parameters for Aircraft Based on a Wind Tunnel Virtual Flight Test // Aerospace. 2023. T. 10. p. 350.
 12. Abu Salem K., Palaia G., Chiarelli M. R., Bianchi M. A Simulation Framework for Aircraft Take-Off Considering Ground Effect Aerodynamics in Conceptual Design // Aerospace. 2023. T. 10. p. 459.
 13. Bravo-Mosquera P. D., Cerón-Muñoz H. D., Catalano F. M. Potential Propulsive and Aerodynamic Benefits of a New Aircraft Concept: A Low-Speed Experimental Study // Aerospace. 2023. T. 10. p. 651.
 14. Li H., Li Y., Zhao Z., Wang X., Yang H., Ma S. High-Speed Virtual Flight-Testing Platform for Performance Evaluation of Pitch Maneuvers // Aerospace. 2023. T. 10. p. 962.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.942

СОВРЕМЕННЫЕ ПРОБЛЕМЫ АЭРОДИНАМИКИ ВОЗДУШНЫХ СУДОВ

Кириллов Д.О.

ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА", Санкт-Петербург, Россия (196210, город Санкт-Петербург, ул. Пилотов, д.38), e-mail: dimanchik20130@gmail.com

В статье рассматриваются современные проблемы аэродинамики воздушных судов, связанные с повышением их экономичности, безопасности и снижением экологического воздействия. Обсуждаются некоторые основные тенденции классической компоновки маршрутных самолетов, а также особенности некоторых перспективных летательных аппаратов. Особое внимание уделяется снижению лобового сопротивления и повышению аэродинамического качества воздушного судна за счет использования передовых разработок.

Ключевые слова: Аэродинамика самолета, гражданская авиация, воздушное судно.

MODERN PROBLEMS OF AIRCRAFT AERODYNAMICS.

Kirillov D.O.

"ST. PETERSBURG STATE UNIVERSITY OF CIVIL AVIATION NAMED AFTER AIR CHIEF MARSHAL A.A. NOVIKOV", St. Petersburg, Russia (196210, St. Petersburg, ул. Pilotov, д.38), e-mail: ¹Kvakolka885@gmail.com, ²drots2005@mail.ru, ³borovikovadasha05@mail.ru

The article deals with modern problems of aircraft aerodynamics related to increasing their efficiency, safety and reducing environmental impact. Some of the main trends in the classical layout of route aircraft are discussed, as well as the features of some promising aircraft. Special attention is paid to reducing drag and improving the aerodynamic quality of the aircraft through the use of advanced developments.

Keywords: Aircraft aerodynamics, civil aviation, aircraft.

Введение

В ходе развития авиационной науки и технического прогресса воздушные суда улучшались по нескольким параметрам, таким как экономичность, безопасность полетов и экологическое воздействие на окружающую среду (снижение уровня шума и загрязнения). Например, на Рисунке 1 наглядно представлено развитие воздушных судов с точки зрения экономичности.

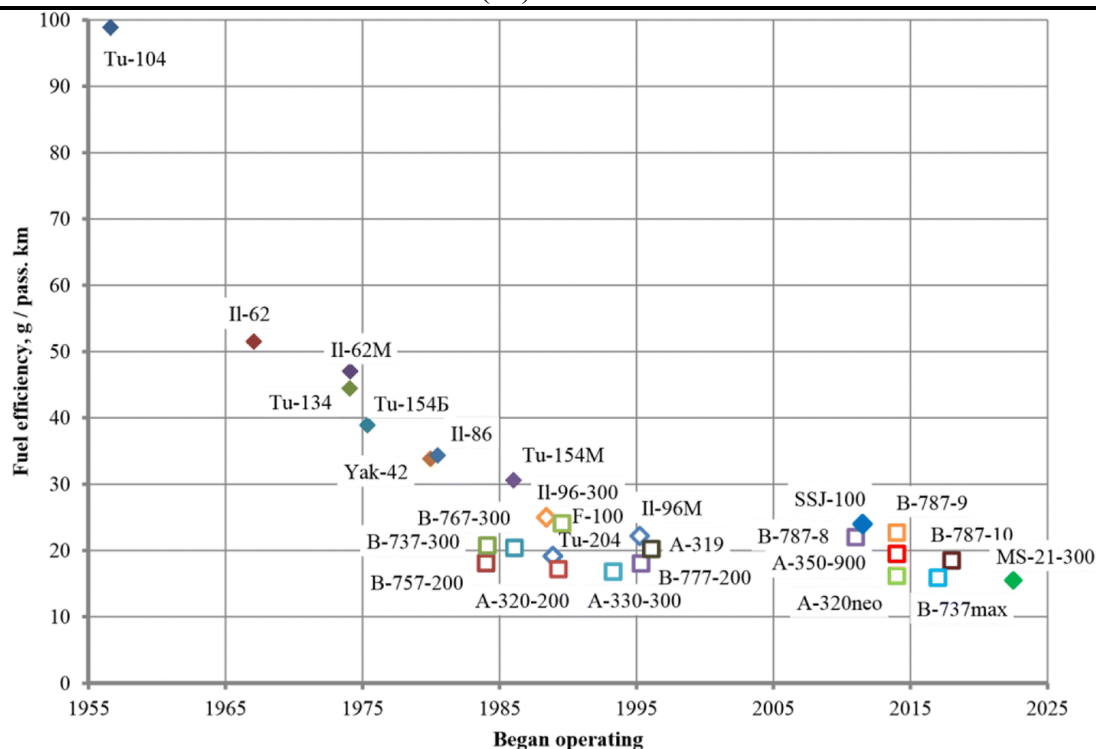


Рисунок 1. - Изменение топливной эффективности воздушных судов на маршруте с течением времени

Исследователи из различных российских организаций прогнозируют развитие науки и технологий в авиации в будущем в различных областях. Так количество авиационных инцидентов должно сократиться в 8,5 раз к 2030 году, а также ожидается снижение уровня шума и выбросов в атмосферу. В свою очередь, задачи аэродинамической науки определяются необходимостью улучшения этих показателей.

Формула дальности полета Бреге

$$L \sim \frac{K \cdot M}{C_E} \ln \frac{G_1}{G_0} \quad (1)$$

позволяет определить ключевые аэродинамические параметры, которые необходимо улучшить. Прежде всего, это увеличение крейсерского аэродинамического качества (K), крейсерского числа Маха (M), а также снижение удельного расхода топлива и минимизация веса конструкции (G_1 , G_0 - вес самолета в начале и в конце полета).

В свою очередь, максимальное отношение подъемной силы к лобовому сопротивлению может быть достигнуто следующим образом:

$$K_{max} = \frac{1}{2} \sqrt{\frac{\pi \lambda}{C_f \bar{S}_{вл}}} \quad (2)$$

где λ – эффективный коэффициент удлинения крыла, C_f – коэффициент трения обшивки, $\bar{S}_{вл}$ – площадь увлажненной поверхности самолета, деленная на площадь крыла.

Таким образом, существуют еще три направления улучшения экономических характеристик летательного аппарата, связанные с аэродинамикой: увеличение удлинения, уменьшение сопротивления трения и уменьшение относительной площади смачивания летательного аппарата.

Основными составляющими полного крейсерского сопротивления современных самолетов являются сопротивление трения, сопротивление, обусловленное подъемной силой, и волновое сопротивление. Влияние первых двух в области околозвуковых скоростей достигает 50 и 40% от полного сопротивления соответственно. Это показывает, что снижение сопротивления трения является основным источником увеличения аэродинамического качества самолета. Следует отметить, что увеличение аэродинамического качества связано не только со снижением лобового сопротивления, но и с увеличением грузоподъемности за счет улучшения формы и поиска новых компоновочных решений. Для успешного решения поставленных задач и обеспечения перспективного технического задела необходимы своевременные моно и мультидисциплинарные научные исследования.

Основные направления развития классической компоновки самолета

Следует признать, что аэродинамический потенциал современных сверхкритических крыльев находится на пределе, поэтому для продвижения вперед необходимо исследовать и внедрять некоторые новые перспективные технологии. Среди них следует выделить следующие:

- Адаптивные крылья для околозвуковых скоростей;
- Новые типы законцовок крыла;
- Организация ламинарного обтекания хвостового оперения, гондол двигателей, а затем и крыльев;
- Снижение сопротивления турбулентному трению;
- Усовершенствованные типы механизации;
- Активные и пассивные системы управления потоком (мини и макроустройства, синтетические форсунки, приводы и т.д.);
- Активное управление вектором тяги;
- Переход к компоновкам с умеренным запасом устойчивости и слегка неустойчивой компоновкой.

Проблема увеличения крейсерской скорости (числа Маха) связана с преодолением интенсивного нарастания лобового сопротивления, возникающего из-за наличия интенсивной ударной волны, замыкающей локальную область сверхзвукового потока. Использование сверхкритических профилей и крыльев позволило перейти к более высокому числу Маха при заданном угле стреловидности и относительной толщине крыла. В настоящее время современные методы аэродинамического проектирования позволяют оттянуть упомянутое увеличение лобового сопротивления до более высоких скоростей, используя глобальную численную оптимизацию аэродинамической формы крыла для заданной относительной толщины и формы в плане. Дальнейшее увеличение скорости полета, скорее всего, возможно только с помощью методов управления потоком и воздействия на ударную волну. Это могут быть, например, какие-то специальные приводы или вихревые генераторы [1], которые создают дополнительный вихрь или тангенциальную струю, обдувающую поверхность крыла [2, 3].

Чаше всего за более высокие скоростные возможности сверхкритических крыльев необходимо платить увеличением относительной толщины крыла с целью снижения веса конструкции или увеличения удлинения, что, как известно, и приводит к уменьшению лобового сопротивления. Ту-204 и Самолеты Ил-96 с удлинением крыла $\lambda = 9,2 \div 10$

демонстрируют такой подход к аэродинамическому проектированию, превосходя своих предшественников Ту-154 и Ил-86 по максимальному значению аэродинамического качества более чем 2 единицы. Следует отметить, что использование сверхкритических крыльев является причиной увеличения момента тангажа при движении носом вниз, что приводит к увеличению аэродинамического сопротивления. Однако эти потери могут быть снижены за счет некоторого снижения продольной устойчивости самолета и использования современных систем управления полетом, обеспечивающих безопасность.

Использование композитов в конструкции крыла открывает новые возможности для аэродинамического проектирования. С одной стороны, вес планера может быть уменьшен, с другой стороны, удлинение крыла может быть увеличено при том же весе конструкции. Прогнозирование летно-технических характеристик самолета показывает, что удлинение увеличивается. Именно поэтому для российского пассажирского самолета нового поколения МС-21 было реализовано рекордное удлинение крыла с $\lambda = 11,45$. Увеличение удлинения приводит к увеличению коэффициента подъемной силы, соответствующего максимальному аэродинамическому качеству.

Увеличение удлинения крыла приводит к увеличению веса крыла за счет уменьшения хорд и толщины. Одним из возможных способов снижения веса может быть использование дополнительных опорных элементов - подкосов крыла (Рисунок 2). В последнее время эта конфигурация интенсивно исследуется [4-7]. Предварительные расчеты показали, что при использовании таких элементов в конструкции самолета можно было бы достичь оптимального удлинения крыла до 14-15, однако для подтверждения таких оценок требуются более глубокие исследования.



Рисунок 2. - Компоновка самолета с подкосами крыла

Следует отметить, что дальнейшее увеличение удлинения, а, следовательно, и размаха крыльев ограничено размерами существующих рулевых дорожек и ангаров. Одним из возможных решений этой проблемы является использование вертикальных или

складывающихся законцовок крыла, что позволяет увеличить эффективное удлинение крыла при ограниченном размахе.

Важным элементом для повышения уровня аэродинамического сопротивления компоновки является оптимальное расположение мотогондол, что весьма актуально в связи с тенденцией увеличения передаточного числа и размеров двигателей в перспективе. Следует отметить, что двигатели с высокой степенью двухконтурности имеют меньший расход топлива и более низкий уровень шума, но оказывают негативное влияние на обтекание корпуса самолета, включая фазы взлета и посадки, из-за ограничений по размаху и дальности выдвижения корневой части предкрылка. Кроме того, крупногабаритные двигатели мотогондолы, расположенные под крылом, требуют более длинных стоек шасси, что приводит к увеличению веса конструкции. Применение процедур оптимизации позволяет значительно снизить негативное взаимодействие мотогондол. Потеря максимальной подъемной силы при использовании недостаточно эффективных подъемно-транспортных устройств может быть компенсирована, например, применением струйного обдува в зоне соединения крыла с пилоном.

Разработана техническая концепция самолета интегральной компоновки с силовой установкой, распределенной по конструкции крыла (Рисунок 3). Идея распределенной силовой установки полностью рассмотрена в диссертационном отчете [8]. Экспериментальные исследования разработанной модели показали, что такой способ интеграции силовой установки в конструкцию планера обеспечивает увеличение отношения подъемной силы к лобовому сопротивлению примерно на 15% по сравнению с классической компоновкой.

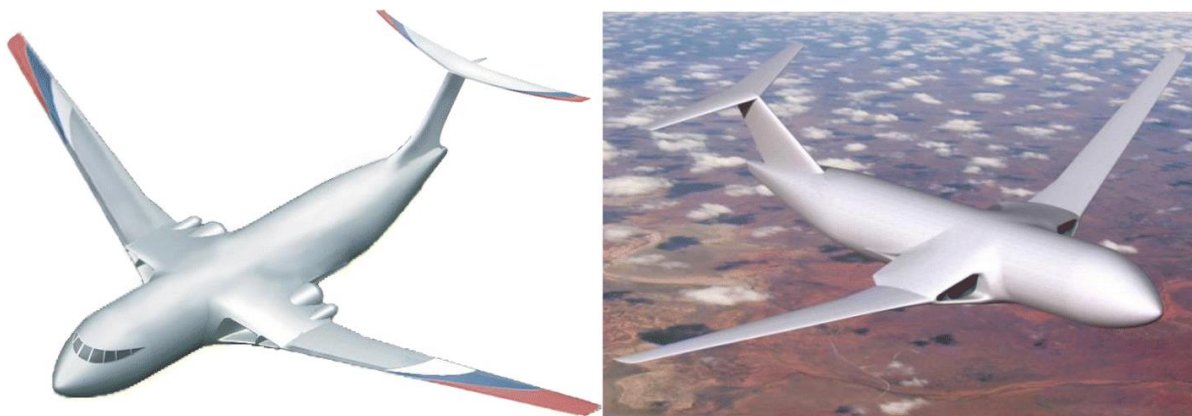


Рисунок 3. - Самолет с силовой установкой, встроенной в конструкцию крыла

Заключение

Современные проблемы аэродинамики воздушных судов остаются ключевым фактором для дальнейшего развития авиационной техники. Выделены перспективные технологии, которые должны быть внедрены для совершенствования аэродинамической компоновки пассажирских самолетов. Основные направления исследований и разработок, такие как улучшение аэродинамического качества, снижение сопротивления трению и внедрение новых конструктивных решений, направлены на повышение экономичности и снижение негативного воздействия на окружающую среду.

В будущем, с внедрением адаптивных технологий и интеграцией новых материалов, ожидается существенное улучшение летно-технических характеристик воздушных судов.

Перспективы развития аэродинамики включают в себя как классические методы оптимизации, так и инновационные подходы, такие как активное управление потоком и использование встроенной силовой установки. Все это способствует более эффективной и безопасной эксплуатации воздушных судов, одновременно снижая экологическое влияние и улучшая эксплуатационные параметры.

Список литературы

1. Брутян, Мурад Абрамович. Задачи управления течением жидкости и газа : монография / М. А. Брутян ; ЦАГИ, Центральный аэрогидродинамический ин-т им. проф. Н. Е. Жуковского. - Москва : Наука, 2015.
2. Investigation of the flow control of the transonic profile using tangential jet blowing / K. A. Abramova, M. A. Brutyan, S. V. Lyapunov [et al.] // 6th European Conference on Aeronautics and Space Sciences (EUCASS), Poland, Krakow, June 29 – December 03 in 2015. – Poland, Krakow: Airbus Group, 2015. – pp. 25-26. – PUBLISHING HOUSE XGOHPT.
3. Петров А. В. Энергетические методы увеличения подъемной силы крыла / А.В. Петров. — Москва : Физматлит, 2011. — 402 с.
4. Carrier G., Atino O., Decouan S., Chantre-Jervois J.-L., Liozun S., Paluch V., Rodde A.-M. and Toussaint S. A study of the configuration of a wing with struts for future commercial vehicles. // In ICAS 2012-597
5. Ko A, Mason W.H. and Grossman B. Transonic aerodynamics of the joint of wing supports. // In AIAA-2003-4062
6. Gern F., KO A., Grossman B., Haftka R., Kapania R.K. and Mason V. Weight reduction during transportation due to MDO: Transonic wing transport with struts. // In AIAA-2005-4667
7. Seber G., Ran H., Shets Ya.A. and Mavris D.N. Multidisciplinary optimization of aircraft design with a truss wing with improved aerodynamic analysis. // In AIAA-2011-3179.
8. Hajehzade, A. Analysis of a distributed propulsion system located above the wing. // Diploma report. Published by: Delft University of Technology, 2018.

References

1. Brutyan, Murad Abramovich. Tasks of controlling the flow of liquid and gas : monograph / M. A. Brutyan ; TsAGI, Central Aerohydrodynamic Institute named after Prof. N. E. Zhukovsky. - Moscow : Nauka, 2015.
2. Investigation of the flow control of the transonic profile using tangential jet blowing / K. A. Abramova, M. A. Brutyan, S. V. Lyapunov [et al.] // 6th European Conference on Aeronautics and Space Sciences (EUCASS), Poland, Krakow, June 29 – December 03 in 2015. – Poland, Krakow: Airbus Group, 2015. – pp. 25-26. – PUBLISHING HOUSE XGOHPT.
3. Petrov A.V. Energy methods of increasing wing lift / A.V. Petrov. — Moscow : Fizmatlit, 2011. — p.402
4. Carrier G., Atino O., Decouan S., Chantre-Jervois J.-L., Liozun S., Paluch V., Rodde A.-M. and Toussaint S. A study of the configuration of a wing with struts for future commercial vehicles. // In ICAS 2012-597
5. Ko A, Mason W.H. and Grossman B. Transonic aerodynamics of the joint of wing supports. // In AIAA-2003-4062

6. Gern F., KO A., Grossman B., Haftka R., Kapania R.K. and Mason V. Weight reduction during transportation due to MDO: Transonic wing transport with struts. // In AIAA-2005–4667
 7. Seber G., Ran H., Shets Ya.A. and Mavris D.N. Multidisciplinary optimization of aircraft design with a truss wing with improved aerodynamic analysis. // In AIAA-2011–3179.
 8. Hajehzade, A. Analysis of a distributed propulsion system located above the wing. // Diploma report. Published by: Delft University of Technology, 2018.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 355.232.6

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ОПЕРАЦИЯМИ ВВС США

Яковицкий С.А., Иванов А.А., ¹Вавринюк С.А.

ФГКОУ ВО «ВОЕННАЯ ОРДЕНОВ ЖУКОВА И ЛЕНИНА КРАСНОЗНАМЕННАЯ АКАДЕМИЯ СВЯЗИ ИМЕНИ МАРШАЛА СОВЕТСКОГО СОЮЗА С.М.БУДЕННОГО» МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, Санкт-Петербург, Россия (194064, город Санкт-Петербург, Тихорецкий пр-кт, д.3), e-mail: ¹ logoshik@mail.ru

Командованием ВВС США продолжается проведение комплекса мероприятий по совершенствованию системы управления информационными операциями. В связи с возрастанием угроз в кибернетическом пространстве со стороны России и Китая принято решение о повышении статуса структур управления кибернетическими операциями в ВВС, до уровня отдельного командования, непосредственно подчиненного министру и начальнику штаба ВВС.

Ключевые слова: Авиакрыло, боевые действия в электромагнитном спектре, военно-воздушные силы, информационная война, кибероперация, командование, операционная среда, операция, Объединенная боевая информационно-управляющая система во всех сферах, самолет, радиоэлектронная борьба.

IMPROVING THE U.S. AIR FORCE INFORMATION OPERATIONS MANAGEMENT SYSTEM

Yakovitsky S.A., Ivanov A.A., ¹ Vavrinyuk S.A.

MILITARY ORDER OF ZHUKOV AND LENIN RED BANNER ACADEMY OF COMMUNICATIONS NAMED AFTER MARSHAL OF THE SOVIET UNION S.M. BUDYONNY OF THE MINISTRY OF DEFENSE OF THE RUSSIAN FEDERATION, St. Petersburg, Russia (194064, St. Petersburg, Tikhoretsky prospekt, 3), e-mail: ¹ logoshik@mail.ru

The US Air Force Command continues to carry out a set of measures to improve the information operations command structure. Due to the increasing threats in the cyber space from Russia and China, it was decided to raise the status of the cyber operations command structures in the Air Force to the level of a separate Command directly subordinate to the Minister and Chief of Staff of the Air Force.

Keywords: Air wing, Electromagnetic Spectrum Warfare, Air Force, Information Warfare, cyber operation, Command, operational environment, operation, Joint All-Domain Command and Control, aircraft, Electronic Warfare.

Командованием ВВС США в настоящее время уделяется большое внимание проведению комплекса мероприятий по совершенствованию системы управления информационными операциями. Оно в отличие от командований других видов вооруженных сил (ВС) США пошло по пути интеграции управления силами и средствами информационных операций. Процесс поиска оптимальных структур продолжается уже около 5 лет.

Так, в начале в октябре 2019 года на базе бывших 24 и 25 воздушных армий (ВА) ВВС, отвечавших соответственно за кибернетические операции и разведывательные операции, была сформирована новая 16 ВА ВВС (кибернетическое командование) (авиабаза Лэклэнд, штат Техас).



Эмблема 16 ВА

Основная цель ее создания было объединение всех сил и средств ведения информационных операций под единым управлением. В задачи 16 ВА вошли: проведение операций в кибернетическом пространстве, разведывательных, психологических операций, РЭБ, операций (действий) по взаимодействию с гражданской администрацией и общественностью, метеорологической разведки, специальной разведки по соблюдению международных договоров. Командование ВВС рассматривало создание 16 ВА как важнейший эксперимент в ВВС, который поможет в создании Объединенной боевой информационно-управляющей системы во всех сферах (Joint All-Domain Command and Control) в рамках подготовки к ведению

многосферных операций [1].

Следует отметить, что в каждый вид вооруженных сил США пошел по своему пути интеграции своих сил и средств, подготовки к проведению всего спектра информационных операций. Так, в Сухопутных войсках и Военно-морских силах США с 2019 года были созданы командования кибернетических операций, командования разведки существовали до этого и продолжают функционировать раздельно. Их возглавляют разные командующие. В морской пехоте созданы командования киберопераций, космическое, разведывательное, а с января 2023 года – новое информационное командование. Все эти четыре командования, несмотря на то, что они отдельные, возглавляется одним генералом. Исследования по поиску оптимальных структур управления продолжается во всех видах ВС.

В марте 2020 года в результате объединения 624 и 625 оперативных центров 24 и 25 ВА соответственно, ответственных за координацию операций в кибернетическом пространстве и проведение разведывательных операций, в составе 16 ВА был создан 616 оперативный центр информационной войны. Основная его задача – оперативное управление всеми силами с средствами информационной войны ВВС. Данный орган управления рассматривался как важнейший в условиях повышения уровня противостояния с Россией и Китаем в информационной области.

В настоящее время 16 ВА включает:

- 616 оперативный центр;
- 67, 688 крылья боевых действий в кибернетическом пространстве;
- 9 разведывательное авиакрыло (на вооружении 21 самолет U-2S);
- 55 авиакрыло (на вооружении 17 самолетов RC-135V/W, 2 RC-135U, 3 RC-135S, 2 OC-135, 1 WC-135, 12 EC-130H*);
- 70, 363, 480 крылья разведывательных операций;
- 319 разведывательное авиакрыло БпЛА (на вооружении 12 БпЛА RQ-4B);
- 557 крыло метеорологической разведки.

Рассматривается вопрос о формировании единого центра управления информационными операциями ВВС. Пока этот вопрос прорабатывается концептуально [2].

За прошедшие годы командующий 16 ВА неоднократно высказывался, что руководству так и не удалось добиться желаемого эффекта - интеграции сил и средств в ходе проведения боевых действий/операций в виду их разного предназначения и подчиненности.

В очередном отчете аналитического центра «RAND Corporation» от 30.07.2024 г. командование ВВС было подвергнуто жесткой критике. В документе отмечено, что командование ВВС рассматривает информационные операции как второстепенные, уделяя основное внимание боевым операциям. До сих пор не разработаны практические требования и функции для всех структур, участвующих в проведении информационных операций и обеспечивающих структур (организаций). Информационная война включает множество компонентов, а летный состав ВВС не имеет необходимой подготовки и квалификации по ее комплексному ведению. «Поле боя перегружено административно-организационными, управленческими нормативами и указаниями. Несмотря на все организационно-штатные решения, единого главного органа управления всеми силами и средствами информационных операций нет. С другой стороны, наличие таких объединенных, подготовленных структур может создать высокую уязвимость системы» [1]. Современные боевые авиационные средства могут быть выведены из строя в результате кибернетических атак и действий противника в электромагнитном спектре. Дезинформация может привести к ложному нацеливанию, а компрометация системы управления вообще к перехвату управления со стороны противника. На проводившихся в последнее время учениях ВВС вопросы информационного воздействия со стороны противника отрабатывались условно (по имитационным вводным), отдавая приоритет боевому применению авиации. Личный состав и штабы не готовы к действиям в условиях реального воздействия противника в информационном пространстве. С целью устранения имеющихся проблем аналитическим центром RAND были сформированы предложения.

Ряд военных экспертов полагает, что выбранный ВВС путь является тупиковым. В тоже время следует отметить, что командованием морской пехоты США создаются аналогичные ВВС структуры управления силами и средствами для ведения информационных операций [3].

В настоящее время в штабе ВВС управление разведки (A2) и управление связи и сетевых технологий (A6) объединены в единое управление (A2/6), которое возглавляет трехзвездный генерал. Он является заместителем начальника штаба ВВС по разведке, наблюдению, операциям в кибернетическом пространстве.

В целях повышения значимости сил и средств кибернетических операций, 28 августа 2024 года было официально объявлено о разделении данного управления. Управление A2 вновь будет сконцентрировано на вопросах разведки, наблюдения и рекогносцировки. Вероятно, силы и средства разведки будут выведены из состава 16 ВА в отдельную структуру. Управление A6 кроме вопросов связи, сетевых технологий, будет решать задачи в кибернетическом пространстве. 16 ВА (кибернетическое командование) сохранится и будет поднят ее статус до уровня командования (кибернетической службы) ВВС, подчиняющейся непосредственно начальнику штаба и министру ВВС.

Изменения планируется провести до весны 2025 года.

Принимаемые меры направлены на повышение роли кибербезопасности ВВС в будущем конфликте, который связан с ростом угроз, исходящих со стороны Китая. США считают 2027 год вероятным для вторжения Китая на Тайвань. Именно под этим предлогом Пентагон активизировал военные приготовления, а также информационную кампанию по дискредитации КНР.

** - с 2023 года происходит снятие с вооружения самолетов РЭБ EC-130H «Compass Call», выработавших свой ресурс и морально устаревших. Самолеты будут заменены на новые самолеты РЭБ EC-37B «Compass Call».*

Список литературы

1. Яковицкий С.А., Голубенко Н.Ю., Вавринюк С.А. Развертывание элементов боевой информационно-управляющей системы ВВС США "ABMS" Актуальные вопросы борьбы с преступлениями. 2023. № 1. С. 11-14.
2. <https://defensescoop.com/>(Дата обращения 30.08.2024 г.).
3. <https://www.airandspaceforces.com/>(Дата обращения 31.08.2024 г.).

References

1. Yakovitsky S.A., Golubenko N.Yu., Vavrinyuk S.A. Identification of elements of the combat information and control system of the US Air Force "ABMS" Topical issues of the fight against prestige. 2023. No. 1. pp. 11-14.
 2. <https://defensescoop.com/>(Accessed 30.08.2024).
 3. <https://www.airandspaceforces.com/>(Accessed 08/31/2024).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.942.2

УСТОЙЧИВЫЙ БЛОКЧЕЙН. ПУТИ МИНИМИЗАЦИИ ЭНЕРГОПОТРЕБЛЕНИЯ

Марква Т.Д.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: norm_staffchik@mail.ru

Блокчейн-технология, несмотря на свои преимущества в обеспечении безопасности и децентрализации, сталкивается с проблемой высокого энергопотребления и значительного углеродного следа. Настоящая статья исследует пути минимизации энергозатрат и углеродного следа блокчейн-систем с целью обеспечения их устойчивого развития. Рассматриваются различные подходы, включая переход на альтернативные консенсусные механизмы, оптимизацию аппаратного обеспечения, использование возобновляемых источников энергии и применение офсетных программ для компенсации выбросов углерода. Авторы анализируют преимущества и ограничения каждого подхода, а также предлагают комплексные стратегии для достижения экологической устойчивости блокчейн-систем.

Ключевые слова: Блокчейн, энергопотребление, углеродный след, устойчивое развитие, консенсусные механизмы, возобновляемые источники энергии, офсетные программы.

A STABLE BLOCKCHAIN. WAYS TO MINIMIZE ENERGY CONSUMPTION

Markva T.D.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: norm_staffchik@mail.ru

Blockchain technology, despite its advantages in ensuring security and decentralization, faces the problem of high energy consumption and a significant carbon footprint. This article explores ways to minimize the energy consumption and carbon footprint of blockchain systems in order to ensure their sustainable development. Various approaches are being considered, including the transition to alternative consensus mechanisms, hardware optimization, the use of renewable energy sources and the use of offset programs to offset carbon emissions. The authors analyze the advantages and limitations of each approach, as well as propose comprehensive strategies to achieve environmental sustainability of blockchain systems.

Keywords: Blockchain, energy consumption, carbon footprint, sustainable development, consensus mechanisms, renewable energy sources, offset programs.

Введение

Блокчейн-технология, основанная на принципах децентрализации, прозрачности и безопасности, привлекла значительное внимание в различных отраслях, включая финансы, логистику, здравоохранение и многие другие. Однако, несмотря на свои преимущества, блокчейн-системы сталкиваются с серьезной проблемой высокого энергопотребления и значительного углеродного следа. Энергозатраты на поддержание работы блокчейн-сетей и майнинг криптовалют являются предметом беспокойства с точки зрения экологической устойчивости и воздействия на окружающую среду.

Энергопотребление и углеродный след блокчейн-систем

Блокчейн-технология, основанная на принципах децентрализации и распределенного реестра, требует значительных вычислительных мощностей и, соответственно, высокого энергопотребления. Ключевую роль в обеспечении безопасности и консенсуса в блокчейн-сетях играют консенсусные механизмы, наиболее распространенным из которых является механизм "Доказательства выполнения работы" (Proof-of-Work, PoW). PoW требует от майнеров решения сложных вычислительных задач для добавления нового блока в цепочку, что сопряжено с огромными затратами энергии. Согласно оценкам, глобальное энергопотребление сети Биткоин, крупнейшей криптовалюты, основанной на PoW, в 2022 году составляло около 127 ТВт*ч в год, что сопоставимо с энергопотреблением таких стран, как Нидерланды или Объединенные Арабские Эмираты.

Высокое энергопотребление блокчейн-систем также приводит к значительному углеродному следу, поскольку значительная часть энергии для майнинга криптовалют по-прежнему вырабатывается из ископаемых видов топлива, таких как уголь, нефть и природный газ. Согласно исследованиям, углеродный след сети Биткоин в 2022 году оценивался примерно в 69 миллионов метрических тонн CO₂, что эквивалентно выбросам небольшой страны. Это связано с тем, что процесс майнинга Биткоина требует интенсивных вычислений, которые потребляют огромное количество электроэнергии, производимой преимущественно из ископаемых видов топлива. [3, с.669]

Помимо Биткоина, существует множество других блокчейн-проектов и криптовалют, которые также имеют значительный углеродный след. Например, энергопотребление сети Ethereum, второй по популярности криптовалюты, оценивается примерно в 78 ТВт*ч в год, что эквивалентно углеродному следу около 35 миллионов метрических тонн CO₂. Другие крупные блокчейн-сети, такие как Bitcoin Cash, Litecoin и Monero, также вносят свой вклад в общее энергопотребление и углеродный след. [4, с.115]

Стоит отметить, что энергопотребление и углеродный след блокчейн-систем не ограничиваются только майнингом криптовалют. Сами узлы, поддерживающие работу распределенных реестров, также требуют значительных вычислительных мощностей и, следовательно, энергозатрат. Кроме того, необходимо учитывать энергопотребление, связанное с производством и утилизацией оборудования для майнинга, а также с охлаждением майнинговых ферм.

В целом, высокое энергопотребление и значительный углеродный след блокчейн-систем являются серьезными проблемами, которые необходимо решать для обеспечения экологической устойчивости и минимизации негативного воздействия на окружающую среду. Поиск путей снижения энергозатрат и переход на использование возобновляемых источников энергии являются ключевыми задачами для развития экологически чистых и устойчивых блокчейн-технологий. [5, с.500]

Пути минимизации энергопотребления

Для решения проблемы высокого энергопотребления блокчейн-систем необходимо рассмотреть комплексный подход, включающий в себя различные стратегии и методы. Одним из наиболее перспективных путей является переход на альтернативные консенсусные

механизмы, которые не требуют значительных вычислительных мощностей и, следовательно, снижают энергопотребление.

Наиболее распространенным альтернативным механизмом является "Доказательство доли владения" (Proof-of-Stake, PoS). В отличие от PoW, в PoS для валидации транзакций и создания новых блоков используется алгоритм случайного выбора узлов, пропорциональный их доле в общем пуле криптовалюты. Этот механизм не требует решения сложных вычислительных задач, что значительно снижает энергозатраты по сравнению с PoW. Согласно оценкам, переход на PoS может сократить энергопотребление блокчейн-сети более чем на 99%.

Помимо PoS, существуют и другие перспективные консенсусные механизмы, такие как "Доказательство авторитета" (Proof-of-Authority, PoA), "Доказательство истории" (Proof-of-History, PoH) и "Доказательство пространства" (Proof-of-Space, PoSpace). Каждый из них имеет свои преимущества и ограничения, и выбор подходящего механизма зависит от конкретных требований и особенностей блокчейн-системы.

Оптимизация аппаратного обеспечения, используемого для майнинга и поддержки работы блокчейн-сетей, также может внести значительный вклад в снижение энергопотребления. Использование более энергоэффективных процессоров, графических ускорителей и специализированных чипов для майнинга может существенно сократить энергозатраты. Кроме того, важным аспектом является оптимизация систем охлаждения и энергоснабжения майнинговых ферм. Применение передовых технологий охлаждения, таких как жидкостное охлаждение или иммерсионное охлаждение, может значительно повысить энергоэффективность.

Другие подходы к снижению энергопотребления включают в себя сжатие данных и оптимизацию протоколов передачи данных в блокчейн-сетях, а также использование более эффективных алгоритмов шифрования и хеширования. Кроме того, внедрение технологий распределенных вычислений и параллельной обработки данных может снизить нагрузку на отдельные узлы и, следовательно, уменьшить их энергопотребление.

Помимо технологических решений, важную роль играет также повышение осведомленности и образование участников блокчейн-сообщества о проблеме энергопотребления и ее влиянии на окружающую среду. Поощрение использования энергоэффективных практик и "зеленых" технологий, а также стимулирование исследований и разработок в этой области может способствовать созданию более устойчивых блокчейн-систем. [1, с.643]

В целом, минимизация энергопотребления блокчейн-систем требует комплексного подхода, включающего в себя как технологические инновации, так и изменения в области регулирования, образования и повышения осведомленности. Только объединив усилия всех заинтересованных сторон, мы сможем создать действительно устойчивые и экологически чистые блокчейн-технологии.

Пути минимизации углеродного следа

Наряду с сокращением энергопотребления, важной задачей является минимизация углеродного следа блокчейн-систем. Углеродный след напрямую связан с использованием ископаемых видов топлива для выработки электроэнергии, необходимой для майнинга криптовалют и поддержания работы блокчейн-сетей. Поэтому переход на использование

возобновляемых источников энергии является одним из ключевых путей снижения углеродного следа.

Использование солнечной, ветровой и гидроэнергетики для обеспечения энергопотребности блокчейн-систем может значительно снизить выбросы парниковых газов и, следовательно, уменьшить углеродный след. Многие майнинговые компании и блокчейн-проекты уже начали переходить на возобновляемые источники энергии, строя солнечные электростанции и ветропарки вблизи своих майнинговых ферм. [2, с.93]

Помимо использования возобновляемых источников энергии, важным шагом в минимизации углеродного следа является применение офсетных программ, направленных на компенсацию выбросов углерода. Одним из наиболее распространенных подходов является лесовосстановление и посадка новых деревьев, которые поглощают углекислый газ из атмосферы. Некоторые блокчейн-проекты уже сотрудничают с экологическими организациями и инвестируют средства в программы лесовосстановления и защиты лесов.

Другие офсетные программы включают в себя захват и хранение углерода, инвестиции в технологии улавливания и утилизации углекислого газа, а также поддержку проектов по развитию экологически чистых технологий и альтернативной энергетики.

Государственное регулирование и стимулирование "зеленых" блокчейн-проектов также может сыграть важную роль в минимизации углеродного следа. Введение налоговых льгот и субсидий для компаний, использующих возобновляемые источники энергии или применяющих офсетные программы, может стимулировать переход к более экологичным практикам.

Кроме того, важно повышать осведомленность участников блокчейн-сообщества о проблеме углеродного следа и ее последствиях для окружающей среды. Проведение образовательных кампаний, организация конференций и семинаров, посвященных этой теме, может способствовать изменению отношения и поведения участников индустрии.

Минимизация углеродного следа блокчейн-систем требует комплексного подхода, включающего в себя использование возобновляемых источников энергии, применение офсетных программ, государственное регулирование и повышение осведомленности. Только объединив усилия всех заинтересованных сторон, мы сможем создать действительно устойчивые и экологически чистые блокчейн-технологии, которые не наносят вреда окружающей среде.

Заключение

В заключение следует отметить, что проблема высокого энергопотребления и значительного углеродного следа блокчейн-систем требует незамедлительного решения для обеспечения их устойчивого развития и минимизации негативного воздействия на окружающую среду.

В рамках настоящего исследования были рассмотрены различные пути минимизации энергопотребления и углеродного следа блокчейн-систем. Одним из наиболее перспективных подходов является переход на альтернативные консенсусные механизмы, такие как "Доказательство доли владения" (PoS), которые не требуют значительных вычислительных мощностей и, следовательно, снижают энергозатраты. Кроме того, оптимизация аппаратного обеспечения, используемого для майнинга и поддержки работы блокчейн-сетей, также может существенно сократить энергопотребление.

Для минимизации углеродного следа блокчейн-систем крайне важен переход на использование возобновляемых источников энергии, таких как солнечная, ветровая и гидроэнергетика. Применение офсетных программ, направленных на компенсацию выбросов углерода, таких как лесовосстановление, захват и хранение углерода, а также инвестиции в экологически чистые технологии, также является эффективным способом снижения углеродного следа.

Следует отметить, что для достижения устойчивого развития блокчейн-систем необходим комплексный подход, сочетающий в себе технологические инновации, государственное регулирование и стимулирование "зеленых" блокчейн-проектов, а также повышение осведомленности участников индустрии о проблеме энергопотребления и углеродного следа.

Дальнейшие исследования и разработки в области устойчивого блокчейна должны быть направлены на поиск новых энергоэффективных консенсусных механизмов, оптимизацию протоколов и алгоритмов, а также внедрение передовых технологий, таких как распределенные вычисления, параллельная обработка данных и эффективное охлаждение майнинговых ферм.

В целом, обеспечение экологической устойчивости блокчейн-систем является неотъемлемой частью их успешного развития и широкого внедрения в различных сферах. Только объединив усилия всех заинтересованных сторон, включая разработчиков, майнеров, регуляторов и экологические организации, мы сможем создать действительно устойчивые и экологически чистые блокчейн-технологии, которые будут способствовать достижению целей устойчивого развития и сохранению окружающей среды для будущих поколений.

Список литературы

1. Кушнир Д. В., Скробов Д. В. Обеспечение безопасности в технологии блокчейн //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 642-648.
2. Красов А. В. и др. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии //ОФТАЛЬМОХИРУРГИЯ. – 2022. – №. 4s. – С. 92-101.
3. Макарова А. К., Поляничева А. В., Саматова К. А. Анализ уязвимостей оборудования передачи голосового трафика //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 665-669.
4. Алехин Р. В. и др. Исследование критической уязвимости сервиса аутентификации и последствий для медицинских учреждений, относящихся к субъектам критической информационной инфраструктуры //Офтальмохирургия. – 2022. – №. 4s. – С. 115-122.
5. Шариков П. И., Красов А. В. Исследование возможности вложения цифрового водяного знака в байт-код путем замены уязвимого байт-кода Java класса //Информационная безопасность регионов России (ИБРР-2017). – 2017. – С. 499-500.

References

1. Kushnir D. V., Skrobov D. V. Ensuring security in blockchain technology //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 642-648.

2. Krasov A.V. et al. Current threats to information security in the field of healthcare and ophthalmology //OPHTHALMOSURGERY. - 2022. – No. 4s. – pp. 92-101.
 3. Makarova A. K., Polyanicheva A.V., Samatova K. A. Vulnerability analysis of voice traffic transmission equipment //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 665-669.
 4. Alekhine R. V. et al. Investigation of the critical vulnerability of the authentication service and the consequences for medical institutions related to the subjects of critical information infrastructure //Ophthalmosurgery. - 2022. – No. 4s. – pp. 115-122.
 5. Sharikov P. I., Krasov A.V. Investigation of the possibility of embedding a digital watermark in bytecode by replacing the vulnerable Java class bytecode //Information security of the regions of Russia (IBRD-2017). – 2017. – pp. 499-500.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 621.311

АКТУАЛЬНОСТЬ РАЗРАБОТКИ МЕТОДОВ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ НАДЕЖНОСТИ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМ

¹**Мартынов А.П., Головинов В.В., Гладкина Е.М., Малышев А.М., Гаркушин Д.М.**
ФГБОУ ВО "ДОНСКОЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ", АЗОВО-ЧЕРНОМОРСКИЙ ИНЖЕНЕРНЫЙ ИНСТИТУТ - ФИЛИАЛ В Г. ЗЕРНОГРАДЕ, Зерноград, Россия (347740, Ростовская область, Зерноградский район, город Зерноград, ул. им Ленина, д. 21), e-mail: ¹alpmart@mail.ru

Оценка уровня надежности электроэнергетических систем является весьма сложной и нетривиальной задачей. В настоящее время существуют различные подходы и методы количественной оценки надежности. Но сохраняется актуальность разработки новых упрощенных методов ее оценки, что подтверждается основными разделами энергетической стратегии России на период до 2030 г. и концепцией обеспечения надежности в электроэнергетике.

Ключевые слова: Теория надежности, структурная надежность, функциональная надежность, показатели надежности, методы оценки надежности.

THE RELEVANCE OF THE DEVELOPMENT OF QUANTITATIVE METHODS RELIABILITY ASSESSMENTS OF ELECTRIC POWER SYSTEMS

¹**Martynov A.P., Golovinov V.V., Gladkina E.M., Malyshev A.M., Garkushin D.M.**
"DON STATE AGRARIAN UNIVERSITY", AZOV-BLACK SEA ENGINEERING INSTITUTE - BRANCH IN ZERNOGRAD, Zernograd, Russia (347740, Rostov region, Zernogradsky district, Zernograd city, Lenin street, 21), e-mail: ¹alpmart@mail.ru

Assessing the reliability of electric power systems is a very difficult and non-trivial task. Currently, there are various approaches and methods for quantifying reliability. However, the development of new simplified methods of its assessment remains relevant, which is confirmed by the main sections of Russia's energy strategy for the period up to 2030 and the concept of ensuring reliability in the electric power industry.

Keywords: Reliability theory, structural reliability, functional reliability, reliability indicators, reliability assessment methods.

Надежность – это свойство объекта выполнять заданные функции в заданном объеме при определенных условиях функционирования [1]. Если мы рассматриваем надежность электроэнергетических систем, то здесь понятие надежности можно трактовать как способность этих систем обеспечивать электроэнергией требуемого качества потребителей в любой момент времени, т.е. не допуская перерывов электроснабжения, а также сведение к минимуму аварийных ситуаций, которые могут повлечь за собой опасность для жизни и здоровья людей или нанести вред окружающей среде. Объектом в электроэнергетической системе может быть отдельный ее элемент (изделие), комплект оборудования (например трансформаторная подстанция), какая-то часть системы или система в целом [1, 2].

В общей теории надежности выделяют понятия структурной и функциональной надежности. Структурная надежность подразумевает исследование структуры электроэнергетической системы, деление ее на отдельные элементы, надежность которых определяется отдельно, с последующей оценкой влияния каждого элемента на надежность всей системы. Функциональная надежность определяет насколько система или отдельная ее часть правильно и в заданном объеме выполняет все требуемые функции [3 - 6].

Функциональная надежность подразделяется на балансовую и режимную надежность. Балансовая надежность рассматривает систему с точки зрения достаточности ресурсов (генерирующих мощностей), нехватка которых может повлечь ухудшение качества электрической энергии, отключение части потребителей электрической энергии или опрокидывание генераторов на электростанциях, что может перейти в лавинообразный процесс и остановить работу всей системы. Чтобы избежать подобных ситуаций и обеспечить высокий уровень балансовой надежности необходимо создавать новые генерирующие мощности и обеспечивать резервирование системы, а также обеспечивать своевременное техническое обслуживание, текущие и капитальные ремонты электроустановок [7]. Режимная надежность обусловлена режимами работы системы и может зависеть от балансовой надежности. Различные режимы работы электроэнергетических систем могут приводить к аварийным ситуациям, отключению участков системы, части потребителей электроэнергии, снижению ее показателей качества, установленных ГОСТ Р 32144-2013 [5].

На современном этапе развития электроэнергетических систем задачи оценки их надежности весьма актуальны для обеспечения бесперебойного электроснабжения производственных и коммунально-бытовых потребителей, ведь для этого необходимо правильно оценивать уровни надежности.

Исследованию проблемы надежности и ее количественной оценке посвящены работы многих зарубежных и российских ученых: В.Я. Хорольский, М.А. Таранов, А.М. Исупова, Б. Дилон, Ф. Прошан, В.В. Зорин, Н.А. Казак, А.А. Гришкевич, В.В. Тисленко, Р. Алан, Б.В. Гнеденко, и многих других.

В электроэнергетических системах наиболее существенным является оценка их функциональной надежности, т.е. с точки зрения выполнения требуемых функций по обеспечению бесперебойного и качественного электроснабжения, так как различные внешние и внутренние факторы могут привести к нарушению этих функций или их отказу. А это в свою очередь может привести к весьма негативным последствиям, таким как выход оборудования из строя, опасности для людей и окружающей среды, значительным экономическим ущербам. В связи с этим оценку и учет надежности электроэнергетических систем требуется производить при их проектировании, строительстве и эксплуатации [8].

В настоящее время разработаны и применяются различные методы количественной оценки уровней надежности электроэнергетических систем. Какие-то из них можно назвать классическими, другие же только появились, третьи продолжают свое развитие.

Сегодня для определения уровня надежности электроэнергетических систем существуют только достаточно хорошие математические методы и модели, но включающие в себя ряд допущений. При оценке надежности этих систем необходимо учитывать их особенности, а не только теоретические модели. Надо отметить, что основной трудностью определения надежности здесь является невозможность проведения натурных

экспериментальных исследований. Из всего выше сказанного можно сделать вывод, что создание новых и совершенствование существующих методов оценки надежности электроэнергетических систем является актуальной задачей [2].

Теория надежности как наука возникла в пятидесятых годах двадцатого столетия. Основная ее задача – это разработать и изучить методы, которые обеспечат эффективность работы разных элементов (изделий, устройств, систем) в процессе их эксплуатации [9].

В настоящее время вопросам надежности посвящено большое количество работ, они вызывают немалый интерес во всем мире. Однако, несмотря на большое количество работ в данной области, в настоящее время актуальность этой темы не снижается. Связано это с тем, что подключаются новые потребители, создаются сложные системы электроснабжения.

На практике специалист в области электроэнергетики постоянно принимает разные решения: выбирает оптимальные варианты системы; подбирает режимы работы систем в условиях, которые отличаются от нормальных; производит ремонты, замены и оперативные переключения. На выбор данных решений оказывает влияние большое число разных факторов. Для некоторых из них можно произвести количественный анализ и расчет, вследствие чего можно сузить область возможных вариантов принятия решений; другие не поддаются количественному описанию. Это приводит к неопределенности при выборе решений. Несмотря на это, специалистам необходимо их принимать, соединяя практические знания с количественными расчетами и инженерной интуицией, а также проводить качественный анализ проводимых задач. При этом возникает риск выбора ошибочных и неоптимальных решений. Соответственно, чем больше разнообразных факторов, которые нельзя просчитать, тем больше вероятность того, что можно принять неправильные решения и получить их отрицательные последствия. Надежность среди всех разнообразных факторов занимает особое место. Поэтому появилась потребность в количественной оценке аварийных ситуаций и их последствий.

В настоящее время основной тенденцией в энергетике является создание больших энергообъединений, у которых имеется сложная структура, с одной стороны – это приводит к увеличению доли системных аварий, в результате которых единичный отказ может повлечь за собой каскадное развитие аварии и охватить значительную часть энергообъединения, с другой стороны – объединение позволяет получить значимые экономические преимущества. Поэтому необходимо проанализировать все затраты, связанные с повышением уровня надежности. Чтобы повысить надежность довольно часто принимают решения о резервировании или дублировании достаточно большого количества потребителей, что приводит к большим капитальным затратам, следовательно, это решение должно быть надлежащим образом обосновано. Рассчитав ущерб, нанесенный потребителям из-за перерыва электроснабжения, убытки из-за аварийного ремонта, и расходы, направленные на повышение надежности, можно оптимизировать уровень надёжности электроэнергетического оборудования и систем в целом [8].

Существенный рост потребления электрической энергии связан с качественным изменением потребителей. Последнее определено введением новых технологий и углублением электрификации разных производств, что приводит к увеличению зависимости нормального функционирования потребителей от надежности снабжения электрической энергией [10]. Это может привести к значительному материальному ущербу из-за нарушения

энергоснабжения, а в некоторых случаях привести к масштабам национального бедствия, доказательством чему служат ряд аварий в разных странах мира, например, США – Канада в августе 2003 г.; Швеция – Дания – Италия в сентябре 2003 г.; в мае 2005 г. – авария в Москве; в июне 2005 г. – авария в Благовещенске, Амурской области. Таким образом, ряд непредвиденных и случайных причин может привести к потере электроэнергии, либо снизить ее качество у части или даже у всех потребителей системы электроснабжения. Нарушение электроснабжения из-за системных аварий, как уже говорилось выше, может привести к серьезному ущербу, который может быть также связан с угрозой для жизни людей. Например, Нью-Йоркская авария в США привела к тому, что более чем на десять часов на территории с населением приблизительно 30 миллионов человек была практически приостановлена жизнедеятельность. Ущерб от данной аварии, по предварительным расчетам, превышал сто миллионов долларов [8].

В некоторых электроэнергетических системах число аварий может достигать в течение года нескольких десятков, а годовой недоотпуск электроэнергии из-за последствий аварий – нескольких миллиардов киловатт-часов. Суммарная общая мощность генераторов, которые одновременно простаивают в аварийном ремонте, составляет десятки миллионов киловатт. Всевозможные последствия от ненадежности элементов системы становятся существенными, в связи с этим необходимо постоянно совершенствовать методы, позволяющие прогнозировать развитие, проектирование, строительство, монтаж и эксплуатацию электроэнергетических систем, с помощью которых можно было бы наиболее полно учитывать надежность и экономично тратить средства, которые выделяются на её обеспечение [8]. Таким образом, на сегодняшний день оценка показателей надежности систем электроснабжения становится одной из важных задач развития в области энергетики.

Создание новых и расширение без того сложных электроэнергетических систем требует таких методов оценки надежности, которые бы позволили при проектировании учитывать опыт эксплуатации, провести анализ различных вариантов обеспечения надежности, а также спрогнозировать надежность новых энергосистем.

Существующие на сегодняшний момент различные методы количественной оценки показателей надежности электроэнергетических систем весьма громоздки, поэтому вопросы выбора и применения упрощенных методов расчета надежности, позволяющие более эффективно, и с меньшими вычислительными затратами решать задачи оценки надежности, приобретают большое значение.

Таким образом, количественная оценка уровня надежности различных схем электроснабжения является в современных условиях актуальной темой, что подтверждается основными разделами энергетической стратегии России на период до 2030 г. и концепции обеспечения надежности в электроэнергетике [7,11].

Список литературы

1. ГОСТ 27.002–2015. Надежность в технике. Термины и определения. М.: Стандартинформ, 2016. 24 с.
2. Анищенко В.А. Надежность систем электроснабжения: учеб. пособие. Мн.: УП «Технопринт», 2002. 160 с.

3. Васильев И.Е. Надежность электроснабжения: учебное пособие для вузов. М. Издательский дом МЭИ, 2014. 174 с.
4. Куликов А. Л., Осокин В. Л., Папков Б. В., Шилова Т. В. Расширение понятия «надежность» в современной электроэнергетике // *Вестник НГИЭИ.* 2018. № 3 (82). С. 88-98.
5. Манов Н.А., Хохлов М.В., Чукреев Ю.Я. Методы и модели исследования надежности электроэнергетических систем / под ред. Н.А. Манова: монография. Сыктывкар.: изд-во Коми научного центра УрО РАН, 2010. 292 с.
6. Чукреев Ю.Я. Модели обеспечения надежности электроэнергетических систем. Сыктывкар, 1995. 173 с.
7. Энергетическая стратегия России на период до 2030 года, утв. распоряжением Правительства Российской Федерации от 13.11.2009 г. №1715-р [Электронный ресурс]. URL: <https://minenergo.gov.ru/node/1026/> (дата обращения 28.03.2019).
8. Папков Б. В., Куликов А. Л. Теория систем и системный анализ для электроэнергетиков. М. : Изд-во Юрайт, 2016. 470 с.
9. Воропай Н.И. Теория систем для электроэнергетиков: учебное пособие. Новосибирск: Издательская фирма РАН, 2000. 273 с.
10. Папков Б.В., Пашали Д.Ю. Надежность и эффективность электроснабжения: учебное пособие. Уфа: УГАТУ, 2005. 380 с.
11. Воропай Н.И. Концепция обеспечения надежности в электроэнергетике// Воропай Н. И., Ковалёв Г. Ф., Кучеров Ю. Н. и др. – М.: ООО ИД «ЭНЕРГИЯ», 2013. 212 с.

References

1. GOST 27.002–2015. Reliability in technology. Terms and definitions. Moscow: Standartinform, 2016. p. 24
2. Anishchenko V.A. Reliability of power supply systems: textbook. manual. Mn.: UP "Technoprint", 2002. p.160
3. Vasiliev I.E. Reliability of power supply: a textbook for universities. M. Publishing House of the Moscow Institute of Economics, 2014. p.174 .
4. Kulikov A. L., Osokin V. L., Papkov B. V., Shilova T. V. Expansion of the concept of "reliability" in modern electric power industry. Vestnik NGIEI. 2018. No. 3 (82). pp. 88-98.
5. Manov N.A., Khokhlov M.V., Chukreev Yu.Ya. Methods and models of reliability research of electric power systems / edited by N.A. Manov: monograph. Syktyvkar.: publishing house of the Komi Scientific Center of the Ural Branch of the Russian Academy of Sciences, 2010. p. 292 .
6. Chukreev Yu.Ya. Models for ensuring the reliability of electric power systems. Syktyvkar, 1995. p.173 .
7. The Energy Strategy of Russia for the period up to 2030, approved by the decree of the Government of the Russian Federation dated 11/13/2009 No. 1715-r [Electronic resource]. URL: <https://minenergo.gov.ru/node/1026/> / (accessed 03/28/2019).
8. Papkov B. V., Kulikov A. L. Theory of systems and system analysis for electroeneretics. Moscow : Yurayt Publishing House, 2016. p. 470.

9. Voropai N.I. Theory of systems for electric power engineers: a textbook. Novosibirsk: Publishing Company of the Russian Academy of Sciences, 2000. p.273.
 10. Papkov B.V., Pashali D.Yu. Reliability and efficiency of power supply: a textbook. Ufa: UGATU, 2005. p.380.
 11. Voropai N.I. The concept of ensuring reliability in the electric power industry// Voro-pai N. I., Kovalev G. F., Kuchеров Yu. N. et al. – М.: ООО ID ENERGIA, 2013. p. 212.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 539.3

ТЕРМОНАПРЯЖЕННОЕ СОСТОЯНИЕ ТВЭЛА С ПЕРЕМЕННЫМ КОЭФФИЦИЕНТОМ ЛИНЕЙНОГО РАСШИРЕНИЯ

Канарейкин А.И.

ФГБОУ ВО «РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГЕОЛОГОРАЗВЕДОЧНЫЙ
УНИВЕРСИТЕТ ИМЕНИ СЕРГО ОРДЖОНИКИДЗЕ (МГРИ)», Москва, Россия, (117485, г.
Москва, ул. Миклухо-Маклая, 23), e-mail: kanareykins@mail.ru

Работа посвящена повышению надёжности конструкции твэлов, которая определяется уровнем и характером распределения внутренних напряжений. Основной целью статьи является моделирование термонапряжений твэла с объемным тепловыделением. При этом учитывается координатная зависимость коэффициента линейного расширения. Решение получено с применением методов дифференцирования. Полученный результат может полезен для определения термонапряжённого состояния твэлов. А также открывает возможность снижения температурных напряжений в твэле с координатной зависимостью коэффициента линейного расширения.

Ключевые слова: Температурное поле, твэл, цилиндр, коэффициент линейного расширения, функция Эри, граница области, тензор.

THERMALLY STRESSED STATE OF A FUEL ELEMENT WITH A VARIABLE COEFFICIENT OF LINEAR EXPANSION

Kanareykin A.I.

SERGO ORDZHONIKIDZE RUSSIAN STATE UNIVERSITY FOR GEOLOGICAL PROSPECTING,
Moscow, Russia, (117485, Moscow, st. Miklukho-Maklaya 23), e-mail: kanareykins@mail.ru

The work is devoted to improving the reliability of the fuel element design, which is determined by the level and nature of the internal stress distribution. The main purpose of the article is to simulate thermal stresses of a fuel element with volumetric heat release. The coordinate dependence of the linear expansion coefficient is taken into account. The solution was obtained using differentiation methods. The result obtained can be useful for determining the thermally stressed state of fuel rods. It also opens up the possibility of reducing temperature stresses in fuel rods with a coordinate dependence of the linear expansion coefficient.

Keywords: Temperature field, fuel element, cylinder, coefficient of linear expansion, Erie function, boundary of the region, tensor.

Переменные свойства материала при наличии неоднородного температурного поля вносят дополнительный вклад в изменение термонапряженного состояния. Поэтому возникает необходимость исследования влияния переменных свойств материала на возможность управления прочностными свойствами материала, для обеспечения безопасности эксплуатации изделий новой техники. Их определение в общем случае сводится к решению уравнений математической физики и весьма часто представляет значительные математические трудности [1-6].

При проектировании твэлов используют материалы с переменными свойствами. Их использование даёт возможность улучшить прочность характеристики и в конечном счёте управлять уровнем и характером распределения напряжений. Среди последних преобладающую роль занимают температурные напряжения. Их появление обусловлено неоднородной температурной деформацией [7-10]. В материалах ядерной техники подобная деформация связана с объёмным тепловыделением за счёт превращения кинетической энергии атомов деления тяжёлых элементов (урана, плутония, тория) в тепловую. При определении термонапряжений объёмное тепловыделение считается постоянной величиной. Её зависимость от различных факторов носит параметрический характер и не влияет на решение задач теплопроводности. Однако в некоторых случаях тепловыделение имеет координатную зависимость [11-17].

Актуальность работы обусловлена тем, что в работе учитывается координатная зависимость коэффициентом линейного расширения. Что приводит к изменению термонапряжённого состояния твэла. При этом прочность и надёжность ядерных реакторов определяется уровнем и характером распределения внутренних напряжений.

Целью работы является моделирование термонапряжений твэла с переменным коэффициентом линейного расширения.

Для этого рассмотрим сплошной длинный цилиндр с объёмным тепловыделением и переменным по радиусу коэффициентом линейного расширения. Для плоской задачи термоупругости компоненты тензора термонапряжений определяют через функцию напряжений (функция Эри), которая находится из решения задачи

$$\Delta \Delta F = -\frac{E}{1-\nu} \Delta(\alpha T) \quad (1)$$

где F - функция напряжений Эри,

E - модуль Юнга,

T - температурное поле,

ν - коэффициент Пуассона,

α - переменный коэффициент линейного расширения, который меняется по закону

$$\alpha = \alpha_0 \left(1 + \left(\frac{r}{R} \right)^2 \right) \quad (2)$$

где: α_0 – коэффициент линейного расширения при $r=0$, R - внешний радиус цилиндра. Функция напряжений F подчиняется уравнению (полярные координаты)

$$\frac{\partial^4 F}{\partial r^4} + \frac{2}{r} \frac{\partial^3 F}{\partial r^3} - \frac{1}{r^2} \frac{\partial^2 F}{\partial r^2} + \frac{1}{r^3} \frac{\partial F}{\partial r} = -\frac{E}{1-\nu} \Delta(\alpha T) \quad (3)$$

При решении уравнения (3) будем учитывать граничные условия на внешнем контуре

$$F = \frac{\partial F}{\partial n} = 0 \quad (4)$$

С учётом (2) выражение (3) примет вид

$$\frac{\partial^4 F}{\partial r^4} + \frac{2}{r} \frac{\partial^3 F}{\partial r^3} - \frac{1}{r^2} \frac{\partial^2 F}{\partial r^2} + \frac{1}{r^3} \frac{\partial F}{\partial r} = -\frac{4\alpha E q_v}{\lambda(1-\nu)} \frac{r^2}{R^2} \quad (5)$$

Решение уравнения (5) ищем в виде чётных степеней

$$F = C_1 + C_2 r^2 + C_3 r^4 + C_4 r^6 \quad (5)$$

Искомая функция напряжений F находится из решения системы уравнений

$$\begin{cases} C_1 + C_2 R^2 + C_3 R^4 + C_4 R^6 = 0 \\ 2C_2 R + 4C_3 R^3 + 6C_4 R^5 = 0 \\ 64C_3 + 576C_4 R^2 = -\frac{4\alpha E q_v}{\lambda(1-\nu)} \frac{r^2}{R^2} \end{cases} \quad (6)$$

Решение самой системы (6) даёт значения констант

$$\begin{cases} C_1 = -\frac{\alpha E q_v}{72\lambda(1-\nu)} R^4 \\ C_2 = \frac{11\alpha E q_v}{48\lambda(1-\nu)} R^2 \\ C_3 = 0 \\ C_4 = -\frac{\alpha E q_v}{144\lambda(1-\nu)R^2} \end{cases} \quad (7)$$

Окончательно функция напряжений принимает вид

$$F = \frac{\alpha E q_v R^4}{144\lambda(1-\nu)} \left(2 - 3 \frac{r^2}{R^2} + \frac{r^6}{R^6} \right) \quad (8)$$

Температурные напряжения при известной функции F определяются весьма просто

$$\sigma_{rr} = \frac{1}{r} \frac{\partial F}{\partial r} = \frac{\alpha E q_v R^2}{24\lambda(1-\nu)} \left(\frac{r^4}{R^4} - 1 \right) \quad (9)$$

$$\sigma_{\theta\theta} = \frac{\partial^2 F}{\partial r^2} = \frac{\alpha E q_v R^2}{24\lambda(1-\nu)} \left(5 \frac{r^4}{R^4} - 1 \right) \quad (10)$$

$$\sigma_{zz} = \sigma_{rr} + \sigma_{\theta\theta} = \frac{\alpha E q_v R^2}{12\lambda(1-\nu)} \left(3 \frac{r^4}{R^4} - 1 \right) \quad (11)$$

Графические зависимости компонент тензора термонапряжений приведены на Рисунке 1 в безразмерном виде.

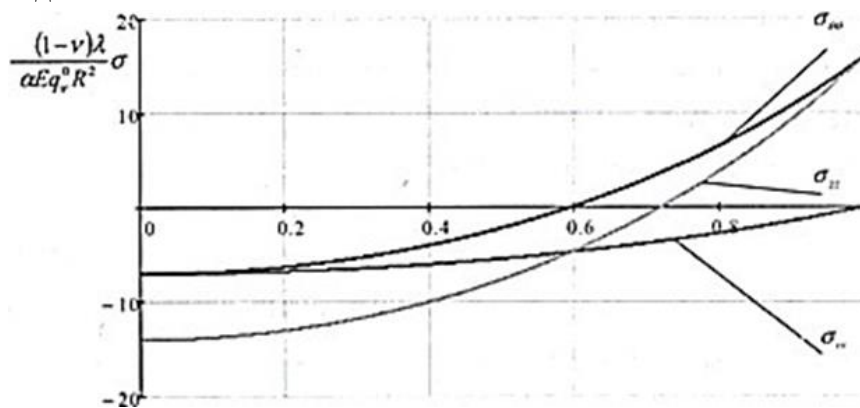


Рисунок 1 - Компоненты тензора термонапряжений в безразмерном виде.

Таким образом, в статье была решена задача об определении напряжённого состояния твэла с коэффициентом линейного расширения. Как следует из полученных выражений, Температурные напряжения подчиняются параболическому закону. Уровень и характер распределения термонапряжений зависят от координатной зависимости коэффициента линейного расширения. Таким образом, показана принципиальная возможность управления

термонапряженным состоянием тепловыделяющего цилиндра путем изменения коэффициента линейного расширения.

Список литературы

1. Доллежалъ, Н. А. Канальный ядерный энергетический реактор / Н. А. Доллежалъ, И. Я. Емельянов. — М.: Атомиздат, 1980. — 208 с.
2. Kanareykin, A. I. Simulation of a fuel element made of plutonium dioxide // IOP Conference Series: Earth and Environmental Science. 2022. Т. 1045. № 1. С. 012070.
3. Kanareykin, A. I. Mathematical modeling of the fuel element of a nuclear reactor taking into account the temperature dependence of the thermal conductivity of the fuel element made of uranium oxide // IOP Conference Series: Earth and Environmental Science. 4. Сер. "IV International Scientific and Practical Conference "Actual Problems of the Energy Complex: Physical Processes, Mining, Production, Transmission, Processing and Environmental Protection"", 2022. С. 012012.
4. Kolpakov A., Tagantsev A. K., Berlyand L., Kanareykin A. Nonlinear dielectric response of periodic composite materials // Journal of Electroceramics. 2007. Vol. 18. № 1-2. Pp. 129-137.
5. Крамеров, А. Я. Инженерные расчеты ядерных реакторов / А. Я. Крамеров, Я. В. Шевелев. — 2-е изд., перераб. и доп. — М.: Энергоатомиздат, 1984. — 736 с.
6. Newman C., Hansen G., Gaston D. Three-dimensional coupled simulation of thermomechanics, heat, and oxygen diffusion in UO₂ nuclear fuel rods // Journal of Nuclear Materials. – 2009. – Vol. 392. – № 1. – p. 6-15.
7. Симонова О.С., Логинов В.С. Одномерная нестационарная модель тепловыделяющей системы из произвольного числа твэлов и неактивных элементов // Фундаментальные исследования. 2014. № 5–3. С. 503–506.
8. Дунайцев А.А., Солонин В.И. Процессы массообмена в пучках оребранных стержней // Проблемы машиностроения и автоматизации. 2016. № 1. С. 125–134.
9. Ramirez J. C., Stan M., Cristea P. Simulations of heat and oxygendiffusion in UO₂ nuclear fuel rods // Journal of nuclear materials. – 2006. – Т. 359, № 3. – С. 174-184.
10. Mihaila B. et al. Simulations of coupled heat transport, oxygen diffusion, and thermal expansion in UO₂ nuclear fuel elements // Journal of Nuclear Materials. – 2009. – Vol. 394, № 2. – p. 182-189.
11. Семенович, О.В. Моделирование теплофизических процессов в тепловыделяющих сборках и активных зонах водоохлаждаемых ядерных реакторов / О.В. Семенович // Тезисы докладов и сообщений. XIV Минский международный форум по тепло и массообмену. 23–26 мая 2016 г.: в 3-х т. – Минск: ИТМО им. А.В. Лыкова НАН Беларуси, 2016. – Т. 3. – С. 410–404.
12. Kang C. H. et al. 3D finite element analysis of a nuclear fuel rod with gap elements between the pellet and the cladding // Journal of Nuclear Science and Technology. – 2015. – P. 1-8.
13. Власов, Н.М. Тепловыделяющие элементы ядерных ракетных двигателей / Н.М. Власов, И.И. Федик. - М.: ЦНИИ атоминформ, 2001. - 208с.
14. Петухов, Б.С., Генин, А.Г., Ковалев, С.А. Теплообмен в ядерных энергетических установках. - М.: Атомиздат, 1974. - 408 с.

15. Иванов, В. В. Распределение температуры в теле эллиптического сечения с внутренним источником тепла. Известия Томского политехнического института: журнал / – Томск: Томский политехнический университет, 1964. – Т. 125. – 67 с.
16. Канарейкин, А. И. Распределение температурного поля в твэле с эллиптическим поперечным сечением // Научные труды Калужского государственного университета им. К.Э. Циолковского, серия: естественные науки. - 2016. – С. 230 – 231.
17. Kanareykin A. 2023. Simplified dynamic model of a nuclear reactor. E3S Web of Conferences 402: 05025.
18. Канарейкин, А. И. Определение температурного поля твэла с переменным объемным тепловыделением при граничном условии первого рода // Международный журнал информационных технологий и энергоэффективности, 2024. Т. 9. - № 8 (46). - С. 137-142.

References

1. Dollezhal N. A., Emelyanov I. Ya. Moscow, Atomizdat Publ., 1980. 208 p.
2. Kanareykin, A. I. Simulation of a fuel element made of plutonium dioxide // IOP Conference Series: Earth and Environmental Science. 2022. T. 1045. № 1. C. 012070.
3. Kanareykin, A. I. Mathematical modeling of the fuel element of a nuclear reactor taking into account the temperature dependence of the thermal conductivity of the fuel element made of uranium oxide // IOP Conference Series: Earth and Environmental Science. 4. Сер. "IV International Scientific and Practical Conference "Actual Problems of the Energy Complex: Physical Processes, Mining, Production, Transmission, Processing and Environmental Protection"", 2022. C. 012012.
4. Kolpakov A., Tagantsev A. K., Berlyand L., Kanareykin A. Nonlinear dielectric response of periodic composite materials // Journal of Electroceramics. 2007. Vol. 18. № 1-2. pp. 129-137.
5. Kramerov, A. Ya. Engineering calculations of nuclear reactors / A. Ya. Kramerov, Ya. V. Shevelev. — 2nd ed., reprint. and additional — M.: Energoatomizdat, 1984. — p.736
6. Newman C., Hansen G., Gaston D. Three-dimensional coupled simulation of thermomechanics, heat, and oxygen diffusion in UO₂ nuclear fuel rods // Journal of Nuclear Materials. – 2009. – Vol. 392. – № 1. – pp.. 6-15.
7. Simonova O.S., Loginov V.S. One-dimensional nonstationary model of a heat-generating system from an arbitrary number of fuel rods and inactive elements // Fundamental research. 2014. No. 5-3. pp. 503-506.
8. Dunaytsev A.A., Solonin V.I. Mass transfer processes in bundles of finned rods // Problems of mechanical engineering and automation. 2016. No. 1. pp. 125-134.9.
9. Ramirez J. C., Stan M., Cristea P. Simulations of heat and oxygendiffusion in UO₂ nuclear fuel rods // Journal of nuclear materials. – 2006. – Т. 359, № 3. – pp. 174-184.
10. Mihaila B. et al. Simulations of coupled heat transport, oxygen diffusion, and thermal expansion in UO₂ nuclear fuel elements // Journal of Nuclear Materials. – 2009. – Vol. 394, № 2. – pp. 182-189.
11. Semenov, Oh.V. Modeling of thermophysical processes in thermovelevating aggregates and active wawrabh zonach water-cooled wawrabh yadern wawrabh reactor / O.V. Semyonovich / theses. 23-26 May 2016: in 3-H. - Minsk: ITMO im. A.V. Lirmkova NAN Belarussi, 2016. - Т. 3. - pp. 410–404.

12. Kang C. H. et al. 3D finite element analysis of a nuclear fuel rod with gap elements between the pellet and the cladding // Journal of Nuclear Science and Technology. – 2015. – P. 1-8.
 13. Vlasov, N.M. Fuel elements of nuclear rocket engines / N.M. Vlasov, I.I. Fedik. - - М.: Tsniiatominform, 2001. - p.208.
 14. Petukhov, B.S., Genin, A.G., Kovalev, S.A. Heat transfer in nuclear power plants. - М.: Atomizdat, 1974. – p.408.
 15. Ivanov, V. V. Temperature distribution in an elliptical body with an internal heat source. Proceedings of the Tomsk Polytechnic Institute: journal / – Tomsk: Tomsk Polytechnic University, 1964. – Vol. 125. – p.67.
 16. Kanarekin, A. I. Distribution of the temperature field in a fuel element with an elliptical cross section // Scientific works of the Kaluga State University named after K.E. Tsiolkovsky, series: natural sciences. - 2016. – pp. 230-231.
 17. Kanareykin A. 2023. Simplified dynamic model of a nuclear reactor. E3S Web of Conferences 402: 05025.
 18. Kanarekin, A. I. Determination of the temperature field of a fuel element with variable volumetric heat release under a boundary condition of the first kind // International Journal of Information Technologies and Energy Efficiency, 2024. Vol. 9. - № 8 (46). - pp. 137-142.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 624.21

ОБСЛЕДОВАНИЕ И ОЦЕНКА НЕСУЩЕЙ СПОСОБНОСТИ ДЕМОНТИРУЕМЫХ СТАЛЕЖЕЛЕЗОБЕТОННЫХ ПРОЛЕТНЫХ СТРОЕНИЙ

¹Зиннуров Т.А., ²Ионов И.А.

¹ФГБОУ ВО «КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ», Казань, Россия, (420043, Республика Татарстан, город Казань, Зеленая ул., д.1), e-mail: leongar@mail.ru

²ООО «ГРАДПРАКТИКА», Москва, Россия (115280, город Москва, ул. Ленинская Слобода, д. 26, эт/ном/ком 4/XXXII-73/1), e-mail: igor.pwt@mail.ru

Статья посвящена вопросам предотвращения аварий при демонтаже стальных и железобетонных пролетных конструкций с дефектами. В ней содержится описание и анализ различных методов демонтажа, а также указаны ключевые элементы отчета об обследовании и необходимые расчеты, основываясь на выбранном способе демонтажа. Рассматриваются специфические аспекты расчета несущей способности и грузоподъемности конструкций с дефектами. В статье описан пример опасного дефекта – провисания – и методы его выявления.

Ключевые слова: Сталежелезобетонные пролетные строения, демонтаж, обследование, оценка несущей способности, дефекты, провисание.

THE SURVEY AND THE CALCULATION OF THE CARRYING CAPACITY OF DISMANTLED COMPOSITE BRIDGE SPANS

¹Zinnurov T.A., ²Ionov I.A.

¹KAZAN STATE UNIVERSITY OF ARCHITECTURE AND CIVIL ENGINEERING, Kazan, Russia, (420043, Republic of Tatarstan, Kazan, Zelenaya str., 1), e-mail: leongar@mail.ru

²GRADPRAKTIKA LLC, Moscow, Russia (115280, Moscow, Leninskaya Sloboda str., 26, fl/pom/kom 4/XXXII-73/1), e-mail: igor.pwt@mail.ru

The article is devoted to the issues of accident prevention during dismantling of steel and reinforced concrete span structures with defects. It contains a description and analysis of various dismantling methods, as well as key elements of the survey report and the necessary calculations based on the selected dismantling method. Specific aspects of calculating the bearing capacity and load-bearing capacity of structures with defects are considered. The article describes an example of a dangerous defect - sagging - and methods for its detection.

Keywords: Composite beam spans, dismantling, survey, calculation of carrying capacity, calculation of load capacity, defects, sagging.

Введение

Сталежелезобетонные мосты – одна из самых распространенных конструкций мостов, применяемая с 40-50-х гг. XX века. Такие конструкции мостов имеют ряд преимуществ перед стальными – ж/б плита проезжей части дешевле и проще в изготовлении, чем ортотропная металлическая конструкция. Одним из авторов, заложившим базу для применения комбинированных конструкций стал Е.Е. Гибшман [1]. Профессор описал в своей работе основные принципы конструирования и расчета таких мостов. Продолжили совершенствовать подходы к применению сталежелезобетона Н.Н. Стрелецкий, П.М. Саламахин, С.А.

Ильясевич [2-4]. Современное состояние вопроса проектирования и расчета таких конструкций широко изучено М.М. Корнеевым, П.П. Ефимовым [5-8]. Численное моделирование сложных конструкций – неотъемлемая часть современного проектирования. В работах [9-13] описано приложение современных методов расчета комбинированных систем с использованием программных комплексов.

Срок службы сталежелезобетонных пролетных строений мостов согласно СП 35.13300 составляет 100 лет, срок для первого ремонта 50 лет, срок службы после ремонта не менее 25 лет. Логично, что сооружения, построенные в середине XX века подходят к концу своего срока службы. Если пролетное строение сильно изношено, то ремонт может быть экономически нецелесообразен, и следует заменить пролетное строение на новое. Исследования в области обследования, оценки, ремонта и реконструкции проводились Бокаревым С. А., Быстровым В. А., Феоктистовой Е. П. и др. [14-18]. Демонтаж пролетных строений описан в работе [19], однако автор не приводит описания работ по демонтажу сталежелезобетонной конструкции.

В ходе работ по реконструкции сталежелезобетонных балочных мостов не редко случаются аварии и обрушения несущих конструкций. Авторы считают, что главные причины аварий на таких мостах: несоблюдение организациями технологии производства работ, предусмотренной проектом, вследствие незнания принципов работы конструкции; ошибки проектной и рабочей документации.

Цель исследования авторов – осветить вопросы обследования и оценки сталежелезобетонных пролетных строений мостовых сооружений с дефектами при проектировании их демонтажа.

Для достижения целей работы подробно разобраны способы демонтажа, приведен перечень необходимой документации, перечень расчетов для проекта демонтажа, разобран случай одного из распространенных дефектов – провисания, вызванного расстройством шва объединения железобетонной плиты со стальной частью.

Материалы и методы

Оценка несущей способности пролетного строения чаще всего требуется при разработке проектной документации по реконструкции (капитальному ремонту) сооружения для выбора способа реконструкции или полной замене пролетного строения. Чаще всего после предпроектного обследования без оценки несущей способности принимается решение о замене пролетного строения в связи с несоответствием его актуальным требованиям (по габариту проезда, по грузоподъемности, по безопасности), наличием дефектов (мостового полотна, пролетного строения, опорных частей и др.). Корректность таких решений не оспаривается. При этом необходимость оценки несущей способности пролетного строения зачастую не отпадает, поскольку усилия, возникающие при его демонтаже (в зависимости от способа), могут в некоторых элементах превышать эксплуатационные. Однако, в процессе работ по демонтажу пролетного строения в нем могут возникнуть усилия, превышающие эксплуатационные, что при отсутствии оценки несущей способности может привести к аварии.

Нормативные документы ОДН 218.0.032-2003, СП 79.13330, СТО 002494680-0032-2004 подробно описывают содержание, виды и состав работ производимых обследований. Заказчик не всегда способен правильно оценить результаты обследования, в результате чего могут быть приняты некорректные решения в проекте демонтажа.

Рассмотрим способы и порядок демонтажа сталежелезобетонных пролетных строения:

- Разборка на временных опорах. Под пролетное строение с шагом 8...12 м устанавливаются временные опоры, производится его демонтаж. При данном способе последовательность разборки большого значения не имеет, допустимо использование ударной техники для демонтажа плиты. Способ требует минимум исходных данных и минимум расчетов, но является наиболее затратным и не везде применим.
- Демонтаж взрывом. Применяется достаточно редко ввиду ограниченной применимости, отсутствия у заказчика опыта производства взрывных работ, отсутствия нормативной базы. Способ требует больше исходных данных, чем способ 1. Так, в частности, для расчета мощности взрыва требуется точно знать геометрические характеристики.
- Демонтаж сбрасыванием. Производится сдвижкой пролетного строения на временные опоры с последующим опрокидыванием. Применяется редко, имеет низкую стоимость реализации, имеет значительные ограничения по области применения. Данному динамическому воздействию посвящена работа [20].
- Поэтапная разборка. В разных вариантах это самый распространенный метод. Рассмотрим общую последовательность разборки:
 - Демонтаж элементов мостового полотна;
 - Демонтаж плиты проезжей части;
 - Демонтаж металлоконструкций блоков главных балок.

Используются следующие способы: выкатка стальной части пролетного строения, демонтаж плетей блоков главных балок с использованием кранов. В данном способе могут применяться одна или несколько временных опор. Если известна технология монтажа, то демонтаж следует производить в обратной последовательности. Способ требует максимальную полноту исходных данных, является наиболее трудоемким с точки зрения проектирования и реализации, но при этом наиболее дешевый (если не рассматривать демонтаж взрывом).

Далее рассмотрим способ демонтажа поэтапной разборки. Для разработки проектной (рабочей) документации организации – разработчику проекта для изучения и анализа, должна предоставляться следующая документация:

- Проектная документация на строительство;
- Исполнительная документация по строительству;
- Проектная документация на ремонты (если проводились);
- Исполнительная документация по ремонтам (если проводились);
- Технический паспорт мостового сооружения;
- Книга моста (если она имеется);
- Отчеты о предпроектном и других (если проводились) обследованиях и испытаниях.

Зачастую часть перечисленной документации отсутствует.

Приведем минимальный набор данных по пролетному строению, требуемых в общем случае (при варианте демонтажа поэтапной разборкой) для разработки документации по его демонтажу, который должен содержаться в отчете о предпроектном обследовании:

- Схема моста;

- Габарит проезда и полная ширина пролетного строения;
- Расстояния между осями главных балок, между поперечными связями, расположение продольных и поперечных ребер стенок балок;
- Эпюра материалов пролетного строения;
- Конструкция продольных и поперечных связей, домкратных балок;
- Геометрические размеры плиты проезжей части; наличие трещин и ширина их раскрытия (максимальный шаг измерения 6м);
- Данные об элементах мостового полотна, толщины слоев дорожной одежды (максимальный шаг измерения 6м);
- Марки сталей и бетона конструкций;
- Данные об армировании в зонах промежуточных опор;
- Данные о конструкции шва объединения
- Вертикальные профили (продольный и поперечный) проезжей части и блоков главных балок (желательно в уровне верха или низа вертикальной стенки);
- Ведомость дефектов, фотоотчет.

Приведем перечень расчетов, необходимых при разработке документации по демонтажу.

В первую очередь следует определить действующие усилия от постоянных и временных нагрузок на стадии эксплуатации. Далее следует определить усилия, возникающие при предполагаемом способе демонтажа, и сравнить их с эксплуатационными. В случае если последние ниже, рекомендуется рассмотреть возможность снизить усилия, возникающие при демонтаже.

В оценке несущей способности пролетного строения нет необходимости в следующих ситуациях: когда достоверно известна технология строительства, отсутствие значимых дефектов в конструкции, демонтаж выполняется строго в обратной последовательности монтажа, и пролетное строение дополнительно «облегчено» (удалены консоли, смонтированы дополнительные временные опоры). В остальных случаях оценка несущей способности пролетного строения обязательна.

Достоверную картину НДС (напряженно-деформированного состояния) пролетного строения возможно получить лишь имея полный набор данных предпроектного обследования, а также вышеперечисленную документацию по пролетному строению, достоверно зная стадийность сооружения.

При отсутствии проектной и рабочей документации, данных о технологии строительства, опираясь на данные предпроектного обследования возможно получить пределы сформировавшихся напряжений и усилий. Определяющим фактором в таком случае, как правило, являются критерии прочности и устойчивости конструкции. Производится два постадийных расчета.

Неблагоприятная последовательность производства работ для НДС стальных главных балок – плита проезжей части бетонируется (монтируется, в случае укладки сборных плит) в одну стадию. После набора прочности плиты (участков омоноличивания) в работу сооружается мостовое полотно;

Неблагоприятная последовательность производства работ для НДС плиты проезжей части - сборка блоков главных балок и бетонирование плиты (либо укладка сборных плит и омоноличивание швов) выполняется на временных опорах, расположенных с шагом 8...12 м.

После включения плиты в работу временные опоры демонтируются, прикладывается нагрузка от мостового полотна.

В расчетах при отсутствии данных об арматуре, она не учитывается.

Расчеты следует производить с учетом возможности образования трещин. При отсутствии данных об арматуре принимается, что в сечениях на промежуточных опорах плита не воспринимает растягивающих усилий (работает только стальное сечение).

Результатом этих расчетов являются огибающие эпюры напряжений и усилий, показывающие возможное НДС пролетного строения.

Затем производится расчет пролетного строения с дефектами на стадии эксплуатации и стадийный расчет демонтажа. Результаты сравниваются эксплуатационными. Усилия при демонтаже должны быть меньше минимальных теоретических усилий при эксплуатации с дефектами.

Один из самых распространенных видов дефектов сталежелезобетонных пролетных строений – провисание.

Провисание пролетного строения – такой фактический продольный профиль при действии постоянных нагрузок, который ниже линии проектного продольного профиля.

Возможные причины провисания:

1. Отступления от проектной технологии (этапности) сооружения железобетонной плиты;
2. Отсутствие учета (или некорректный учет) ползучести бетона в проекте;
3. Сверхпроектные постоянные нагрузки (увеличение веса дорожной одежды при некачественном ремонте);
4. Остаточные деформации вследствие пропуска нерасчетных тяжелых временных нагрузок;
5. Расстройство шва объединения железобетонной плиты со стальной частью.

Первая причина не может быть выявлена без наличия исполнительных съемок продольного профиля главных балок пролетного строения, как на стадиях монтажа, так и перед приемкой в эксплуатацию.

Вторая причина может быть определена расчетным путем, но для этого необходимы соответствующие исходные данные. В 1950-1960-х годах не было достаточного опыта эксплуатации сталежелезобетонных пролетных строений, явление ползучести могло быть не учтено или учтено не в полной мере.

Третья причина выявляется при квалифицированном обследовании.

Четвертую причину невозможно выявить без данных о пропуске сверхтяжелых нагрузок по пролетному строению.

Последняя причина наиболее опасна. Расстройство шва объединения превращает сталежелезобетонную конструкцию в стальную, металлическая часть испытывает усилия, не предусмотренные проектом.

Данный дефект легко выявляется в процессе проведения испытаний. При динамических испытаниях превышение фактического периода собственных колебаний над расчетным может указывать на нарушение работы шва объединения. Аналогично, увеличение прогибов, измеренных в результате статических испытаний также может свидетельствовать о наличии данного дефекта.

В ходе статических испытаний можно точно определить зоны, где произошло нарушение работы шва, путем измерения изменений значений напряжений, как фибровых, так и по верхней и нижней частям стенки. Эти изменения наглядно демонстрируются в результатах расчета задачи (Рисунки 1-4).

Результат и обсуждение

Для наглядности выводов о влиянии расстройтва шва объединения на НДС конструкции рассмотрена следующая задача: неразрезное трехпролетное сталежелезобетонное пролетное строение по схеме 18+27+18м, нагруженное равномерно распределенной по плите нагрузкой, высота стальной балки 1.2м, толщина железобетонной плиты 0.25м. Рассмотрены 4 расчетных случая:

Сталежелезобетонная конструкция работает, как единое целое, без дефектов шва (Рисунок 1);

Полное расстройство шва объединения (Рисунок 2);

Расстройство шва объединения на участках в пролетах (Рисунок 3);

Расстройство шва объединения в опорных участках на промежуточных и крайних опорах (Рисунок 4).

Ниже приведены результаты расчетов. На (Рисунки 1-4) показан фасад балки, в цвете показаны только сжимающие напряжения, растянутые участки окрашены серым цветом.

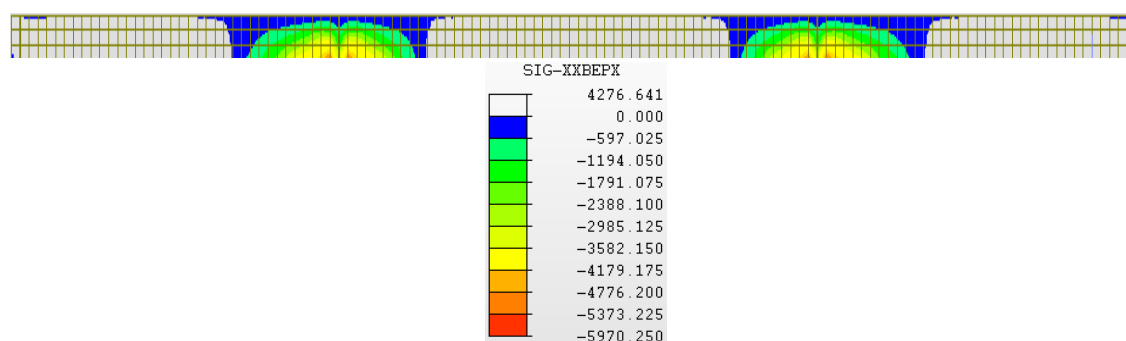


Рисунок1 - Распределение нормальных напряжений в балке, тс/м². Расчетный случай 1

В первом случае центр тяжести сечения расположен вблизи верхнего пояса.

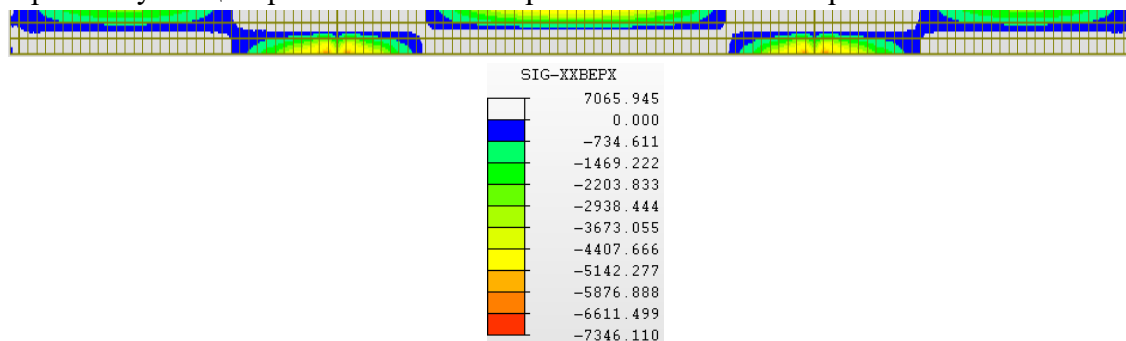


Рисунок 2 - Распределение нормальных напряжений в балке, тс/м². Расчетный случай 2

Во втором случае центр тяжести сечения расположен вблизи середины стенки. Стальная балка работает отдельно от плиты.

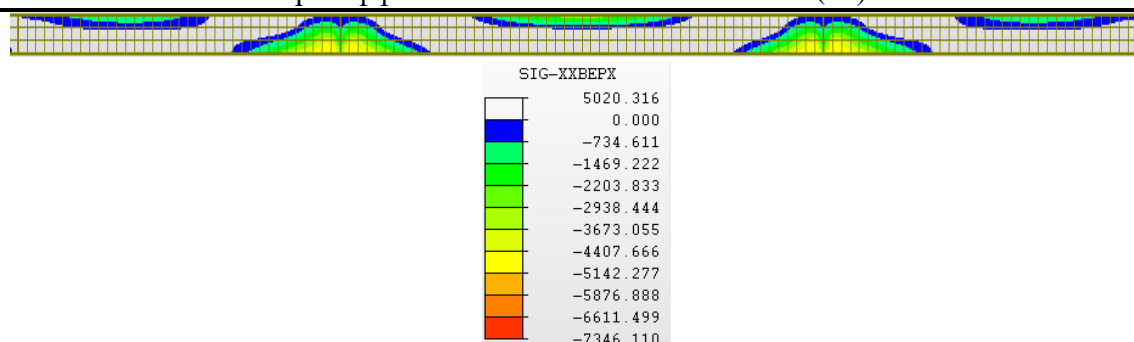


Рисунок 3 - Распределение нормальных напряжений в балке, тс/м². Расчетный случай 3

В третьем случае стальная балка работает отдельно от плиты на участках в пролетах.

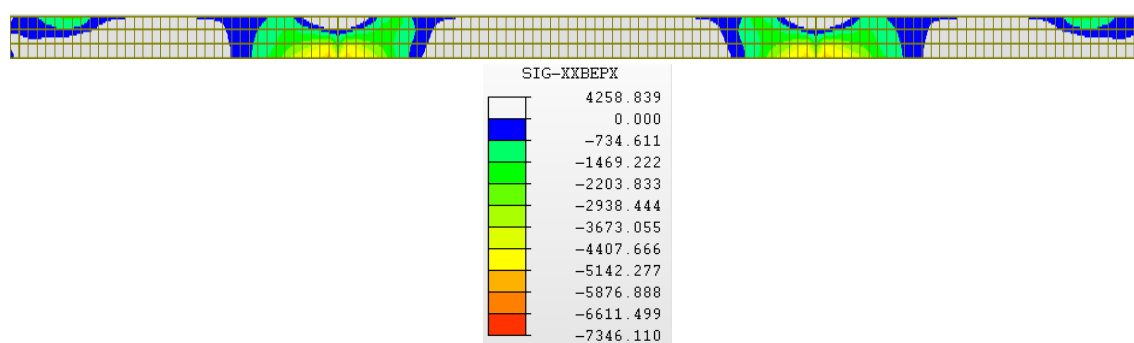


Рисунок 4 - Распределение нормальных напряжений в балке, тс/м². Расчетный случай 4

В четвертом случае стальная балка работает отдельно от плиты на опорных участках.

Аналогичную картину можно получить на практике при производстве статических испытаний путем постановки с определенным шагом в верхней и нижней зоне стенки датчиков (тензодатчики), измеряющих относительную деформацию, по которой вычисляется изменение напряжения. Далее расчетным путем, сравнивая результаты со значениями, полученными на практике, достаточно точно можно выявить зоны пролетного строения с нарушением работы шва объединения. При этом следует иметь в виду, что возможен нелинейный закон работы шва. Например, на определенном участке произошло смятие бетона в зоне упоров, сдвигающие усилия перераспределяются на соседние участки. При малых нагрузках на этом участке (где нарушена работа шва) в сечении может работать только стальная балка, при увеличении нагрузки плита может частично вовлекаться в работу. То есть статическую нагрузку рекомендуется прикладывать поэтапно, производя при этом измерения.

В соответствии с СТО 002494680-0032-2004, выявление зон с нарушением работы шва объединения рекомендуется производить визуально, либо путем измерения смещения плиты относительно стальной балки. Также в СТО указано, что смещение экспериментально определенного положения нейтральной оси сечения вниз может свидетельствовать о расстройстве шва в непосредственной близости к рассматриваемому сечению.

Заключение

1. Для безопасного демонтажа сталежелезобетонных пролетных строений необходимо правильно собрать как можно более полный набор исходных данных о конструкции. В случае

отсутствия достоверной информации о технологии производства плиты следует предположить наиболее неблагоприятную последовательность работ.

2. Следует подчеркнуть, что определить сформировавшуюся несущую способность конструкции сталежелезобетонного пролетного строения в процессе испытаний невозможно. Доступные средства измерений позволяют с достаточной точностью фиксировать изменения напряжений и перемещений в зависимости от приложенной нагрузки, однако они не способны выявить реальные действующие в элементе напряжения.

3. Дефекты пролетного строения могут повлечь аварию при выполнении демонтажа. Один из самых распространенных дефектов – расстройство шва объединения можно обнаружить и оценить способами, описанными в статье.

Список литературы

1. Гибшман Е. Е. Мосты со стальными балками, объединёнными с железобетонной плитой. М.: Дориздат, 1952. - 86 с.
2. Стрелецкий Н. Н. Сталежелезобетонные пролетные строения мостов. 2-е изд., перераб. и доп. – М.: Транспорт, 1981. – 360 с.
3. Саламахин П. М. Инженерные сооружения в транспортном строительстве. М.: Издательский центр «Академия», 2007. – 352 с.
4. Ильясевич С. А. Металлические коробчатые мосты. М.: Транспорт, 1970 – 280 с.
5. Корнеев М. М. Сталежелезобетонные мосты: теоретическое и практическое пособие по проектированию. – СПб.: ФГБОУ ВПО ПГУПС, 2015. – 400с.
6. Ефимов П. П. Проектирование мостов. Омск, 2006. – 110 с.
7. Корнеев М. М. Стальные мосты. К., 2003. – 547 с.
8. Корнеев М. М. Стальные мосты. Теоретическое и практическое пособие по проектированию мостов в двух томах. К.: Издательство «Академпред», 2010. – Т. 1. – 532 с.
9. Шишов М. А. Особенности расчета и проектирования шва объединения железобетонной плиты со стальной конструкцией в сталежелезобетонных пролётных строениях автодорожных мостов / М. А. Шишов, А. А. Галимзянов // Транспортное строительство. – 2016. – № 3. – С. 3–6.
10. Метод изготовления предварительно напряженных конструкций с композитным армированием и композитным фибробетоном / Т. А. Зиннуров, А. А. Пискунов, О. К. Петропавловских [и др.] // Транспортные сооружения. – 2017. – Т. 4, № 2. – С. 5. – DOI 10.15862/05TS217. – EDN ZEKYSD
11. Зиннуров, Т. А. Исследование совместной работы деревянных составных балок / Т. А. Зиннуров, К. А. Нурмухаметов // Современное строительство и архитектура. – 2017. – № 4(08). – С. 20-23. – DOI 10.18454/mca.2017.08.4. – EDN ZUCURP.
12. Мирсаяпов И. Т. Исследование напряженно-деформированного состояния сталежелезобетонных балок с частичной заделкой двутавровых сечений в бетоне / И. Т. Мирсаяпов, И. М. Гиматдинов // Известия Казанского государственного архитектурно-строительного университета. – 2022. – № 3(61). – С. 56-66. – DOI 10.52409/20731523_2022_3_56. – EDN FDMELF.
13. Мирсаяпов И. Т. Исследование напряженно-деформированного состояния сталежелезобетонных балок нового типа железнодорожных мостов / И. Т. Мирсаяпов,

- А. Т. Валиев // Известия Казанского государственного архитектурно-строительного университета. – 2023. – № 1(63). – С. 31-42. – DOI 10.52409/20731523_2023_1_31. – EDN ECDUWC.
14. Бокарев С. А. Об эффективности некоторых способов оценки технического состояния сталежелезобетонных пролетных строений / С. А. Бокарев, Л. Ю. Соловьев, Д. Н. Цветков // Вісник Дніпропетровського національного університету залізничного транспорту ім. академіка В. Лазаряна. – 2007. – № 14. – С. 162-167. – EDN UJIVX.
15. Быстров В. А. Методика определения ресурса конструкций сталежелезобетонных и металлических мостов с учетом их фактической динамической нагруженности и дефектности / В. А. Быстров // Инновации и долговечность объектов транспортной инфраструктуры (материалы, конструкции, технологии): Материалы научно-практической конференции, Санкт-Петербург, 14 ноября 2018 года / Под редакцией М. П. Клековкиной. – Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, 2019. – С. 84-89. – EDN QXVEMO
16. Феоктистова Е. П. Оценка остаточного усталостного ресурса металлических балок сталежелезобетонных пролетных строений автодорожных мостов / Е. П. Феоктистова // Транспортные сооружения. – 2019. – Т. 6, № 3. – С. 13. – EDN SYASXU.
17. Быстров В. А. Проблемы обоснования режимов фактической динамической нагруженности и ресурса долговечности конструкций сталежелезобетонных автодорожных и городских мостов / В. А. Быстров, Н. В. Козак, Д. А. Ярошутин // Транспортные сооружения. – 2019. – Т. 6, № 4. – С. 5. – DOI 10.15862/06SATS419. – EDN GBIJSS.
18. Н. В. Козак, А. В. Сырков, В. А. Быстров, Д. А. Ярошутин. Анализ влияния отказов элементов объединения на эксплуатационную надежность сталежелезобетонных пролетных строений автодорожных мостов // Транспортные сооружения. – 2023. – Т. 10, № 3. – DOI 10.15862/07SATS323. – EDN STEARU
19. Веселовский В. Ю. Анализ современных методов демонтажа пролетных строений / В. Ю. Веселовский // Модернизация и научные исследования в транспортном комплексе. – 2013. – Т. 3. – С. 100-109. – EDN QCVGQX.
20. Зылева Н. В. Оценка динамических воздействий на наземные сооружения при демонтаже пролетного строения методом сбрасывания / Н. В. Зылева // Вестник Томского государственного архитектурно-строительного университета. – 2007. – № 3(16). – С. 139-147. – EDN JUCZXZ.

References

1. Gibshman E. E. Bridges with steel beams combined with a reinforced concrete slab. M.: Dorizdat, 1952. - p. 86
2. Streletsky N. N. Steel-reinforced concrete superstructures bridges. 2nd ed., reprint. and additional. – M.: Transport, 1981. – p. 360
3. Salamakhin P. M. Engineering structures in transport construction. M.: Publishing center "Academy", 2007. – p. 352
4. Ilyasevich S. A. Metal box bridges. M.: Transport, 1970 – p. 280
5. Korneev M. M. Steel-reinforced concrete bridges: a theoretical and practical guide to design. – St. Petersburg: FGBOU VPO PGUPS, 2015. – p. 400

6. Efimov P. P. Bridge design. Omsk, 2006. – p. 110
7. Korneev M. M. Steel bridges. K.:, 2003. – p. 547
8. Korneev M. M. Steel bridges. Theoretical and practical guide to bridge design in two volumes. K.: Publishing house "Academpres", 2010. – Vol. 1. – p. 532
9. Shishov M. A. Features of calculation and design of the joint of a reinforced concrete slab with a steel structure in steel–reinforced concrete superstructures of road bridges / M. A. Shishov, A. A. Galimzyanov // Transport construction. – 2016. – No. 3. - pp. 3-6.
10. The method of manufacturing prestressed structures with composite reinforcement and composite fiber concrete / T. A. Zinnurov, A. A. Piskunov, O. K. Petropavlovsk [et al.] // Transport structures. - 2017. – Vol. 4, No. 2. – p. 5. – DOI 10.15862/05TS217. – EDN ZEKYSD.
11. Zinnurov, T. A. The study of the joint work of wooden composite beams / T. A. Zinnurov, K. A. Nurmukhametov // Modern construction and architecture. – 2017. – № 4(08). – pp. 20-23. – DOI 10.18454/mca.2017.08.4. – EDN ZUCURP
12. Mirsayapov I. T. Investigation of the stress-strain state of steel-reinforced concrete beams with partial sealing of I-sections in concrete / I. T. Mirsayapov, I. M. Gimatdinov // Izvestiya Kazan State University of Architecture and Civil Engineering. – 2022. – № 3(61). – pp. 56-66. – DOI 10.52409/20731523_2022_3_56. – EDN FDSELF.
13. Mirsayapov I. T. Investigation of the stress-strain state of steel-reinforced concrete beams of a new type of railway bridges / I. T. Mirsayapov, A. T. Valiev // Izvestiya Kazan State University of Architecture and Civil Engineering. – 2023. – № 1(63). – pp. 31-42. – DOI 10.52409/20731523_2023_1_31. – EDN ECDUWC
14. Bokarev S. A. On the effectiveness of some methods for assessing the technical condition of steel-reinforced concrete superstructures / S. A. Bokarev, L. Yu. Solovyov, D. N. Tsvetkov // Bulletin of the Dniester National University of Hospital Transport im. academician V. Lazaryan. - 2007. – No. 14. – pp. 162-167. – EDN UJIIVX.
15. Bystrov V. A. Methodology for determining the resource of structures of steel-reinforced concrete and metal bridges, taking into account their actual dynamic loading and defects / V. A. Bystrov // Innovations and durability of transport infrastructure facilities (materials, structures, technologies): Materials of the scientific and practical conference, St. Petersburg, November 14, 2018 / Edited by M. P. Klekovkina. – St. Petersburg: St. Petersburg State University of Architecture and Civil Engineering, 2019. - pp. 84-89. – EDN QXVEMO.
16. Feoktistova E. P. Evaluation of the residual fatigue life of metal beams of steel-reinforced concrete superstructures of road bridges / E. P. Feoktistova // Transport structures. – 2019. – Vol. 6, No. 3. – p.13. – EDN SYASXU.
17. Bystrov V. A. Problems of substantiation of the modes of actual dynamic loading and durability of structures of steel-reinforced concrete road and city bridges / V. A. Bystrov, N. V. Kozak, D. A. Yaroshutin // Transport structures. – 2019. – Vol. 6, No. 4. – p. 5. – DOI 10.15862/06SATS419. – EDN GBIJSS.
18. N. V. Kozak, A.V. Syrkov, V. A. Bystrov, D. A. Yaroshutin. Analysis of the impact of failures of association elements on the operational reliability of steel-reinforced concrete superstructures of road bridges // Transport structures. - 2023. – Vol. 10, No. 3. – DOI 10.15862/07SATS323. – EDN STEARU.

19. Veselovsky V. Yu. Analysis of modern methods of dismantling superstructures / V. Yu. Veselovsky // Modernization and scientific research in the transport complex. – 2013. – Vol. 3. – pp. 100-109. – EDN QCVGQX.
 20. Zyleva N. V. Assessment of dynamic impacts on ground structures during the dismantling of a superstructure by dropping / N. V. Zyleva // Bulletin of the Tomsk State University of Architecture and Civil Engineering. – 2007. – № 3(16). – pp. 139-147. – EDN JUCZXZ.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 535 (623.4) (355)

АНАЛИЗ ВОЗДЕЙСТВИЯ ЛАЗЕРНОГО ИЗЛУЧЕНИЯ НА ОПТИЧЕСКИЕ УСТРОЙСТВА БПЛА

Ворганов А.А., Котенёв Е.В., ¹Курдюмов И.А., Каленский И.А., Федоров А.М.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», г. Москва, Россия
(119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: ¹kurdyumov-2003@mail.ru

В данной статье рассматривается воздействие лазерного излучения на оптические устройства беспилотных летательных аппаратов (БПЛА). Особое внимание уделяется анализу механизмов повреждения оптических компонентов под воздействием высокоэнергетического лазерного излучения, а также методам защиты и минимизации рисков. Исследование включает экспериментальные данные и теоретические модели, которые позволяют оценить устойчивость различных типов оптических устройств к лазерному воздействию. Результаты исследования могут быть полезны для разработки более надежных и устойчивых оптических систем для БПЛА, а также для повышения их безопасности и эффективности в условиях потенциальных угроз.

Ключевые слова: Лазерное излучение, оптические устройства, беспилотные летательные аппараты (БПЛА), повреждение оптических компонентов, защита оптических систем, экспериментальные данные, теоретические модели.

ANALYSIS OF THE EFFECT OF LASER RADIATION ON UAV OPTICAL DEVICES

Varganov A.A., Kotenev E.V., Kurdyumov I.A., Kalensky I.A., Fedorov A.M.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ¹kurdyumov-2003@mail.ru

This article examines the effect of laser radiation on the optical devices of unmanned aerial vehicles (UAVs). Special attention is paid to the analysis of the mechanisms of damage to optical components under the influence of high-energy laser radiation, as well as methods of protection and risk minimization. The study includes experimental data and theoretical models that allow us to assess the resistance of various types of optical devices to laser exposure. The results of the study can be useful for the development of more reliable and stable optical systems for UAVs, as well as for improving their safety and effectiveness in the face of potential threats.

Keywords: Laser radiation, optical devices, unmanned aerial vehicles (UAVs), damage to optical components, protection of optical systems, experimental data, theoretical models.

Введение

Лазерные системы становятся все более актуальным и эффективным средством поражения различных целей, включая беспилотные летательные аппараты (БПЛА). В связи с развитием технологий и появлением новых угроз в области беспилотной авиации, вопрос применения лазерных систем для уничтожения БПЛА становится все более важным. Целью данной статьи является изучение перспектив и применения лазерных систем для поражения беспилотных летательных аппаратов через оптические устройства. Более конкретно, статья будет посвящена анализу возможностей лазерных систем в обнаружении, отслеживании, безопасном отключении и уничтожении беспилотных летательных аппаратов.

Актуальность данной темы обусловлена ростом числа беспилотных летательных аппаратов, которые могут использоваться как для военных, так и для гражданских целей. Они представляют серьезную угрозу для безопасности и конфиденциальности, требуя эффективных методов обнаружения и поражения. Анализ перспектив и применения лазерных систем для уничтожения БПЛА является актуальной задачей, целью которой является определение возможностей и ограничений данного метода борьбы с угрозами, представляемыми беспилотными летательными аппаратами.

1. Теоретические и физические основы лазерных систем для поражения беспилотных летательных аппаратов

1.1. Принцип работы лазера заключается в следующих этапах

Усиление излучения: В основе работы лазера лежит процесс усиления световых волн. Атомы или молекулы в активной среде лазера переходят из возбужденного состояния в основное, испуская фотоны. При этом высвобожденные фотоны могут стимулировать другие атомы к испусканию дополнительных фотонов того же частотного и фазового состояния, что приводит к усилению излучения.

Механизм генерации лазерного излучения: Для генерации лазерного излучения необходимо создать инверсную заселенность уровней энергии в активной среде лазера. Это достигается путем накачки активной среды энергией, которая вынуждает атомы или молекулы переходить в возбужденное состояние. Затем, при стимулированном излучении, происходит усиление световых волн, что приводит к генерации лазерного излучения.

Основные компоненты лазеров: Основными компонентами лазеров являются активная среда (обычно это кристалл, газ или полупроводник), оптический резонатор (зеркала, обеспечивающие многократное отражение световых волн внутри резонатора) и источник накачки (обычно это лампы или полупроводниковые диоды). Также в лазерных системах могут применяться дополнительные элементы, такие как модуляторы, оптические фильтры и детекторы.[1]

1.2. Характеристики влияющие на поражение цели

Смертоносность лазера зависит от многих характеристик, но упрощенно нам будет достаточно следующих:

Одним из ключевых параметров лазерного оружия является выходная мощность. Это количество энергии, которое излучается лазером в виде светового пучка. Чем выше выходная мощность, тем мощнее и эффективнее лазерное оружие. Однако, увеличение выходной мощности приводит к увеличению расходов на энергию и системы охлаждения, а также к увеличению габаритов и массы лазерной установки.

Еще одним важным фактором, влияющим на эффективность лазерного оружия, является расстояние до цели и как следствие - явление дифракции. При увеличении расстояния до цели лазерный луч расширяется, что приводит к уменьшению плотности энергии на поверхности цели. [2] Чем больше расстояние до цели, тем сильнее влияние дифракции на эффективность лазерного оружия. Кроме того, длина волны лазерного излучения также влияет на степень расходимости луча, чем больше длина волны, тем сильнее расходится луч на расстоянии.

Длина волны лазерного излучения также играет важную роль в эффективности лазерного оружия. Чем короче длина волны, тем выше энергия фотонов и тем сильнее взаимодействие лазерного излучения с целью. Однако, создание мощных лазерных систем с короткой длиной волны является технологически сложной задачей.

Коэффициент M^2 является важным параметром, который характеризует качество лазерного луча и его способность фокусироваться на цели. Коэффициент M^2 равен 1 для идеального лазерного луча, который ограничен только дифракцией. Однако, в реальных лазерных системах коэффициент M^2 обычно превышает 1, что свидетельствует о наличии аберраций и искажений в лазерном луче.

Наконец, размер зеркала в лазерных системах также влияет на эффективность лазерного оружия. В лазерных системах используются термостойкие зеркала, которые направляют лазерный луч изнутри установки на подвижную турель, которая фокусирует лазерное излучение на цель с помощью главного зеркала. Чем больше размер зеркала, тем лучше лазерный луч может фокусироваться на цели, создавая как можно меньшую точку на поверхности цели.

Все эти данные являются вводными, с их помощью можно получить еще две принципиально важные для нас величины: диаметр лазерного пятна [м] и энергия лазера, попадающая на поверхность цели [КВт/см²].

Таким образом, эффективность лазерного оружия зависит от многих факторов, включая выходную мощность, расстояние до цели, дифракцию, коэффициент M^2 , длину волны и размер зеркала. При проектировании и использовании лазерных систем необходимо учитывать все эти факторы, чтобы достичь максимальной эффективности лазерного оружия. [3]

Но если изменение вышеперечисленных параметров на более выгодные является достаточно проблематичной задачей, мы можем работать с менее прямыми, но не менее эффективными параметрами. Таким как частота следования импульсов — это количество импульсов, которые формируются лазером в единицу времени. Перспективы работы с этим параметром подробно разобраны в следующем пункте.

2. Ослепление и вывод из строя оптических систем беспилотников с помощью лазеров

Ослепление и вывод из строя оптических систем беспилотников с помощью лазеров основываются на физических явлениях взаимодействия излучения с веществом. Когда лазерный луч попадает на поверхность оптического элемента, происходит поглощение энергии излучения и преобразование ее в тепловую. Это приводит к локальному нагреву поверхности и, как следствие, к термическому разрушению или деформации оптического элемента. При этом, степень повреждения зависит от мощности лазера, длительности воздействия, свойств материала оптического элемента и других факторов.

Также, важную роль играет явление дифракции света. При лазерном ослеплении дифракция может приводить к тому, что луч, преломляется от самой оптической системы БПЛА и рассеивается на соседние элементы, что увеличивает зону повреждения.

Эти физические явления и законы подтверждаются многочисленными исследованиями в области лазерной физики и оптики. Например, в статье «Laser-Induced Damage in Optical Materials» авторы рассматривают механизмы повреждения оптических материалов под

действием лазерного излучения и приводят примеры экспериментальных исследований, подтверждающих эти механизмы.

Экспериментальные исследования показали, что лазерные системы могут быть эффективным средством их поражения. Например, экспериментальная передвижная наземная лазерная система «Афина», представленная в 2017 г компанией Lockheed Martin, была оснащена опытной демонстрационной гибридной лазерной установкой (твердотельный лазер + оптоволоконная активная среда) с заявленной мощностью непрерывного излучения 30 кВт. [4] Установка при тестировании смогла успешно сбить пять задействованных в испытаниях беспилотников. Радиус эффективного действия при такой мощности лазера достигает полутора километров при отведенном времени на уничтожение от 2 до 5 секунд.



Рисунок 1. - Наглядное изображение воздействия лазера на оптику БПЛА.

На Рисунке 1 представлено наглядное изображение воздействия лазера (достаточно слабого и свободного даже для гражданской продажи) на БПЛА. Мы можем отчетливо видеть какое сильное воздействие лазера получает оптика беспилотника. Оператор БПЛА вынужден или

отвернуть камеру, а соответственно потерять контакт с фронтом (противником), или получить высокий риск повреждения матрицы камеры или самого беспилотника. Выполнение боевых задач сводится к нулю, значительно затрудняется управление и в дополнение возникает опасность уничтожения беспилотника с помощью других средств ПВО (или даже стрелкового оружия, при условии низкой высоты полета).[5]

3.Расчёт эффективности лазеров в борьбе с БПЛА

Для оценки эффективности лазеров проведем моделирование и расчёт их действия на оптику БПЛА. При этом мы будем учитывать такие факторы как: выходная мощность излучения лазера, длина волны, расстояние до цели, характеристики оптики самой установки.

На основе результатов проведем анализ эффективности лазерных систем и опишем оптимальные параметры для их применения в конкретных условиях. В процессе расчёта эффективности лазеров необходимо также учитывать особенности конкретного типа БПЛА, такие как тип и размер оптики, материал корпуса, наличие систем защиты от лазерного

излучения и другие факторы, но из-за огромной вариативности, будет произведен общий анализ с несколькими конкретными примерами.

Для наглядности расчеты представлены в виде таблиц ниже.

Таблица 1. - Расчёты №1 различных настроек лазера.

	Выходная мощность, KWm	Расстояние, $км$	Коэфф. M^2	Длина волны, $мкм$	Радиус зеркала, $м$	Диаметр пятна, $м$	Энергия, KWm/cm^2
	Вводные данные установки					Расчётные данные	
№1	50	5	2	1,315	0,5	0,0263	9,20383271
№2	70	5	2	1,315	0,5	0,0263	12,8853651
№3	50	3	2	1,315	0,5	0,0157	25,5662019
№4	50	5	1,5	1,315	0,5	0,0197	16,3623692
№5	50	5	2	1,425	0,5	0,0285	7,83773351
№6	50	5	2	1,315	0,7	0,0187	18,0395121
№7	40	5	2	1,115	0,5	0,0223	10,2414270
№8	30	2	2	1,315	0,2	0,0263	5,52229962
№9	100	7	2	1,315	0,5	0,0368	9,39166603
№10	200	10	2	1,315	0,5	0,0526	9,20383271
№11	20	1	3	1,315	0,1	0,0394	1,63623692
№12	20	2	3	1,315	0,3	0,0263	3,68153308
№13	50	3	2	1,615	0,2	0,04845	2,71201851
№14	10	2	2	1,315	0,3	0,01753	4,14172472

Данные говорят о возможности использования подобных систем для полного уничтожения БПЛА противника, но используемая мощность слишком высока для практического использования. Но если сконцентрироваться на взаимодействии на оптику, то для этой цели можно использовать меньшую мощность.

Приведем пример со стандартным материалом в матрицах камер - кремний. При попадании на фотокатод лазерного импульса он поглощает излучение всей своей толщиной и нагревается (температура уничтожения 1415 С). [6] При наносекундных импульсах можно в первом приближении пренебречь теплоотводом в стеклянную подложку. При попадании на структуру мощного лазерного импульса излучение поглощается, в основном, в материале металлических дорожек и в полупроводниковых слоях. Поглощением в изолирующих слоях можно пренебречь. Поглощенное излучение преобразуется в тепло. Наибольшую концентрацию тепловыделения можно ожидать в металлических дорожках и сильно легированных областях полупроводника.

Таким образом, мощность достаточная для выхода из строя кремниевых фотокатодов в камере равна приблизительно 1,6кВт. Из результатов измерений видно, что данная мощность достигается всеми рассмотренными лазерами, даже лазером мощностью 20кВт на расстоянии 1км. При этом диаметр пучка лазера будет достаточной ширины для попадания по БПЛА. Учитывая предыдущие выводы, представим новые расчёты, с некоторыми дополнительными условиями, а также диаграмму соотношения диаметра пятна и энергии. Во-первых,

измерение №11 в первой таблице перенесем во вторую, так как оно идеально удовлетворяет условию достаточной мощности взаимодействия на камеру БПЛА и имеет реалистичную требуемую мощность. Во-вторых, эффективным расстоянием поражения примем 1 километр.

Таблица 2. - Расчёты №2 различных настроек лазера

	Выходная мощность, <i>KВт</i>	Расстояние, <i>км</i>	Коэфф. <i>M2</i>	Длина волны, <i>мкм</i>	Радиус зеркала, <i>м</i>	Диаметр пятна, <i>м</i>	Энергия, <i>KВт/см2</i>
	Вводные данные установки					Расчётные данные	
№1	20	1	3	1,315	0,1	0,0394	1,63623692
№2	15	1	3	1,315	0,1	0,0394	1,22717769
№3	15	1	3	1,15	0,1	0,0345	1,60458703
№4	15	1	3	1,315	0,2	0,0197	4,90871077
№5	10	1	2	1,315	0,1	0,0263	1,84076654
№6	5	1	3	1,315	0,1	0,0394	0,40905923
№7	5	1	2	1,315	0,2	0,0131	3,68153308
№8	5	1	2	1,315	0,1	0,0263	0,92038327
№9	5	1	3	1,315	0,2	0,0197	1,63623692
№10	3	1	2	1,315	0,2	0,0131	2,20891985
№11	3	1	3	1,115	0,2	0,0167	1,36552360
№12	3	1	2	1,115	0,1	0,0223	0,76810702
№13	2	1	2	1,315	0,3	0,0087	3,31337977
№14	1	1	2	1,315	0,3	0,0087	1,65668988
№15	1	1	3	1,315	0,5	0,0078	2,04529616

По итогу вторых измерений мы можем сказать, что существуют различные условия для поражения БПЛА с помощью лазеров. Так же мы получили ясную зависимость различных настроек и итоговых результатов воздействия. Например, диаграмма на Рисунке 2 показывает, что с увеличением диаметра пятна лазерного пучка, уменьшается энергия воздействия на беспилотник и наоборот, но также итоговые параметры зависят от других настроек. Более подробно все зависимости расписаны в таблицах ранее.



Рисунок 2. - Диаграмма соотношений диаметра пятна и энергии.

4. Применение определенных лазерных систем для поражения беспилотных летательных аппаратов

4.1. Лазерные системы на основе УКЛИ против БПЛА

Одним из перспективных направлений развития лазерных систем для поражения беспилотников является использование ультракоротких лазерных импульсов (УКЛИ). Это связано с тем, что УКЛИ обладают рядом преимуществ по сравнению с традиционными лазерными системами, такими как высокая пиковая мощность, короткая длительность импульса и низкое тепловое воздействие на окружающую среду.

Принцип действия лазерных систем, основанных на использовании УКЛИ, заключается в генерации лазерных импульсов длительностью до 5 фс ($5 \cdot 10^{-15}$ с). При этом пиковая мощность таких импульсов может достигать нескольких тераватт (в лабораторных условиях достигает петаватт), что значительно превышает мощность традиционных лазерных систем.

Одним из ключевых преимуществ лазерных систем, основанных на использовании УКЛИ, является их способность генерировать лазерные импульсы с очень высокой частотной шириной спектра. Это позволяет эффективно поражать оптические системы беспилотников за счет эффекта многофотонной ионизации. При этом процессе лазерное излучение поглощается оптическими элементами беспилотника, что приводит к их разрушению.

Кроме того, лазерные системы, основанные на использовании УКЛИ, могут эффективно использоваться для поражения целей, находящихся в движении. Это связано с тем, что короткая длительность лазерных импульсов позволяет минимизировать влияние эффекта Доплера, который может снизить эффективность поражения движущихся целей.

Одним из примеров лазерных систем, основанных на использовании УКЛИ, является система LWIR (Long-Wave Infrared) Laser Weapon, разработанная компанией Raytheon. Эта система использует лазерные импульсы длительностью несколько пикосекунд и пиковую мощность несколько киловатт. LWIR Laser Weapon способна эффективно поражать оптические системы беспилотников на расстоянии до нескольких километров.

4.2. Лазерные системы на основе высокоэнергетических лазеров

Разработанный армией США, HEL MD представляет собой наземную лазерную систему, способную противостоять различным угрозам, включая беспилотники. Она использует высокоэнергетический лазер для выведения из строя или уничтожения беспилотников, либо ослепляя их оптические системы, либо нанося физические повреждения.

В системе HEL MD используется твердотельный лазер, генерирующий высокосфокусированный луч света в инфракрасном диапазоне. Лазерный луч создается путем усиления низкоэнергетического лазерного луча с помощью ряда специализированных оптических компонентов, включая усилители и резонаторы. Полученный высокоэнергетический лазерный луч направляется на цель с помощью высокоточной системы слежения.

Когда лазерный луч попадает на цель, он быстро нагревает ее поверхность это может привести к физическому повреждению цели, например расплавлению или прогоранию компонентов оптики или к выходу из строя или датчиков БПЛА.

Система HEL MD разработана с высокой точностью, что позволяет ей фокусировать лазерный луч на очень маленькой области цели. Это позволяет нейтрализовать или уничтожить цель с минимальным сопутствующим ущербом.

В целом система HEL MD использует принцип направленной энергии для генерации высокосфокусированного лазерного луча, который может нейтрализовать или уничтожить цель.

Заключение

В статье рассмотрены перспективы и применение лазерных систем для поражения беспилотных летательных аппаратов. Было показано, что оптические системы беспилотников являются одними из наиболее уязвимых компонентов, и их вывод из строя может быть эффективным способом нейтрализации БПЛА.

Обзор существующих разработок лазерных систем для поражения беспилотников показал, что перспективными являются системы, основанные на использовании ультракоротких лазерных импульсов и высоко-фокусированных лучах в инфракрасном диапазоне. Перспективы развития лазерных систем для поражения беспилотников связаны с дальнейшим совершенствованием технологий генерации ультракоротких лазерных импульсов, а также с разработкой новых методов использования высоко-сфокусированных лучей в инфракрасном диапазоне. Одним из перспективных направлений является создание систем, способных автоматически обнаруживать и сопровождать цели, а также оптимизировать параметры лазерного излучения в зависимости от типа и характеристик оптических систем беспилотника.

В общем, лазерные системы для поражения беспилотников являются перспективным направлением развития военной техники, и их дальнейшее совершенствование будет способствовать повышению эффективности борьбы с беспилотными летательными аппаратами.

Список литературы

1. Аполлонов В. В. Лазерное оружие: проблемы и перспективы //Путь науки. – 2016. – №. 2. – С. 33.
2. Leonovich G. I. et al. Airborne LIDAR in ensuring gliding UAV flight mode //VESTNIK of Samara University. Aerospace and Mechanical Engineering. – 2014. – Т. 13. – №. 2. – С. 88-90.
3. П. Г. Крюков, “Лазеры ультракоротких импульсов”, Квантовая электроника, 31:2 (2001), С. 96–101
4. Шайдаев М. Ш. Лазерные системы для борьбы с беспилотными летательными аппаратами: преимущества и недостатки //Академическая мысль. – 2023. – №. 4 (25). – С. 157-162.
5. Ristau D. (ed.). Laser-induced damage in optical materials. – CRC Press, 2014.
6. Bennett H. E. et al. Laser-induced damage in optical materials: fifteenth ASTM symposium //Applied optics. – 1986. – Т. 25. – №. 2. – С. 290-270.

References

1. Apollonov V. V. Laser weapons: problems and prospects //The path of science. - 2016. – No. 2. – p. 33.
 2. Leonovich G. I. et al. Airborne LASER in ensuring gliding UAV flight mode //VESTNIK of Samara University. Aerospace and Mechanical Engineering. - 2014. – Vol. 13. – No. 2. – pp. 88-90.
 3. P. G. Kryukov, “Ultrashort pulse lasers”, Quantum Electronics, 31:2 (2001), pp. 96-101
 4. Shaidayev M. S. Laser systems for combating unmanned aerial vehicles: advantages and disadvantages //Academic thought. – 2023. – №. 4 (25). – Pp. 157-162.
 5. Ristau D. (ed.). Laser-induced damage in optical materials. – CRC Press, 2014.
 6. Bennett H. E. et al. Laser-induced damage in optical materials: fifth ASTM symposium //Applied optics. – 1986. – vol. 25. – No. 2. – pp. 290-270.
-