

ISSN 2221-7975



## ТРУДЫ

СЕВЕРО-КАВКАЗСКОГО ФИЛИАЛА  
ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ  
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО  
БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ  
«МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ  
СВЯЗИ И ИНФОРМАТИКИ»

РОСТОВ-НА-ДОНУ  
2023



Северо-Кавказский филиал ордена Трудового Красного  
Знамени федерального государственного бюджетного  
образовательного учреждения высшего образования  
«Московский технический университет связи и информатики»

---



**ТРУДЫ**  
**СЕВЕРО-КАВКАЗСКОГО ФИЛИАЛА**  
**МОСКОВСКОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА**  
**СВЯЗИ И ИНФОРМАТИКИ**

Подготовлены по результатам  
XVI  
Всероссийской научно-практической конференции  
«ИНФОКОМ 2023»

**Ростов-на-Дону**  
**2023**

УДК 621.396.1

ББК 32

Т 78

Т 78 Труды Северо-Кавказского филиала Московского технического университета связи и информатики - Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2023, 377 с.

Сборник зарегистрирован в международном центре ISSN (ISSN 2221-7975) и включен в перечень журналов РИНЦ

Сборник размещен в открытом бесплатном доступе на сайте [www.skf-mtusi.ru](http://www.skf-mtusi.ru)

В настоящий сборник включены статьи, подготовленные по результатам работы XVI Всероссийской научно-практической конференции «ИНФОКОМ 2023». Сборник объединяет статьи по актуальным научным направлениям развития инфокоммуникаций, математического моделирования систем и средств связи, а также инфокоммуникационных технологий в сфере образования.

Материалы статей, представленных в сборнике, даны в авторской редакции.

Сборник рассчитан на научных сотрудников, студентов и специалистов, работающих в области современных инфокоммуникационных технологий связи и информационных технологий в образовании.

Составление, дизайн, редакционная верстка сборника: Решетникова И.В.,  
Головенко М.В.

© СКФ МТУСИ, 2023

---

Текст: электронный  
Полиграфический центр «Университет» СКФ МТУСИ,  
Ростов-на-Дону, 344002, ул. Серафимовича, 62

## СОДЕРЖАНИЕ

### СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИЙ

Головской В.А., Влох Д.Д. Графовая модель функционирования когнитивной радиосистемы.....	11
Бородин А.В., Бородин А.А. Современные пироэлектрические приемники теплового излучения.....	18
Ершов В.В., Руденко Н.В., Кузенков Е.А., Васильев А.Э. О возможности построения резервного источника питания базовой станции сотовой связи на основе суперконденсаторов и аккумуляторных батарей.....	20
Елисеев А.В., Жуковский А.Г., Клименко М.Я., Разыкова М.Р. Анализ методов верификации данных авиационной телекоммуникационной системы.....	26
Елисеев А.В., Жуковский А.Г., Клименко М.Я., Разыкова М.Р. Обоснование структуры современной гибридной радиотехнической системы поиска терпящих бедствия транспортных средств.....	35
Руденко Н.В., Ершов В.В., Васильев А.Э. Локальная электроэнергетическая система с использованием возобновляемых источников для электроснабжения автономных объектов связи.....	42
Алферова И.А., Енгибарян И.А., Решетникова, И.В., Сафарьян О.А., Юхнов В.И. Погрешность формирования частоты в цифровых каналах передачи данных, обусловленная эффектом джиттера.....	46
Алферова И.А., Безуглов Ю.Д., Енгибарян И.А., Сафарьян О.А., Юхнов В.И. Влияние нестабильности частоты на вероятность битовой ошибки при передаче М-Кам-сигналов.....	52
Алферова И.А., Енгибарян И.А., Решетникова И.В., Сафарьян О.А., Юхнов В.И. Влияние кратковременной нестабильности частоты на отношение сигнал/шум в каналах связи.....	60
Фан Туан Ань Моделирование и анализ пик-фактора и коэффициента ошибок символов для амплитудно-фазовой модуляции.....	65
Дворниченко А.С. Основные понятия и способы применения API.....	79
Харченко В.В., Рудый С.В., Варгазарова А.Э., Болдырихин Н.В. Многочастотные антенны системы сотовой связи.....	83
Карпенко Е.А., Коршун А.М. Нейросетевая видеоаналитика как перспективное направление развития видеонаблюдения.....	85
Ба М. Построение КВ приемника-сканера для обнаружения ЛЧМ-сигналов зондирования на основе HASKRF ONE.....	87
Фам Дык Хи, Нгуен Ван Кыонг, Николаев А.В. Радиоэлектронные средства военно-инженерной службы Вьетнамской Народной Армии и перспектива их развития.....	94
Лазаренко С.В., Гриценко В.В., Решетникова И.В. Элементы устройства оценки параметров телеметрических сообщений.....	101
Пугачев И.В., Хумарянц С.Р., Решетникова И.В. Оценка эффективности алгоритма определения параметров аналогового сигнала на фоне помех.....	108
Пугачев И.В., Вехтер А.К., Решетникова О.А. Синтез системы ФАПЧ из условия максимума функции обобщенной мощности.....	115



<b>Лазаренко С.В., Лихачев Д.А., Пеньков А.С., Манин А.А.</b> Анализ эффективности фильтра объединенного принципа максимума при обработке информации о состоянии беспилотного летательного аппарата.....	<b>121</b>
<b>Пугачев И.В., Зубков А.Н., Зехцер В.О., Безуглов Ю.Д.</b> Структура цифровой системы оценки параметров телеметрических сообщений.....	<b>126</b>
<b>Лазаренко С.В., Евтюхов В.М., Енгибарян И.А.</b> Синтез интеллектуального фильтра сопровождения с нечеткой стратегией настройки параметров в задачах автоматизации управления воздушным движением.....	<b>132</b>
<b>Пугачев И.В., Камер Е.О., Юхнов В.И.</b> Адаптивные многорежимные регуляторы автоматизированных радиотехнических систем.....	<b>138</b>
<b>Кожяев Э.З., Ухов П.Э.</b> Дистанционное зондирование земли. Анализ способов получения информационных материалов.....	<b>145</b>

## ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

<b>Фатхулин Т.Д., Кожанов М.С.</b> Проблемы хранения и управления результатами статического анализа в жизненном цикле разработки безопасного по и пути их решения.....	<b>152</b>
<b>Фатхулин Т.Д., Климов Н.Ю., Гежин С.А.</b> Анализ нейросетевых технологий, позволяющих генерировать текст.....	<b>161</b>
<b>Фатхулин Т.Д., Лушин Е.А.</b> Анализ развития автоматической генерации кода для WEB-сервисов.....	<b>168</b>
<b>Фатхулин Т.Д., Фатхулина Г.Г., Ментус М.В.</b> Разработка методики формирования запроса к нейросети с целью генерации изображений с учетом рекомендаций компьютерной лингвистики.....	<b>175</b>
<b>Фролова М.М., Лобзенко П.В.</b> Мобильное устройство на нейросети для построения карты местности в графическом интерфейсе.....	<b>184</b>
<b>Ремигин П.И., Лобзенко П.В.</b> Сетевое приложение для службы технической поддержки.....	<b>188</b>
<b>Пузырная Л.В., Лобзенко П.В.</b> Оптимизация вычислительной сети предприятия с помощью метода виртуализации.....	<b>192</b>
<b>Кожанов А.Б., Лобзенко П.В.</b> Комбинированная CRM отдела обеспечения.....	<b>196</b>
<b>Зайцев И.О., Лобзенко П.В.</b> База данных администратора IT компании.....	<b>199</b>
<b>Головинов С.Э., Лобзенко П.В.</b> Автозапоминание нового материала при обучении.....	<b>201</b>
<b>Герцовский Н.Ю., Лобзенко П.В.</b> Сервер распределенной обучающей системы.....	<b>204</b>
<b>Зайцев Е.А., Устименко Д.Л.</b> Перспективы использования искусственного интеллекта в электроэнергетике.....	<b>207</b>
<b>Леонов М.П., Устименко Д.Л.</b> Этические аспекты искусственного интеллекта.....	<b>210</b>
<b>Найденова Ю.И., Решетникова И.В., Сафарьян О.А.</b> Построение экспертной системы для оценки криптостойкости алгоритма шифрования RSA.....	<b>213</b>
<b>Кобак В.Г., Киянов Д.И., Жуковский Д.А., Панков Д.Е.</b> Использование SYMPY для нахождения хроматического числа графа методом Mapy.....	<b>216</b>
<b>Комоцкий Р.И., Болдырихин Н.В.</b> Технология компьютерного зрения на основе нейросетей.....	<b>220</b>

<b>Юхнов В.И., Сосновский А.И., Болдырихин Н.В., Сосновский И.А.</b> Применение искусственного интеллекта для решения задачи обеспечения безопасности информации, передаваемой в сетях.....	<b>223</b>
<b>Кобак В.Г., Киянов Д.И., Швидченко С.А., Ермакова С.Д.</b> Сравнение жадного алгоритма NETWORKX с методом Mapy.....	<b>226</b>
<b>Дубровина А.И.</b> Детекция инцидентов при возникновении сбоя в системе «Умный Дом».....	<b>229</b>
<b>Кутузов М.В.</b> Использование инпейтинга в компьютерной графике: создание реалистичных виртуальных миров.....	<b>233</b>
<b>Мирошниченко Д.В.</b> Обзор существующих систем электронного документооборота и их сравнения с точки зрения эффективности сбора и обработки данных.....	<b>237</b>
<b>Михайлова А.А.</b> Обзор платформ для разработки мобильных приложений на Android.....	<b>241</b>
<b>Ядрец Э.А., Карпенко М.В., Болдырихин Н.В.</b> Искусственный интеллект как ключевой элемент в оценке рисков современных антифрод решений.....	<b>246</b>
<b>Мегрибальян Л.Г., Чикалов А.Н.</b> Сайт для поиска и хранения шаблонов юридических документов.....	<b>249</b>
<b>Ковалева Д.Д., Чикалов А.Н.</b> ВЕБ-приложение для анализа и визуализации финансовых данных бизнеса.....	<b>254</b>

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

<b>Юхнов В.И., Красников А.В.</b> Защищенное клиент-серверное хранилище данных...	<b>261</b>
<b>Пикуль Д.А.</b> Анализ искусственного интеллекта в кибербезопасности.....	<b>268</b>
<b>Байтяков Н.А., Мухачев С.В.</b> Анализ кибератак на объекты критической информационной инфраструктуры и мер по их предотвращению.....	<b>272</b>
<b>Грибанов И.В., Борисов Б.П.</b> Анализ эффективности использования систем защиты от DDOS-атак в корпоративных сетях.....	<b>278</b>
<b>Лян Д.И., Корнилова А.В., Куликова О.В.</b> Методы защиты от кликджекинга.....	<b>285</b>
<b>Никитин А.С., Трухлов И.А., Наговицын Т.А.</b> Моделирование кибератак на базе виртуальной платформы.....	<b>287</b>
<b>Гуральский К.Н., Мухачев С.В.</b> Некоторые угрозы информационной безопасности в случае использования онлайн-банка.....	<b>292</b>
<b>Маршаков Д.В., Кокоулина Ю.Д., Аболмасов А.А., Панасюк А.В.</b> Об интерпретируемости нейросетевых платформ интернета вещей в условиях реализации угроз.....	<b>295</b>
<b>Наливайко А.В., Решетникова О.А.</b> Практика создания систем обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры в электроэнергетике.....	<b>300</b>
<b>Казачанский И.А.</b> Настройка виртуального частного сетевого канала между двумя отделами.....	<b>311</b>
<b>Борисенко А.А., Борисов Б.П., Юхнов В.И.</b> Эффективные средства обеспечения безопасности локальной сети.....	<b>315</b>



---

## ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В СФЕРЕ ОБРАЗОВАНИЯ, ЭКОНОМИКИ И МЕНЕДЖМЕНТА

<b>Головина И.В., Александрова Т.Я.</b> Искусственный интеллект в сфере образования: этический аспект.....	<b>318</b>
<b>Константинова Я.Б., Бадёрная О.А., Кокоулина Ю.Д.</b> Влияние структурных дефектов на степень размытия фазовых переходов в сегнетоэлектриках.....	<b>322</b>
<b>Бинеев Э.А.</b> Особенности зарубежных программ безопасности труда.....	<b>326</b>
<b>Забаренко Н.И., Петрова Ю.А.</b> Философия устойчивости и развитие информационных технологий.....	<b>328</b>
<b>Агаркова Е.В.</b> Анализ данных учебного процесса в образовании.....	<b>331</b>
<b>Докучаев С.А., Костецкая Г.С., Светличная Н.О.</b> Использование нейронных сетей в преподавании гуманитарных дисциплин.....	<b>335</b>
<b>Докучаев С.А., Костецкая Г.С., Конкин Б.Б.</b> Цифровая лекция как эффективный элемент образовательного процесса в техническом вузе.....	<b>336</b>
<b>Калиенко И.В., Назарова О.Ю., Решетникова И.В., Ахмед Абдулмалек Абдулкадер Мохаммед, Каун Д.Е.</b> Экспериментальное исследование и моделирование работы аналого-цифрового преобразователя в программе компьютерного моделирования EWB ELECTRONICS WORKBENCH.....	<b>339</b>
<b>Калиенко И.В., Назарова О.Ю., Решетникова И.В., Ахмед Абдулмалек Абдулкадер Мохаммед, Каун Д.Е.</b> Разработка практического занятия и моделирование работы цифроаналогового преобразователя в учебном процессе обучения специалистов в области телекоммуникаций.....	<b>345</b>
<b>Жуковский Д.А., Ермакова С.Д., Думбасар С.А., Панков Д.Е., Лелик Н.М., Константинова С.В.</b> Физика и психология восприятия цвета при работе над проектом сайта или рекламного продукта.....	<b>351</b>
<b>Жуковский А.Г., Жуковский Д.А., Швидченко С.А., Панков Д.Е., Балановская А.Р.</b> Особенности проведения практических занятий по дисциплинам, требующим изменений программно-аппаратной конфигурации компьютеров в условиях обеспечения информационной безопасности.....	<b>356</b>
<b>Джикия А.А., Маврина В.В., Юхнов В.И.</b> Цифровая экономика в управлении образованием и наукой.....	<b>361</b>
<b>Гаевская Л.А.</b> Значение физической культуры в жизни современного студента.....	<b>365</b>
<b>Шевчук П.С., Решетникова О.А.</b> Повышение эффективности системы межведомственного электронного взаимодействия в контексте реализации концепции «Единого Окна».....	<b>367</b>
<b>Светличная Н.О., Конкин Б.Б., Гаевская Л.А., Коршун А.М.</b> Проблемы внедрения искусственного интеллекта в образование.....	<b>374</b>

---

## CONTENTS

### STATE AND PROSPECTS OF INFOCOMMUNICATION DEVELOPMENT

<b>Golovskoy V.A., Vlokh D.D.</b> Graph model of functioning cognitive radio system.....	11
<b>Borodin A.V., Borodin A.A.</b> Modern pyroelectric receivers of thermal radiation.....	18
<b>Ershov V.V., Rudenko N.V., Kuzenkov E.A., Vasiliev A.E.</b> About the possibility of building a backup power source for a cellular base station based on supercapacitors and batteries.....	21
<b>Eliseev A.V., Zhukovsky A.G., Klimenko M.Ya., Razykova M.R.</b> Analysis of data verification methods of the aviation telecommunication system.....	27
<b>Eliseev A.V., Zhukovsky A.G., Klimenko M.Y., Razykova M.R.</b> Substantiation of the structure of a modern hybrid radio engineering search system for vehicles in distress.....	35
<b>Rudenko N.V., Ershov V.V., Vasiliev A.E.</b> Local electric power system using renewable sources for electric supply autonomous communication objects.....	42
<b>Alferova I.A., Engibaryan I.A., Reshetnikova I.V., Safaryan O.A., Yukhnov V.I.</b> Frequency generation error in digital data transmission channels due to the jitter effect....	46
<b>Alferova I.A., Bezuglov Y.D., Engibaryan I.A., Safaryan O.A., Yukhnov V.I.</b> The effect of frequency instability on the probability of bit error in the transmission of M-CAM signals.....	53
<b>Alferova I.A., Engibaryan I.A., Reshetnikova I.V., Safaryan O.A., Yukhnov V.I.</b> The effect of short-term frequency instability on the signal-to-noise ratio in communication channels.....	60
<b>Phan Tuan Anh</b> Simulation and analysis of the PAPR and ser in the M-APSK modulation	66
<b>Dvornichenko A.S.</b> Basic concepts and ways of using the API.....	79
<b>Kharchenko V.V., Rudy S.V., Vartazarova A.E., Boldyrikhin N.B.</b> Multi-frequency antennas of cellular communication systems.....	83
<b>Karpenko E.A., Korshun A.M.</b> Neural network video analytics as a promising direction of video surveillance development.....	85
<b>Ba M.</b> Development of a shortwave receiver-scanner for detecting sounding CHIRP based on HACKRF one.....	87
<b>Pham Duc Huy, Nguyen Van Cuong, Nikolaev A.V.</b> Radio-electronic means of the military engineering service of the Vietnamese People's Army and prospects for their development.....	94
<b>Lazarenko S.V., Gritsenko V.V., Reshetnikova I.V.</b> Elements of the device for evaluating the parameters of telemetry messages.....	102
<b>Pugachev I.V., Khumaryants S.R., Reshetnikova I.V.</b> Evaluation of the effectiveness of the algorithm for determining parameters analog signal against the background of interference.....	108
<b>Pugachev I.V., Vechter A.K., Reshetnikova O.A.</b> Synthesis of The PLL System from the maximum condition of the generalized power function.....	116
<b>Lazarenko S.V., Lihachev D.A., Penkov A.S., Manin A.A.</b> Analysis of the effectiveness of the combined maximum principle filter when processing information about the state of an unmanned aerial vehicle.....	122
<b>Pugachev I.V., Zubkov A.N., Zehcer V.O., Bezuglov Yu.D.</b> The structure of the digital system for evaluating the parameters of telemetry messages.....	126



<b>Lazarenko S.V., Evtyukho V.M., Engibaryan I.A.</b> Synthesis of an intelligent support filter with a fuzzy strategy for setting parameters in air traffic control automation tasks.....	<b>132</b>
<b>Pugachev I.V., Kamer E.O., Yukhnov V.I.</b> Adaptive multi-mode regulators of automated radio engineering systems.....	<b>138</b>
<b>Kozhaev E.Z., Ukhov P.E.</b> Remote sensing of the earth. Analysis of ways to obtain information materials	<b>145</b>

## INFORMATION TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE SYSTEMS

<b>Fatkhulin T.D., Kozhanov M.S.</b> Problems of storing and managing the results of static analysis in the life cycle of secure software development and ways to solve them.....	<b>152</b>
<b>Fatkhulin T.D., Klimov N.Yu., Gezhin S.A.</b> Analysis of neural network techniques for text generation.....	<b>162</b>
<b>Fatkhulin T.D., Lushin E.A.</b> Analysis of the development of automatic code generation for WEB-services.....	<b>169</b>
<b>Fatkhulin T.D., Fatkhulina G.G., Mentus M.V.</b> Development of a method for forming a prompt to a neural network for the purpose of generating images based on the requirements of computational linguistics.....	<b>175</b>
<b>Frolova M.M., Lobzenko P.V.</b> A mobile device on a neural network for building a terrain map in a graphical interface.....	<b>184</b>
<b>Remigin P.I., Lobzenko P.V.</b> Network application for technical support service.....	<b>188</b>
<b>Puzyrnaya L.V., Lobzenko P.V.</b> Optimization of an enterprise computer network using the virtualization method.....	<b>192</b>
<b>Kozhanov A.B., Lobzenko P.V.</b> Combined CRM of the security department.....	<b>196</b>
<b>Zaitsev I.O., Lobzenko P.V.</b> Car service network database.....	<b>199</b>
<b>Golovinov S.E., Lobzenko P.V.</b> Auto-storing new material when learning.....	<b>202</b>
<b>Gertsovsky N.Yu., Lobzenko P.V.</b> Distributed training system server.....	<b>204</b>
<b>Zaytsev E.A., Ustimenko D.L.</b> Prospects for the use of artificial intelligence in the electric power industry.....	<b>207</b>
<b>Leonov M.P., Ustimenko D.L.</b> Ethical aspects of artificial intelligence.....	<b>210</b>
<b>Naydenova J.I., Reshetnikova I.V., Safaryan O.A.</b> Construction of an expert system for assessing the crypto strength of The RSA encryption algorithm.....	<b>213</b>
<b>Kobak V.G., Kiyanov D.I., Zhukovsky D.A., Pankov D.E.</b> Using SYMPY to find the chromatic number of a graph using The Magoo method.....	<b>216</b>
<b>Komotskiy R.I., Boldyrikhin N.B.</b> Computer vision technology based on neural networks.....	<b>220</b>
<b>Yukhnov V.I., Sosnovskiy A.I., Boldyrikhin N.V., Sosnovskiy I.A.</b> The use of artificial intelligence to solve the problem of ensuring the security of information transmitted in networks.....	<b>223</b>
<b>Kobak V.G., Kiyanov D.I., Shvidchenko S.A., Ermakova S.D.</b> The comparison of the greedy NETWORKX algorithm with The Magoo method.....	<b>226</b>
<b>Dubrovina A.I.</b> Detection of incidents when failures occur in The Smart Home system....	<b>229</b>
<b>Kutuzov M.V.</b> Using inpainting in computer graphics: creating realistic virtual worlds.....	<b>233</b>
<b>Miroshnichenko D.V.</b> Overview of existing electronic document management systems and their comparison in terms of data collection and processing efficiency.....	<b>237</b>

<b>Mikhailova A.A.</b> Review of platforms for the development of mobile applications on The Android.....	<b>241</b>
<b>Yadrets E.A., Karpenko M.V., Boldyrikhin N.B.</b> Artificial intelligence as a key element in risk assessment of modern antifraud solutions.....	<b>246</b>
<b>Megribanyan L.G., Chikalov A.N.</b> Website for searching and storing templates legal documents.....	<b>249</b>
<b>Kovaleva D.D., Chikalov A.N.</b> WEB-application for analysis and visualization of business financial data.....	<b>254</b>

## INFORMATION SECURITY

<b>Yukhnov V.I., Krasnikov A.V.</b> Secured client-server data storage.....	<b>261</b>
<b>Pikul D.A.</b> Analysis of artificial intelligence in cybersecurity.....	<b>268</b>
<b>Baytyakov N.A., Mukhachev S.V.</b> Analysis of cyber attacks on critical information infrastructure facilities and measures to prevent them.....	<b>272</b>
<b>Gribanov I.V., Borisov B.P.</b> Analysis of the effectiveness of DDOS protection systems in corporate networks.....	<b>279</b>
<b>Layn D.I., Kornilova A.V., Kulikova O.V.</b> Methods of protection against clickjacking... ..	<b>285</b>
<b>Nikitin A.S., Trukhlov I.A., Nagovitsyn T.A.</b> Simulation of cyber attacks based on a virtual platform.....	<b>288</b>
<b>Guralsky K.N., Mukhachev S.V.</b> Some threats to information security in the case of using an online bank.....	<b>292</b>
<b>Marshakov D.V., Kokoulina Yu.D., Abolmasov A.A., Panasyuk A.V.</b> About the interpretability of neural network platforms of the internet of things in the context of threats.....	<b>296</b>
<b>Nalivaiko A.V., Reshetnikova O.A.</b> The practice of creating information security systems of critical information infrastructure in the electric power industry.....	<b>300</b>
<b>Kazachansky I.A.</b> Setting up a virtual private network channel between the two departments.....	<b>311</b>
<b>Borisenko A.A., Borisov B.P., Yukhnov V.I.</b> Effective means of securing the local network.....	<b>315</b>

## INFORMATION AND COMMUNICATION TECHNOLOGY IN EDUCATION, ECONOMICS AND MANAGEMENT

<b>Golovina I.V., Alexandrova T.Ya.</b> Artificial intelligence in education: ethical aspect....	<b>318</b>
<b>Konstantinova Ya.B., Badernaya O.A., Kokoulina U.D.</b> Influence of structural defects on the degree of blurring of phase transitions in ferroelectric.....	<b>323</b>
<b>Bineev E.A.</b> Features of foreign labor safety programs.....	<b>326</b>
<b>Zabarenko N.I., Petrova Yu.A.</b> The philosophy of sustainable development and information technologies.....	<b>328</b>
<b>Agarkova E.V.</b> Data analysis of the educational process in education.....	<b>331</b>



---

<b>Dokuchaev S.A., Kostetskaya G.S., Svetlichnaya N.O.</b> Using neural networks in teaching humanities subjects.....	<b>335</b>
<b>Dokuchaev S.A., Kostetskaya G.S., Konkin B.B.</b> Digital educational streaming portal as an effective way to form digital competencies in students.....	<b>337</b>
<b>Kaliyenko I.V., Nazarova O.YU., Reshetnikova I.V., Akhmed Abdulmalek Abdulkader Mokhammed, Kaun D.Ye.</b> Experimental research and simulation of the operation of analog-digital converter in the computer simulation program EWB ELECTRONICS WORKBENCH.....	<b>339</b>
<b>Kaliyenko I.V., Nazarova O.YU., Reshetnikova I.V., Akhmed Abdulmalek Abdulkader Mokhammed, Kaun D.Ye.</b> Development of a practical lesson and simulation of the operation of a digital to analog converter in the educational process of training specialists in the field of telecommunications.....	<b>346</b>
<b>Zhukovsky D.A., Ermakova S.D., Dumbasar S.A., Pankov D.E., Lelik N.M., Konstantinova S.V.</b> Physics and psychology of color perception when working on a website or advertising product project.....	<b>351</b>
<b>Zhukovsky A.G., Zhukovsky D.A., Shvidchenko S.A., Pankov D.E., Balanovskaya A.R.</b> Features of conducting practical classes in disciplines requiring changes in the software and hardware configuration of computers in the conditions of information security.....	<b>356</b>
<b>Dzhikiya A.A., Mavrina V.V., Yukhnov V.I.</b> Digital economy in education and science management.....	<b>361</b>
<b>Gayevskaya L.A.</b> The importance of physical culture in life a modern student.....	<b>365</b>
<b>Shevchuk P.S., Reshetnikova O.A.</b> Improving the efficiency of the system of interdepartmental electronic interaction in the context of the implementation of The "Single Window" concept.....	<b>367</b>
<b>Svetlichnaya N.O., Konkin B.B., Gayevskaya L.A., Korshun A.M.</b> Problems of introducing artificial intelligence in the education.....	<b>374</b>

---

## СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИЙ

## STATE AND PROSPECTS OF INFOCOMMUNICATION DEVELOPMENT

В.А. Головской, Д.Д. Влох

### ГРАФОВАЯ МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ КОГНИТИВНОЙ РАДИОСИСТЕМЫ

Краснодарское высшее военное училище им. генерала армии С.М. Штеменко,  
Краснодар, Россия

Ключевые слова: когнитивное радио, граф, модель, множество Парето, оптимальность, весовая функция.

В работе представлена и обоснована разработанная модель функционирования когнитивной радиосистемы, формализованная с помощью ориентированного взвешенного мультиграфа. Модель позволяет формулировать требования к когнитивной радиосистеме и оценивать её характеристики с помощью аппарата теории графов, а также рассматривать различные задачи при исследованиях когнитивных радиосистем, как экземпляры известных массовых задач на графах.

V.A. Golovskoy, D.D. Vlokh

### GRAPH MODEL OF FUNCTIONING COGNITIVE RADIO SYSTEM

Krasnodar Higher Military School named after S.M. Shtemenko, Krasnodar, Russia

Keywords: cognitive radio, graph, model, Pareto set, optimality, weight function.

The paper presents and substantiates the developed model of the functioning of a cognitive radio system, formalized with the help of an oriented weighted multigraph. The model makes it possible to formulate requirements for a cognitive radio system and evaluate its characteristics using the graph theory apparatus, as well as to consider various tasks in the study of cognitive radio systems as instances of well-known mass graph problems.

Телекоммуникации, как и другие технологические отрасли экономики, в настоящее время являются объектом рассмотрения с точки зрения их интеллектуализации. При этом предполагается, что интеллектуализация обеспечит повышение эффективности функционирования телекоммуникационных систем [1]. Одним из подходов к интеллектуализации телекоммуникационных технологий является концепция когнитивного радио [2].

Под когнитивной радиосистемой (КРС) в настоящее время принято понимать систему, использующую технологию [2], обеспечивающую наличие у КРС интеллектуальных способностей  $C_p$ ,  $p = \overline{1, 3}$ , приведенных на рисунке 1.

Исследования в области создания КРС проводятся во многих направлениях [3-13], при этом предметом рассмотрения настоящей работы является основанная на знаниях коррекция эксплуатационных параметров КРС для достижения поставленных перед ней целей, что соответствует способности  $C_2$  на рисунке 1. Среди множества коррелирующих с рассматриваемым авторами подходом к определению знаний [14-18] наиболее близким



определением термина «знания» представляется следующее: эмпирические знания – это знания об априорном множестве потенциально возможных причин-кандидатов и/или о правдоподобных причинно-следственных связях [18]. Цель работы – построение описательной модели функционирования когнитивной радиосистемы.

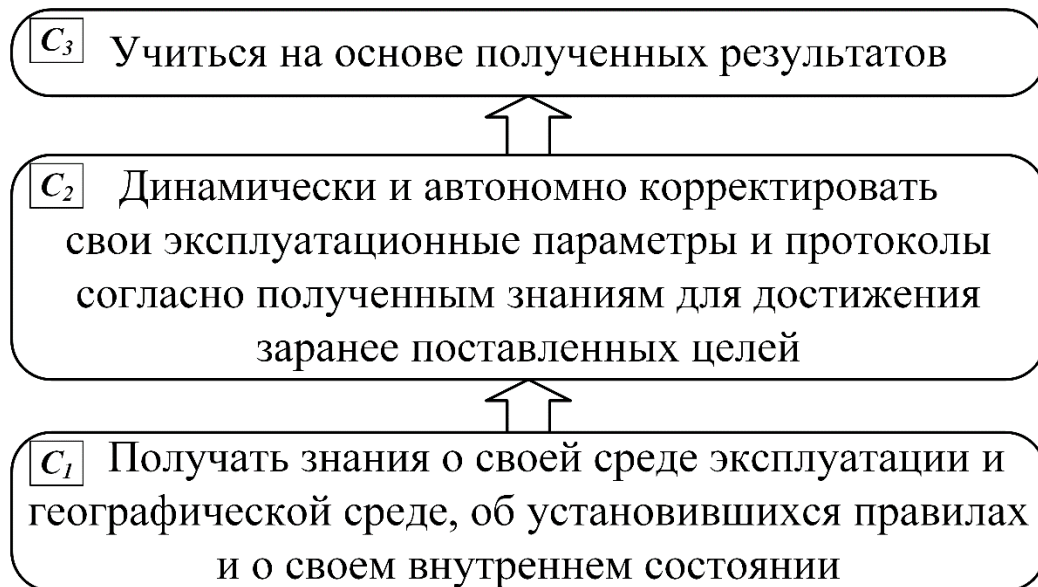


Рисунок 1. Иерархия способностей когнитивной радиосистемы

#### Основная часть.

В работах [11-13] был развит предложенный в статье [10] подход к описанию функционирования КРС с использованием множества образов  $T = \{T_k\}, k = \overline{1, N_K}$ , каждый из которых описывает состояние телекоммуникационного оборудования абонента КРС в фиксированный момент времени. Указанное множество  $T$  формально можно описать декартовым произведением множеств характеристик телекоммуникационного оборудования абонента КРС

$$T = \prod_{i=1}^{N_l} M_i = \left\{ (m_{1,j}, m_{2,v}, \dots, m_{N_l,l}) / m_{1,j} \in M_1, m_{2,v} \in M_2, \dots, m_{N_l,l} \in M_{N_l} \right\}, \quad (1)$$

где  $M_i$  – конечное множество, задающее набор возможных значений  $i$ -й характеристики телекоммуникационного оборудования КРС,  $i = \overline{1, N_l}$ . В фиксированный момент времени конкретный образ абонента КРС  $T_k \in T$  в соответствии с (1) при фиксированных  $k, j, v$  и  $h$  может быть описан, например, кортежем  $T_k = \langle f_l, c_v, P_h \rangle$ , где  $f_l$  –  $l$ -е значение рабочей частоты,  $c_v$  –  $v$ -й тип сигнально-кодовой конструкции,  $P_h$  –  $h$ -е значение мощности излучения.

Исходя из принятого подхода к описанию состояний КРС необходимо построить математическую модель, описывающую переход КРС от образа  $T_k$  к образу  $T_j$  во множестве (1).

В настоящее время достаточно наглядным и практичным является использование для описания энергетической эффективности сигнально-кодовых конструкций водопадоподобных графиков, подобных приведенному на рисунке 2, иллюстрирующих зависимость коэффициента битовых ошибок (BER) от нормированного отношения сигнал/шум ( $E_b/N_0$ ) в канале связи.

Анализ рисунка 2 позволяет оценивать выигрыш в помехоустойчивости (BER) при фиксированном значении отношения энергии бита к спектральной плотности мощности

шума ( $E_b/N_0$ ) или выигрыш  $E_b/N_0$  при фиксированном требуемом значении (BER) одних сигнально-кодовых конструкций относительно других.

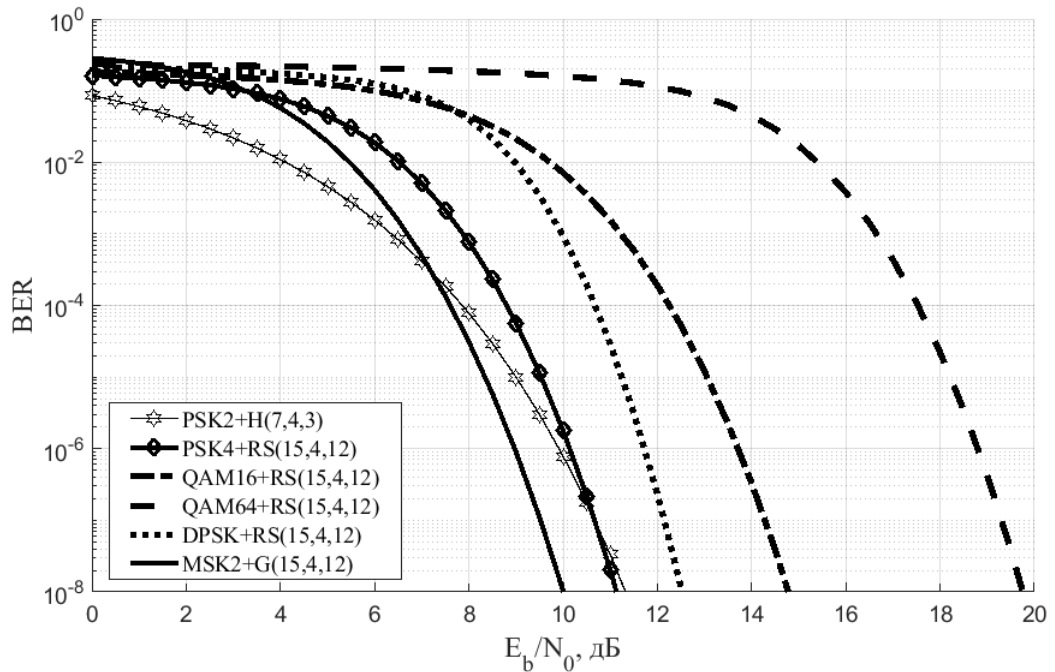


Рисунок 2. Данные об эффективности сигнально-кодовых конструкций

Однако такой подход предполагает наличие фиксированных условий использования сигнально-кодовых конструкций, что не всегда реализуется на практике. Современные условия функционирования динамично меняются, и выигрыш от использования тех или иных сигнально-кодовых конструкций становится не очевидным ввиду наличия дополнительных требований и ограничений. Подобная ситуация может быть описана помеченным ориентированным графом на рисунке 3. Использование графов является традиционным подходом при моделировании в различных телекоммуникационных приложениях [19-23].

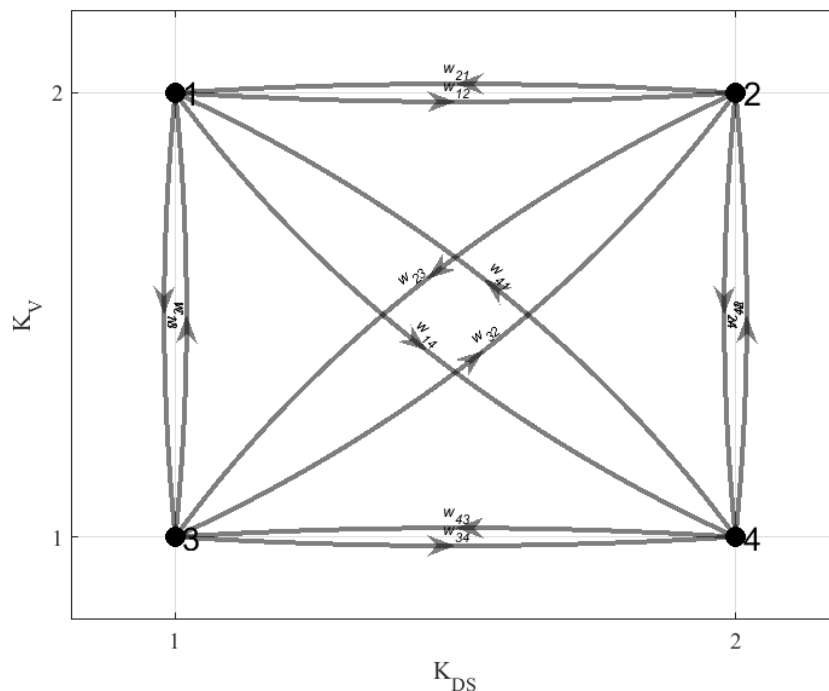


Рисунок 3. Граф состояний КРС

На рисунке 3 при построении графа  $G$  поставлена в соответствие каждому образу  $T_k$  из множества (1) вершина  $V_k \in G$ , а возможности системы переходить из состояния, соответствующего вершине  $V_k$ , в состояние  $V_j$  – дуга  $E_{kj} \in G$ . Граф для наглядности помещен в систему координат, характеризующих качественно относительную эффективность по показателю скорость –  $K_V$  и помехоустойчивость –  $K_{DR}$ , которые будут достигнуты при переходе от из состояния  $V_k$  в состояние  $V_j$ . Каждое ребро  $G$  имеет  $r$ -мерный вектор весов,  $r = 2$ , вида

$$W_{kj} = (w_1, w_2)_{kj}, \quad (2)$$

где  $w_1, w_2$  – целые положительные числа, качественно характеризующие выигрыш по скорости передачи информации и помехоустойчивости приема соответственно при переходе от вершины  $V_k$  к вершине  $V_j$ .

При такой постановке задача нахождения приоритетной для текущего момента времени сигнально-кодовой конструкции достаточно легко решается, однако в современных условиях на функционирование абонентов накладываются такие ограничения, как энергетическая эффективность [24], обеспечение электромагнитной совместимости с другими радиосистемами [25] и другие. Тогда для оценивания эффективности индуктивно можно перейти от двумерной системы координат к  $n$ -мерной, при этом также будет увеличена размерность вектора (2).

Построим 3-взвешенный граф  $G_{CRS}$  в предположении, что существует формирующее векторы

$$W_{kj} = (w_1, w_2, w_3)_{kj}, \quad (3)$$

семейство весовых функций

$$\begin{cases} g_{1,i}(D_R, D_{ENW}) = w_{1,i}, \\ g_{2,i}(D_R, D_{ENW}) = w_{2,i}, \\ g_{3,i}(D_R, D_{ENW}) = w_{3,i}, \end{cases} \quad (4)$$

где  $D_R$  – данные о состоянии ресурсов терминала абонента КРС,  $D_{enw}$  – описание состояния среды, учитывающее параметры распространения радиоволн, радиоэлектронную обстановку и другие. Смысл весов  $w_1$  и  $w_2$  остается тем же, что и в (2), а вес  $w_{3,i}$  характеризует выигрыш по показателю энергоэффективность ( $K_{EE}$ ) при переходе от вершины  $V_k$  к вершине  $V_j$ .

Интересующий нас ориентированный помеченный мультиграф с конечными множествами вершин  $V$  и ребер  $E$  и набором векторов вида (3)

$$G_{CRS} = (V, E, W_{ij}) \quad (5)$$

приведен на рисунке 4, где для наглядности показаны только ребра  $E_{12}, E_{13}, E_{15}, E_{37}, E_{74}, E_{56}, E_{86}, E_{82}$  в предположении, что в текущем состоянии КРС возможны только соответствующие эти ребрам переходы. Указанный граф вследствие размерности вектора (3) называется 3-взвешенным [21]. В целях обеспечения наилучшей наглядности конкретные значения весов приведены только для ребер  $E_{12}, E_{13}, E_{15}$ .

Необходимо отметить, что значения любого  $W_{kj}$  не обязательно являются постоянными во времени, что объясняется изменением радиоэлектронной обстановки ввиду параметрической адаптации сторонних радиосистем, движения абонентов, периодичности работы некоторых радиосистем и другими факторами.

Для пояснения предлагаемой графовой модели рассмотрим нахождение КРС в  $i$ -й

момент времени в состоянии, соответствующем вершине  $V_1$  на рисунке 4. Переход к вершине  $V_5$  характеризуется соответствующим вектором весов  $W_{1,5} = (2,1,2)$ , к вершине  $V_2$  – вектором  $W_{1,2} = (2,2,1)$ , к вершине  $V_3$  – вектором  $W_{1,3} = (1,1,1)$ . С учетом принятого качественного подхода сравнения и выбранной бинарной шкалы возможно следующее сравнение векторов  $W_{1,5} = (2,1,2)$  и  $W_{1,2} = (2,2,1)$ : при переходе к вершине  $V_5$  будет повышен качественный показатель  $K_{EE}$  по сравнению с  $V_2$ , а при альтернативном переходе к  $V_2$  будет повышен качественный показатель  $K_{DR}$  по сравнению с  $V_5$ . С точки зрения скорости передачи информации выигрыша не будет.

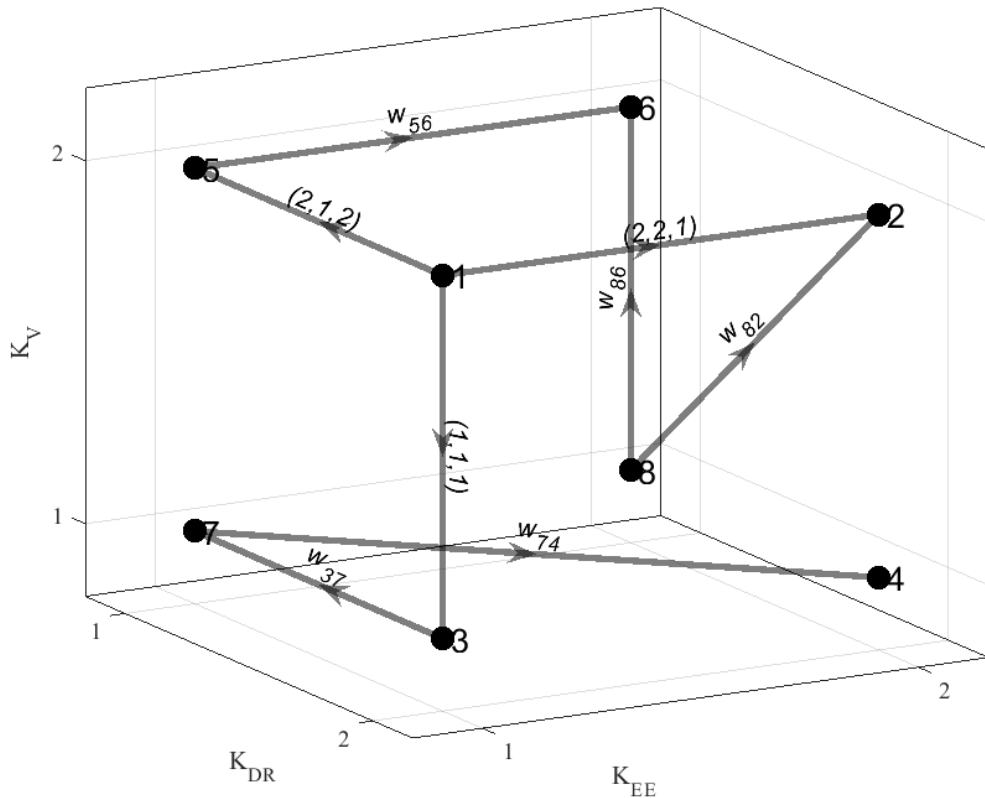


Рисунок 4. Граф  $G_{CRS}$

С позиций теории важности критериев [26] мы можем сказать в этом случае, что  $W_{1,2} = (2,2,1)$  предпочтительнее чем  $W_{1,3} = (1,1,1)$ , т.е. существует лексикографическое отношение предпочтения  $P^0$  между векторами  $W_{1,2}$  и  $W_{1,3}$ , т.е.  $W_{1,2} P^0 W_{1,3}$  и вершина  $V_3$  является доминируемым вариантом, т.е.  $V_2 P_0 V_3$ , где  $P_0$  – лексикографическое отношение предпочтения между альтернативами. В этом случае вершина  $V_2$  и  $V_5$  являются недоминируемыми вариантами или оптимальными по Эджворту-Парето, так как не существует инцидентного вершине  $V_1$  ребра  $V_x$ , вектор весов которого бы обеспечивал  $W_{1,x} P^0 W_{1,2}$  или  $W_{1,x} P^0 W_{1,5}$ . Векторы же  $W_{1,2} = (2,2,1)$  и  $W_{1,5} = (2,1,2)$  являются несравнимыми по отношению  $P^0$ .

Далее рассмотрим влияние важности критериев на сравнение векторных оценок вариантов. Допустим дана информация о важности критериев следующего вида:

$$\Omega = \{1 \succ 2, 2 \succ 3\}, \tag{6}$$

где  $i \succ j$  обозначает приоритет критерия  $i$  над  $j$ .

Набор (6) может быть интерпретирован, как то, что акцент делается на скорости



---

передачи информации и потом на помехоустойчивости. Проведем анализ многокритериальной задачи с учетом данных множества  $\Omega$ , т.е. сравним варианты – векторы  $W_{1,2} = (2, 2, 1)$  и  $W_{1,5} = (2, 1, 2)$ . Анализ этой пары позволяет увидеть предпочтительность варианта  $W_{1,2}$ , т.е. имеет место соотношение  $W_{1,2} P_{\Omega} W_{1,5}$ .

Предложенный подход к описанию условий параметрической адаптации КРС может быть развит путем формирования  $r$ -критериальной оптимизационной задачи с  $r > 3$  и построения допустимых подграфов графа  $G_{CRS}$ , как показано в работе [21]. Допустимые подграфы будут отличаться используемыми для их формирования соответствующими множествами  $\Omega$ .

### **Заключение.**

Предложенная графовая модель позволяет рассматривать различные задачи при исследованиях КРС как экземпляры известных массовых задач на графах, формировать требования к КРС и оценивать различные характеристики этих систем с использованием терминологии графов, а также строить математические модели проблемных ситуаций.

В качестве направлений развития исследований видится доказательство вычислимости семейства функций (4), рассмотрение графа (5) как автомата и описание его в условиях воздействия непреднамеренных помех как случайного графа.

### **СПИСОК ЛИТЕРАТУРЫ**

1. *Chafii M., Bariah L., Muhaidat S., Debbah M.* Twelve Scientific Challenges for 6G: Rethinking the Foundations of Communications Theory. 7 Sep 2022, revised 8 Feb 2023. URL: <https://doi.org/10.48550/arXiv.2207.01843> (дата обращения: 11.10.2023).
2. Report ITU-R SM.2152. Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS). URL: [https://www.itu.int/dms\\_pub/itu-r/opb/rep/R-REP-SM.2152-2009-PDF-e.pdf](https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2152-2009-PDF-e.pdf) (дата обращения: 11.10.2023).
3. *Голубинский А.Н.* Применение искусственной нейронной сети в виде многослойного персептрона для формирования рейтинга частотных каналов в системе когнитивного радио. // Теория и техника радиосвязи. – 2020, № 2, с. 64-73.
4. *Eappen G., Shankar T.* Hybrid PSO-GSA for energy efficient spectrum sensing in cognitive radio network // Physical Communication. – 2020, vol. 40. URL: <https://doi.org/10.1016/j.phycom.2020.101091> (дата обращения: 24.09.2023).
5. *Kalpna Devi M., Umamaheswari K.* Modified artificial bee colony with firefly algorithm based spectrum handoff in cognitive radio network. // International Journal of Intelligent Network. – 2020, vol. 1, p. 67–75. URL: <https://doi.org/10.1016/j.ijin.2020.07.002> (дата обращения: 25.09.2022).
6. *Giral D., Hernández C., Salgado C.* Spectral decision in cognitive radio networks based on deep learning. // Expert Systems with Applications. – 2021, vol. 180. URL: <https://doi.org/10.1016/j.eswa.2021.115080> (дата обращения: 27.02.2023).
7. *Адамовский Е.Р., Чертков В.М., Богуш Р.П.* Модель формирования карты радиосреды для когнитивной системы связи на базе сотовой сети LTE. // Компьютерные исследования и моделирование. – 2022, т. 14, № 1, с. 127-146.
8. *Peter G., Livin J.* Hybrid optimization algorithm based optimal resource allocation for cooperative cognitive radio network. // Array. – 2021, № 12. URL: <https://www.sciencedirect.com/science/article/pii/S2590005621000400> (дата обращения: 29.09.2023).
9. *Alnabelsi S.H., Salameh H.B., Saifan R.R., Darabkh K.A.* A multi-layer hyper-graph routing with jamming-awareness for improved throughput in full-duplex cognitive radio networks. // Journal of King Saud University - Computer and Information Sciences. – 2022. URL: <https://doi.org/10.1016/j.jksuci.2022.01.003>. (дата обращения: 29.09.2023).

10. Головской В.А., Филинов В.С. Предложения по созданию когнитивных систем передачи данных для робототехнических комплексов. // Т-Comm: Телекоммуникации и транспорт. – 2019, т. 13, № 9, с. 22-29.
11. Головской В.А. О моделях в исследованиях когнитивных радиосистем. // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2022, № 2, с. 8-11.
12. Головской В.А. О разрешимости и перечислимости множеств в задачах когнитивного радио. // Прикладная математика и информатика в современном мире / Материалы Всероссийской научно-практической конференции, посвященной 50-летию начала подготовки специалистов в области программирования и прикладной математики на Кубани, Краснодар, 20–23 сентября 2022 года. – Краснодар: ФГБУ «Российское энергетическое агентство» Минэнерго России Краснодарский ЦНТИ-филиал ФГБУ «РЭА» Минэнерго России, 2022. – С. 124-129.
13. Головской В.А. О проблеме ограниченности при исследованиях когнитивных радиосистем. // Радиолокация, навигация, связь / Сборник трудов ХХІХ Международной научно-технической конференции, посвященной 70-летию кафедры радиопизики ВГУ. Воронеж, 2023. – т.5. С. 283-287.
14. Граничин О.Н. Обратные связи, усреднение и рандомизация в управлении и извлечении знаний. // Стохастическая оптимизация в информатике. – 2012, т. 8, № 2, с.3-48.
15. Лекторский В.А., Васильев С.Н., Макаров В.Л., Хабриева Т.Я., Кокошин А.А., Ушаков Д.В., Валуева Е.А., Дубровский Д.И., Черниговская Т.В., Семёнов А.Л., Зискин К.Е., Любимов А.П., Целищев В.В., Алексеев А.Ю. Человек и системы искусственного интеллекта / Под ред. акад. РАН В.А. Лекторского. – СПб.: Издательство «Юридический центр», 2022. 328 с.
16. Каляев И.А. Как измерить искусственный интеллект? // Искусственный интеллект и принятие решений. – 2023. № 1. С. 3-11.
17. Зацман И.М. Данные, информация и знание в научной парадигме информатики. // Информатика и её применения. – 2023, №1, с.116-125.
18. Васильев С.Н. Метод абдуктивного вывода в задачах объяснения наблюдаемого. // Известия Российской академии наук. Теория и системы управления. – 2021, № 1, с.160-168.
19. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. СПб.: Наукоемкие технологии. 2020. 337 с.
20. Солдатенко А.А. Алгоритм оптимальной маршрутизации в мультисервисных телекоммуникационных сетях. // Прикладная дискретная математика. Приложение. – 2018, № 11, с. 122-127.
21. Визинг В.Г. Многокритериальные задачи на графах с максиминным критерием. // Дискретный анализ и исследование операций. – 2011, т. 18, № 5, с. 3-10.
22. Соколова О.Д. Графовые модели для задач функционирования современных сетей передачи данных. // Проблемы информатики. – 2014, № 4(25), с. 61-68.
23. Левин М.Ш. Комбинаторная оптимизация при построении конфигураций систем // Информационные процессы. – 2008, т. 8, № 4, с. 256-300.
24. Манаенко С.С., Дворников С.В., Пшеничников А.В. Теоретические аспекты формирования сигнальных конструкций сложной структуры. Информатика и автоматизация. – 2022, т. 21, № 1, с. 68-94.
25. Grychkin S.E., Stroganova E.P. «Smart City»: Electromagnetic Compatibility Problem. // WECOMF / 2023 Wave Electronics and its Application in Information and Telecommunication Systems, St. Petersburg, 2023. – p. 1-5.
26. Подиновский В.В. Идеи и методы теории важности критериев в многокритериальных задачах принятия решений. – М.: Наука, 2019. 103 с.

## СОВРЕМЕННЫЕ ПИРОЭЛЕКТРИЧЕСКИЕ ПРИЕМНИКИ ТЕПЛООВОГО ИЗЛУЧЕНИЯ

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: пирозлектрический эффект, поляризованность, пирозлектрические приемники, пирозлектрики, тонкие пленки.

В статье названы два основных вида неохлаждаемых теплоприемников: болометрические и пирозлектрические. Перечислены преимущества применения пироприемников. Названы разновидности пирозлектрических материалов: монокристаллы, керамика и тонкие пленки. Перспективным является использование матриц из пирозлектрических материалов в современных приемниках теплового излучения. Рассмотрены наиболее перспективные направления применения пирозлектрических приемников.

A.V. Borodin, A.A. Borodin

## MODERN PYROELECTRIC RECEIVERS OF THERMAL RADIATION

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: pyroelectric effect, polarization, pyroelectric receivers, pyroelectric, thin films.

The article names two main types of uncooled heat sinks: bolometric and pyroelectric. The advantages of using pyro receivers are listed. Varieties of pyroelectric materials are named: single crystals, ceramics and thin films. The use of matrices made of pyroelectric materials in modern thermal radiation receivers is promising. The most promising areas of application of pyroelectric receivers are considered.

Современные неохлаждаемые приемники инфракрасного излучения оказались лучше других термоприемников по высокой эффективности обнаружения источника излучения, надежности, быстродействию, а также малому энергопотреблению. Приемники, использующие пирозлектрический эффект используются в промышленной термографии, в научном приборостроении, военной технике, медицине и т. д. Измерение малых температурных приращений является основной задачей измерительных устройств, использующих промежуточное тепловое преобразование. В связи с этим значительный интерес представляют термометры на основе пирозлектриков, которые при пороговой чувствительности не более 10-7оС реагируют только на изменение температуры.

Для использования максимальной детектирующей способности пирозлектриков на низких частотах можно еще больше уменьшить полосу частот, применяя двумерную матрицу приемников, при этом каждый приемник соответствует одному элементу изображения. Поскольку многие из пирозлектрических материалов являются достаточно хорошими электрическими изоляторами, конструкция такой матрицы значительно упрощается при использовании одной большой пластины материала, на которую проецируется инфракрасное изображение. Если на переднюю поверхность пластины нанесен электрод, то распределение пирозлектрических зарядов на тыльной поверхности воспроизводит инфракрасное изображение. Для считывания распределения зарядов вместо системы электродов можно использовать любой метод, чувствительный к распределению

---

зарядов или электрического поля на поверхности пластины. В последние годы ведется разработка и создание пироэлектрических матриц размерностью более 1500x1500.

Пироэлектрические приемники обладают принципиальными преимуществами перед другими типами тепловых приемников. Эти преимущества обусловлены электростатической природой этих преобразователей генераторного типа. Пироэлектрические приемники могут работать без источников питания, они оказываются более стабильными, чем болометры, в которых сопротивление зависит от абсолютного значения температуры, и менее инерционными, чем вакуумные радиационные термоэлементы и оптико-акустические приёмники излучения. Спектральный диапазон пироэлектрических приемников был распространен как до рентгеновского и  $\gamma$ -излучения, так и до сантиметровых волн.

Пироэлектрические теплотрические преобразователи находят применение в тех областях, где тепловое преобразование является эффективным средством получения информации о физических, химических и биологических процессах или параметрах вещества. В настоящее время пироэлектрические теплотрические преобразователи применяются для измерения всех параметров, характеризующих тепловую цепь: температуры (пиротермометры), теплоемкости и теплопроводности (калориметры), изменения теплосодержания (катарометры). Эти немногие параметры тепловой цепи служат универсальной мерой многочисленных первичных физико-химических величин, непосредственно участвующих в исследуемых процессах. Пироэлектрические термометры являются основой одноименных калориметров и схем измерения теплопроводности. При малых сопротивлениях нагрузки выходное напряжение пиротермометра пропорционально скорости изменения температуры в интервале ее изменения, где пироэлектрический коэффициент можно считать постоянным. Высокая чувствительность пиротермометров в таком режиме позволяет регистрировать малые скорости изменения температуры, практически недостижимые для других термотрических средств. [1]

Полярные кристаллы спонтанно поляризованы при отсутствии внешних электрических полей и обладают отличным от нуля электрическим моментом в единице объема. При неизменных внешних условиях спонтанную поляризацию нельзя обнаружить по зарядам на поверхности кристалла, поскольку они компенсируются свободными зарядами за счет объёмной или поверхностной проводимости кристалла или из внешней среды. Но так как спонтанная поляризация зависит от температуры, её изменение может быть обнаружено при нагреве или охлаждении кристалла на гранях, перпендикулярных к особенной полярной оси. Наблюдаемый при этом эффект называется пироэлектрическим, а полярные кристаллы, которым он свойственен, - пироэлектрическими. Монокристаллы обладают максимальными пироэлектрическими свойствами. Формирование свойств происходит на стадии роста кристаллов, после чего свойства остаются неизменными и нечувствительными к различным воздействиям при эксплуатации.

Пироэлектрическую керамику изготовить легче, чем монокристаллы соответствующего состава. Во многих случаях она обладает пироэлектрическими свойствами, очень близкими к свойствам монокристаллов можно приготовить обширный ряд керамических составов и подобрать свойства материалов для различных применений. Так были изучены пироэлектрические и диэлектрические свойства бинарных систем твердых растворов на основе ниобата натрия:  $(1-x)\text{NaNbO}_3 - x\text{LiNbO}_3$ ,  $(1-x)\text{NaNbO}_3 - x\text{KNbO}_3$ ,  $(1-x)\text{NaNbO}_3 - x\text{PbTiO}_3$  в широком диапазоне параметра  $x$  с целью определения материалов, перспективных для практического использования в качестве пироэлектрических преобразователей различного предназначения. [2]

Разрабатываются тонкие пироактивные плёнки толщиной около 1 мкм и менее с сегнетоэлектрическими свойствами. При нагреве или охлаждении пироэлектрические полимерные пленки генерируют ток, пропорциональный скорости изменения температуры. Получение поляризованного состояния у полимеров и композитов является более сложным процессом, чем у классических сегнетоэлектриков, и их пироактивность более низкая, чем



---

у лучших монокристаллов. Но возможность получения рабочих тел больших размеров с управляемой чувствительностью, а также технологическая простота и более низкая стоимость делают эти материалы весьма перспективными. С помощью полимерных пленок могут быть разработаны приемники излучения с очень большими размерами приемной площади для создания многофункциональных пирозлектрических устройств. Наиболее активными пирозлектриками являются соединения поливинилиденфторид и поливинилфторид. Для получения устойчивого состояния пленки раскатываются до 5 – 15 мкм, после чего поляризуются при температуре 120оС – 140оС в поле  $\approx 106$  В·см<sup>-1</sup> и охлаждаются под полем. [3] В последние годы начали широко применяться микроэлектронные матричные пировидиконы. Такие измерительные приемники могут состоять из большого количества пирозэлементов, образующих пирозлектрическую матрицу (103–105 элементов). Матричные устройства позволяют исследовать пространственное распределение излучения. Разработаны пирозлектрические матрицы, в которых от 10 до 80 тысяч сверхминиатюрных пирозэлементов размещены на одной кремниевой пластине процессора. Каждый элементарный пирозэлемент соединен со входом интегрального транзистора так, что пластинка 1,5x1,5 см<sup>2</sup> представляет собой твердотельный инфракрасный видикон, приемник инфракрасного излучения. Такие неохлаждаемые приемники обладают очень большой чувствительностью, возрастающей как корень квадратный от числа элементов, и способны различать температурный контраст 0,1 – 0,2 градуса.

#### СПИСОК ЛИТЕРАТУРЫ

1. Бородин А.В., Захаров Ю.Н., Резниченко Л.А., Наскалова О.В. Новые перспективные экологически чистые сегнетокерамические материалы для пирозлектрических термометров. - Известия ТРТУ. 2002. № 5 (28). с.123-124.
2. Бородин А.В., Бородина А.А. Перспективные направления использования пирозлектрических материалов. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2021. № 1. с. 22-24.
3. Бородин А.В. Преимущества использования пирозлектрических приемников. «Фундаментальные проблемы радиоэлектронного приборостроения», 2016 т.16 №4 с.19-21.

**В.В. Ершов<sup>1</sup>, Н.В. Руденко<sup>2</sup>, Е.А. Кузенков<sup>1</sup>, А.Э. Васильев<sup>2</sup>**

#### **О ВОЗМОЖНОСТИ ПОСТРОЕНИЯ РЕЗЕРВНОГО ИСТОЧНИКА ПИТАНИЯ БАЗОВОЙ СТАНЦИИ СОТОВОЙ СВЯЗИ НА ОСНОВЕ СУПЕРКОНДЕНСАТОРОВ И АККУМУЛЯТОРНЫХ БАТАРЕЙ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: базовая станция сотовой связи, электроснабжение базовой станции сотовой связи, резервный источник питания, аккумуляторные батареи, суперконденсаторы.

В статье рассмотрен вопрос построения резервного источника питания в составе системы электроснабжения базовой станции сотовой связи, позволяющего сохранять

---

неснижаемый уровень электрической емкости аккумуляторных батарей. Это достигается посредством включения в его состав кроме аккумуляторных батарей суперконденсаторов, которые способны оперативно отдавать мощность в нагрузку, сохраняя емкость аккумуляторных батарей при эксплуатации в режимах повторяющихся кратковременных перерывов в электроснабжении. Проведен анализ эксплуатационно-технических характеристик аккумуляторных батарей, как резервного источника питания для электроприемников базовой станции сотовой связи и сделан вывод о целесообразности включения в состав этого источника суперконденсаторов, позволяющих брать на себя первыми нагрузку на время перерывов в питании от сети. Рассмотрен алгоритм совместного использования суперконденсаторов и аккумуляторных батарей в составе резервного источника питания для электроприемников базовой станции сотовой связи.

V.V. Ershov<sup>1</sup>, N.V. Rudenko<sup>2</sup>, E.A. Kuzenkov<sup>1</sup>, A.E. Vasiliev<sup>2</sup>

## **ABOUT THE POSSIBILITY OF BUILDING A BACKUP POWER SOURCE FOR A CELLULAR BASE STATION BASED ON SUPERCAPACITORS AND BATTERIES**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Federal State Budgetary Educational Institution higher education "Don State Technical  
University", Rostov-on-Don, Russia<sup>2</sup>

**Keywords:** cellular base station, power supply to a cellular base station, backup power supply, batteries, supercapacitors,

The article discusses the issue of constructing a backup power source as part of the power supply system of a cellular communication base station, which allows maintaining an irreducible level of electrical capacity of batteries. This is achieved by including in its composition, in addition to rechargeable batteries, supercapacitors, which are capable of quickly delivering power to the load, preserving the capacity of the batteries when operating in conditions of repeated short-term interruptions in the power supply. An analysis of the operational and technical characteristics of rechargeable batteries as a backup power source for power consumers of a cellular base station was carried out and a conclusion was made about the advisability of including supercapacitors in this source, which allow them to take on the first load of the station's power consumers during interruptions in power supply from the network. An algorithm for the joint use of supercapacitors and batteries as part of a backup power source for electrical consumers of a cellular base station is considered.

### **Введение.**

Современный этап характеризуется бурным развитием технологий в системах телекоммуникаций во всем мире, в том числе и в Российской Федерации. Одним из перспективных направлений, несомненно, является развитие технологий мобильной связи.

Устойчивое функционирование объектов системы сотовой связи обеспечивается надежным и бесперебойным электроснабжением её электроприемников в составе базовых станций (БС) и контроллеров БС.

В соответствии с [1] БС - относится ко второй, а КБС- к первой категории технологических электроприемников по надежности электроснабжения. Это обстоятельство предполагает выполнение целого ряда требований к качеству электроснабжения этих составных элементов сети связи.

Резервным источником электрической энергии в составе системы электропитания БС являются аккумуляторные батареи (АКБ) в сочетании с дизель-электрической установкой (ДЭУ). На возникающие в процессе эксплуатации кратковременные периодические перерывы в электроснабжении в первую очередь реагирует и отдает свою

---

энергию АКБ, т.к. ДЭУ предназначена для работы, как правило, в аварийных ситуациях при длительных перерывах питания.

Любое даже кратковременное подключение АКБ к нагрузке, обусловленное перерывами в электроснабжении, ведет к снижению её электрической емкости, а значит и автономности БС, кроме этого, ухудшаются эксплуатационно-технические характеристики батарей [2]. Восстановление требуемого значения электрической емкости достигается продолжительными затратами времени на подзаряд батарей. Поэтому удержание электрической емкости АКБ, как резервного источника на требуемом уровне является актуальной задачей.

### **Материалы исследования.**

В настоящее время в стране осуществляется реконструкция действующих сетей сотовой связи в направлении перехода на стандарт передачи данных 5G [3]. Переход к более перспективным технологиям предполагает улучшение эксплуатационно - технических характеристик и повышение требований ко всем структурным элементам системы сотовой связи.

Реконструкция существующих сетей стандартов 3G, 4G прежде всего подразумевает модернизацию базовых станций сотовых операторов, включая выбор оптимального решения для аварийного источника бесперебойного питания [3].

Автономность БС по питанию определяется техническими характеристиками источника бесперебойного питания. В практике в качестве такого источника достаточно успешно применяются аккумуляторные батареи (АКБ) [1], которые входят в состав системы электроснабжения БС сетей стандартов вплоть до 5G.

Однако, несмотря на общепризнанные достоинства АКБ по обеспечению бесперебойности питания электроприемников БС в течение установленного нормативными документами времени, они имеют существенные недостатки [3, 4]:

- резкое падение емкости батареи при отрицательных температурах;
- необходимость периодического обслуживания АКБ;
- потребность в резервировании АКБ;
- быстрое истощение ресурса АКБ;
- малое количество циклов работы;
- большой вес;
- выделение газов в процессе работы;
- необходимость технического обслуживания;
- необходимость в климатическом оборудовании;
- потеря емкости при низких температурах.

Герметичным свинцово-кислотным аккумуляторам, применяемым конкретно в системах электропитания БС [1] присущи следующие недостатки:

- «вздутие» с возможной последующей разгерметизацией корпуса, обусловленном избыточным выделением газа;
- окисление выводов питания аккумуляторных батарей, приводящее к возрастанию сопротивления цепи нагрузки [5];
- продолжительное время заряда (примерно в 5 раз медленнее) чем другие аккумуляторы [6].

Указанные недостатки АКБ позволяют ставить вопрос о целесообразности модернизации применяемого аварийного источника бесперебойного питания действующей системы электроснабжения БС на базе таких известных элементов, как суперконденсаторы (СК).

Суперконденсатор — это источник не постоянной, а импульсной мощности, которая ограничена только его эквивалентным внутренним сопротивлением, которое позволяет элементу работать, фактически, на токах короткого замыкания. Главным достоинством

этих устройств является высокая мощность и низкое внутреннее сопротивление, чем они и отличаются от обычных конденсаторов и аккумуляторных батарей [7].

Отличительной особенностью этих устройств от аккумуляторов является их свойство с одной стороны в процессе кратковременного разряда генерировать импульсы достаточно большой мощности, а с другой – быстро восстанавливать отданную в нагрузку мощность в процессе кратковременного заряда.

Такие свойства суперконденсаторов являются чрезвычайно полезными в ситуациях, когда имеют место кратковременные перебои в подаче электроэнергии к элементам системы сотовой связи со стороны централизованного электроснабжения. В регионах с неустойчивым электроснабжением с частыми перерывами в питании, а также для базовых станций, размещенных в труднодоступных и удаленных от источников питания государственной энергосистемы местах применение суперконденсаторов в сочетании с АКБ может дать значительный положительный эффект в плане повышения стабильности электроснабжения оборудования БС мобильных сетей связи. Технические характеристики СК и АКБ представлены в таблице 1 [3].

Таблица 1. Технические характеристики СК и АКБ

Параметр	Суперконденсатор	АКБ
Время заряда	1...30 с	0,3...3 часа
Время разряда	1...30 с	1...5 часов
Энергия	1...20 Вт*ч/кг	20...400 Вт*ч/кг
Мощность	1000-7000 Вт/кг	50...2500 Вт/кг
Количество циклов заряд-разряд	500000-1000000	500...3000

Из данных таблицы следует, что в рамках решаемой задачи по обеспечению электроприемников БС СК уступают АКБ только по времени разряда и энергии. Остальные параметры СК являются более предпочтительными по сравнению с АКБ для периодических импульсных нагрузок. Таким образом применение суперконденсаторов в составе системы электроснабжения БС может позволить [3]:

- обеспечить гарантированное время работы вне зависимости от температуры окружающей среды;
- отказаться от использования климатического оборудования;
- исключить затраты на подогрев АКБ в зимний период;
- исключить необходимость поддержания складского запаса АКБ;
- исключить затраты на сервис и мониторинг состояния АКБ;
- уменьшить затраты на эксплуатацию.

Построение резервного источника питания системы электроснабжения БС целесообразно на основе принципа максимального использования эксплуатационных достоинств входящих в его состав элементов: суперконденсаторов и АКБ. Суперконденсатор, обладая свойством как очень быстро накапливать электрическую энергию и также быстро её отдавать в нагрузку, позволяет компенсировать воздействие импульсных нагрузок на АКБ в процессе кратковременных перерывов электроснабжения. Благодаря этому обстоятельству появляется возможность сократить, если энергии суперконденсаторов оказалось недостаточно для работы электроприемников БС и АКБ включились в работу на продолжающемся временном интервале перерыва, либо полностью исключить расход мощности батарей, если энергии суперконденсаторов оказалось достаточно для работы электроприемников БС в течение временного отрезка перерыва в электропитании.

При этом в обоих случаях после восстановления питания от сети запас электроэнергии суперконденсаторов будет восстановлен в течение единиц-десятков

---

секунд, а во втором – запас электроэнергии АКБ потребует значительно большего времени. Таким образом в обоих случаях электрическая емкость батарей, как важнейший эксплуатационный параметр сохраняется на большем уровне по сравнению с приемом батарей на себя нагрузки даже в течение кратковременного перерыва в питании.

Построение перспективного резервного источника питания системы электроснабжения БС на основе совместного использования достоинств суперконденсаторов и АКБ может позволить сократить либо полностью исключить расход мощности батарей в зависимости от продолжительности временного промежутка кратковременного перерыва в электроснабжении от Госэнергосистемы.

#### **Анализ известных технических решений.**

Одна из крупнейших американских энергетических компаний Duke Energy столкнулась с необходимостью нести значительные затраты, связанные с модернизацией существующей инфраструктуры при подключении возобновляемых источников энергии к распределительной сети. С целью сглаживания нестабильной солнечной генерации, компенсации импульсной мощности и поддержания нагрузки в периоды низкой генерации был установлен гибридный накопитель в составе суперконденсаторов 277 кВт / 8,0 кВт-ч и аккумуляторных батарей 50 кВт / 300 кВт-ч. Суперконденсаторы быстро компенсируют как изменения мощности солнечной генерации, так и импульсные нагрузки, тем самым избавляя аккумуляторы от деградирующих их режимов заряда/разряда. Батареи же обеспечивают долговременное накопление энергии от солнечных батарей и поддержание нагрузки в наиболее оптимальные для этого периоды времени. В результате обеспечено сокращение капитальных затрат на 10-15 % и сокращение операционных затрат на 30 % в сравнении с применением только батарей [8].

При указанных параметрах мощности и энергии СК они обеспечивают работу оборудования в течение 103 секунд, сохраняя энергию АКБ.

В качестве другого примера эффективного решения компенсации импульсной мощности с помощью суперконденсаторов можно привести проект глубоководного порта Yangshan в Китае, расположенного недалеко от Шанхая. 23 портовых крана постоянно создавали значительные изменения (просадки) напряжения длительностью 10-15 секунд. Так как порт расположен в 20 милях от берега, увеличение подводимой мощности и прокладка дополнительных силовых кабелей были очень дорогим решением. В качестве альтернативного решения был разработан и установлен суперконденсаторный накопитель мощностью 3 МВт / 17,2 кВт-ч, обеспечивающий 20-секундную поддержку и компенсацию падения напряжения при работе кранов. В результате обеспечено 38 % сокращение потребления электроэнергии в пиковых режимах, экономия потребления электроэнергии составила \$ 2,9 млн, а экономия за счёт повышения эффективности и сокращения эксплуатационных издержек составила \$ 41 млн [8].

#### **Алгоритм работы резервного источника.**

Сравнительный анализ эксплуатационно-технических характеристик АКБ и СК позволяет представить в первом приближении алгоритм совместного использования этих компонентов в составе резервного комбинированного источника системы электроснабжения БС. С началом временного интервала прекращения электроснабжения электроприемников БС первым элементом в составе такого резервного источника принимает на себя нагрузку СК, обеспечивая бесперебойность функционирования БС.

Система управления фиксирует момент включения СК и обеспечивает контроль текущего значения уровня отдаваемой энергии до минимально допустимого значения отдаваемой им энергии. В момент времени достижения этого уровня минимально допустимого значения системой управления формируется сигнал на выключение СК из работы и включение в работу АКБ, от которых продолжается работа электроприемников БС до окончания времени перерыва в электроснабжении.



После восстановления электроснабжения от Госэнергосистемы АКБ включаются на подзаряд для восстановления уровня электрической емкости. В том случае, если энергии СК оказывается недостаточно для обеспечения работы в течение временного интервала перерыва в электроснабжении, то АКБ не включаются в работу, сохраняя неизменным требуемое значение электрической емкости, а система управления формирует сигнал на заряд СК.

Структурная схема системы электропитания базовой станции, реализующей рассмотренный алгоритм, представлена на рисунке 1. Электрическая энергия от районной энергосистемы подается на трансформаторную подстанцию (ТП). При наличии напряжения в районной электросети и соответствия величины напряжения допусковым параметрам оно через трансформаторную подстанцию (ТП), коммутатор К1 и распределительный щит ЩР1 подается к приемникам станции. Потребляемая мощность контролируется датчиком потребляемой мощности (ДПМ).

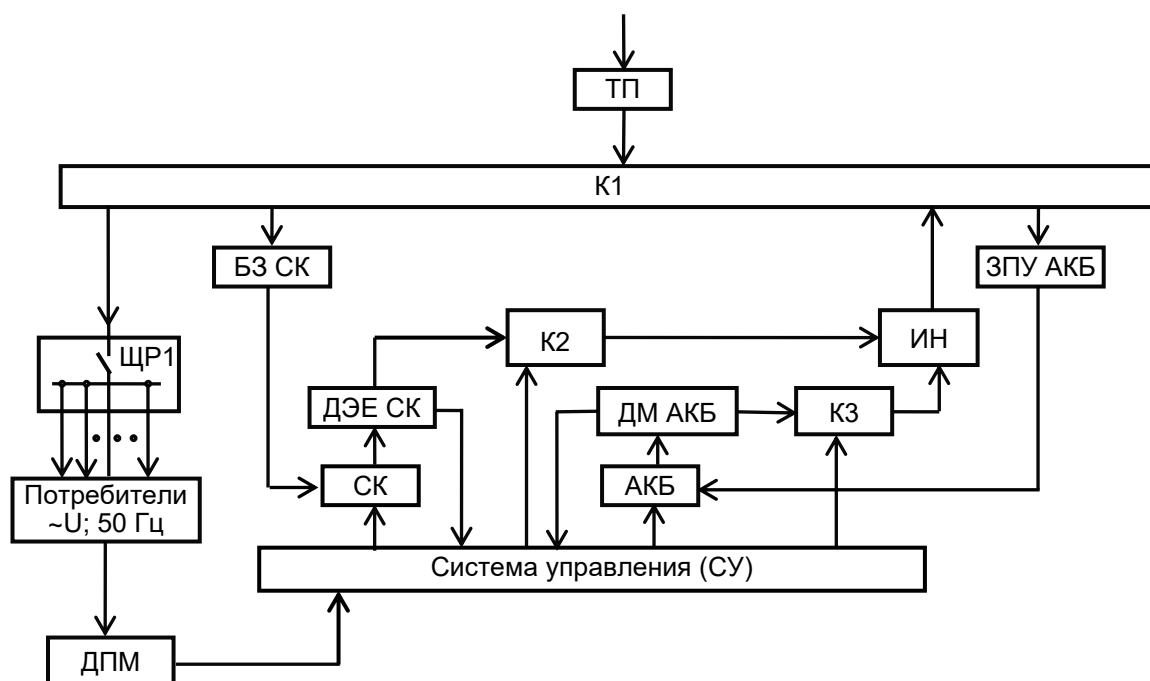


Рисунок 1. Структурная схема системы электропитания базовой станции

При исчезновении или выходе за пределы допусковых значений величины напряжения питающей сети по сигналу от системы управления (СУ) в работу включаются СК и коммутатор К2, который подключает выход СК к входу инвертора напряжения (ИН) и далее через коммутатор К1 к приемникам станции. Текущее значение уровня отдаваемой СК электрической энергии контролируется датчиком электрической емкости СК (ДЭЕ СК).

С достижением этого параметра минимально допустимого значения по сигналу от СУ коммутатор К2 отключает СК от ИН и включается в работу АКБ и коммутатор К3, который подключает выход АКБ к входу ИН и далее также через коммутатор К1 к приемникам станции. Работа электроприемников БС до окончания времени перерыва в электроснабжении осуществляется от АКБ. Текущее значение уровня отдаваемой АКБ электрической энергии контролируется датчиком мощности (ДМ АКБ).

По окончании времени перерыва в электроснабжении подзаряд СК и АКБ осуществляется соответственно от блока заряда суперконденсаторов (БЗ СК) и зарядно-подзарядного устройства АКБ (ЗПУ АКБ).

### **Выводы:**

1. Построение комбинированного резервного источника питания базовой станции сотовой связи на базе АКБ и СК позволяет улучшить эксплуатационные характеристики АКБ за счет принятия СК на себя импульсных повторяющихся нагрузок.
2. Практическое применение такого источника оказывается наиболее эффективным в зонах неустойчивого централизованного электроснабжения.

### **СПИСОК ЛИТЕРАТУРЫ**

1. РД 45.162-2001 (с изм. 2002) МИНИСТЕРСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПО СВЯЗИ И ИНФОРМАТИЗАЦИИ. РУКОВОДЯЩИЙ ДОКУМЕНТ ОТРАСЛИ. ВЕДОМСТВЕННЫЕ НОРМЫ ТЕХНОЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ. КОМПЛЕКСЫ СЕТЕЙ СОТОВОЙ И СПУТНИКОВОЙ ПОДВИЖНОЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ. [Электронный ресурс]: [//http://svarak.ru/document/rd-45162-2001-s-izm-2002](http://svarak.ru/document/rd-45162-2001-s-izm-2002) (дата обращения 18.08.2023 г.)
2. Каково влияние импульсного разряда на эффективность свинцово-кислотных батарей в ватт-часах (Втч)? [Электронный ресурс]: [//https://electronics.stackexchange.com/questions/165421/what-is-the-effect-of-pulsed-discharge-on-watt-hour-wh-efficiency-of-lead-acid](https://electronics.stackexchange.com/questions/165421/what-is-the-effect-of-pulsed-discharge-on-watt-hour-wh-efficiency-of-lead-acid) (дата обращения 05.09.2023 г.)
3. Телекоммуникации – ТПС-Энергетические системы [Электронный ресурс]: [//https://tps-ens.ru/telekommunikacii/](https://tps-ens.ru/telekommunikacii/) (дата обращения 06.09.2023 г.)
4. Телекоммуникации – ТПС-Энергетические системы Возобновляемая энергетика [Электронный ресурс]: [//https://tps-ens.ru/vozobnovljaemaja-jenergetika/](https://tps-ens.ru/vozobnovljaemaja-jenergetika/) (дата обращения 06.09.2023 г.)
5. Герметичные кислотно-свинцовые аккумуляторы. [Электронный ресурс]: [//https://go-radio.ru/accumulator.html](https://go-radio.ru/accumulator.html) (дата обращения 06.09.2023 г.)
6. Типы аккумуляторных батарей и области их применения [Электронный ресурс]: [//https://www.solarhome.ru/batteries/battery-types.htm](https://www.solarhome.ru/batteries/battery-types.htm) (дата обращения 14.09.2023 г.)
7. Суперконденсаторы: что это, зачем и где применяется [Электронный ресурс]: [//https://habr.com/ru/articles/547310/](https://habr.com/ru/articles/547310/) (дата обращения 22.09.2023 г.)
8. Применение суперконденсаторов EDLC в возобновляемой энергетике. Мировая практика [Электронный ресурс]: [//https://econet.ru/articles/150609-primenenie-superkondensatorov-edlc-v-vozobnovlyaemoj-energetike-mirovaya-praktika](https://econet.ru/articles/150609-primenenie-superkondensatorov-edlc-v-vozobnovlyaemoj-energetike-mirovaya-praktika) (дата обращения 22.09.2023 г.)

**А.В. Елисеев<sup>1,2</sup>, А.Г. Жуковский<sup>2</sup>, М.Я. Клименко<sup>1</sup>, М.Р. Разыкова<sup>1</sup>**

### **АНАЛИЗ МЕТОДОВ ВЕРИФИКАЦИИ ДАННЫХ АВИАЦИОННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ**

Донской государственный технический университет, Ростов-на-Дону, Россия<sup>1</sup>  
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: автоматическое зависимое наблюдение вещательного типа (АЗН-В), верификация данных, методы защиты данных АЗН-В.

Показано, что в настоящее время для решения задачи авиационного наблюдения широко используются данные системы автоматического зависимого наблюдения

---

вещательного типа (АЗН-В). Указано на такой существенный недостаток системы АЗН-В как слабая защищенность от процедуры спуфинга по причине отсутствия явных механизмов для защиты конфиденциальности, целостности и доступности данных. Проведен анализ известных методов защиты данных АЗН-В, предложено дополнительно для этих целей использовать угломерно-энергетический метод контроля местоположения воздушного судна, а также бистатический или мультистатический полуактивный радиолокаторы.

**A.V. Eliseev<sup>1,2</sup>, A.G. Zhukovsky<sup>2</sup>, M.Ya. Klimenko<sup>1</sup>, M.R. Razykova<sup>1</sup>**

## **ANALYSIS OF DATA VERIFICATION METHODS OF THE AVIATION TELECOMMUNICATION SYSTEM**

Don State Technical University, Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

**Keywords:** automatic dependent monitoring of broadcast type (AZN-B), data verification, methods of data protection of AZN-B.

It is shown that at present, data from the broadcast-type automatic dependent surveillance system (AZN-B) are widely used to solve the problem of aviation surveillance. It is pointed out that such a significant drawback of the AZN-B system as weak protection from spoofing procedures due to the lack of explicit mechanisms to protect confidentiality, integrity and availability of data. The analysis of the known methods of data protection of the AZN-B is carried out, it is proposed to additionally use for these purposes the angular-energy method of controlling the location of the aircraft, as well as bistatic or multistatic semi-active radars.

Управление воздушным движением самолетов гражданской авиации основывается на данных авиационного наблюдения. В качестве источников таких данных изначально используются радиолокационные системы двух типов: первичные радиолокаторы и вторичные радиолокаторы. Наряду с такими достоинствами как автономность решения задачи наблюдения первичными локаторами, значительная дальность действия, точность и возможность получения адресной информации от конкретного воздушного судна как у вторичных локаторов, указанные источники имеют и такие существенные недостатки как высокая стоимость, сложность обслуживания, ограниченные зоны действия. Для преодоления указанных недостатков были разработаны технологии автоматического зависимого наблюдения как вещательного (АЗН-В), так и контрактного типов [1-6].

Технология АЗН-В предполагает передачу с борта воздушного судна, оборудованного соответствующим устройством, доступную для любого наблюдателя информацию о пространственном положении воздушного судна (ВС), его скорости движения, опознавательного индекса и др. данных. Основным источником навигационной информации для АЗН-В является бортовая аппаратура потребителей глобальной навигационной спутниковой системы (GNSS).

Следует отметить, что технология АЗН-В обеспечивает свободный доступ к данным о координатах ВС всем потребителям, имеющим соответствующее приемное устройство.

Общая структура АЗН-В и схема обмена информационными потоками показаны на рисунке 1 [3]. Из рисунка видно, что источником навигационной информации для АЗН-В являются навигационные космические аппараты, а потребителями выступают как наземные приемные пункты, транслирующие навигационную информацию на диспетчерские пункты, так и бортовая приемная аппаратура ВС, предназначенная для решения задачи предупреждения опасного сближения и столкновения ВС.

Первоначально, с момента появления технологии АЗН-В, рассматривалась перспектива полного отказа от использования первичных и вторичных локаторов. Однако далее, после анализа недостатков АЗН-В, было принято решение о совместной эксплуатации как локаторов, так и оборудования АЗН-В. Следует отметить, что несмотря на имеющиеся недостатки технологии АЗН-В международная организация гражданской авиации (ИКАО) рассматривает АЗН-В в качестве основного метода авиационного наблюдения. Так, например, авиационные администрации США и Европы в своих программах, соответственно, NextGen и SESAR, требуют обязательного оснащения ВС системой АЗН-В [2, 3].

В Российской Федерации, в соответствии с «Концепцией внедрения автоматического зависимого наблюдения на основе единого стандарта...», утвержденной распоряжением Минтранса России от 25 апреля 2018 года № 68, также проводятся мероприятия по внедрению АЗН-В.

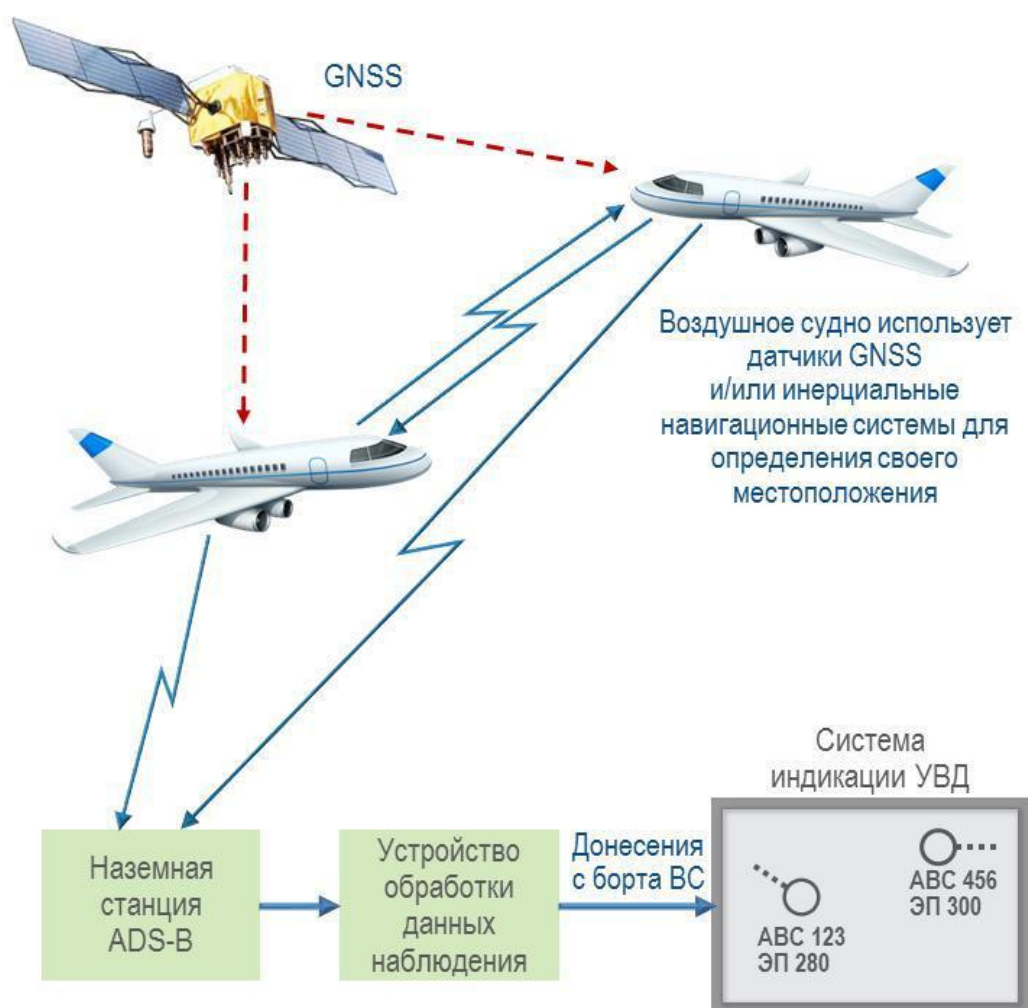


Рисунок 1. Упрощенная структура системы АЗН-В и взаимодействие её элементов [3]

Как уже отмечалось, наряду с существенными достоинствами АЗН-В, такими как низкая стоимость оборудования, высокая точность, характеризуемая точностью GNSS, доступность для потребителей, возможность создания глобальной системы авиационного наблюдения на основе ретрансляции сигналов АЗН-В через спутники-ретрансляторы, имеется и существенный недостаток, обусловленный отсутствием технологий защиты конфиденциальности данных, что может позволить злоумышленникам использовать подмену данных – спуффинг [2].

---

По этой причине в настоящее время актуальной проблемой является верификация данных АЗН-В. Наиболее полно известные методы верификации данных рассмотрены в работе [2]. Однако их можно дополнить на основе анализа других методов, позволяющих получить дополнительную информацию о местоположении ВС, и на этой основе подтвердить или опровергнуть гипотезу о достоверности данных АЗН-В.

Существует достаточно большое количество методов киберзащиты данных АЗН-В, которые упрощенно можно разделить на две группы [2, 3], представленные на рисунке 2.

Методы первой группы рассматривают ВС как абонента мобильной телекоммуникационной сети связи, в которой могут решаться задачи идентификации и аутентификации абонентов. Такие методы в настоящее время находят широкое применение в задачах государственного опознавания. Пример криптографической схемы, обеспечивающей верификацию данных АЗН-В, приведен на рисунке 3 [3], где рассмотрена линия передачи данных типа VDL режима 4 и предлагается использовать асимметричное шифрование на канальном уровне с использованием открытого и закрытого ключей. Однако, как показано в работе [3], методы первой группы сложно применить для верификации данных АЗН-В. Следует отметить, что применение методов первой группы в гражданской авиации существенно снизит достоинство технологии АЗН-В по причине снижения доступности для заинтересованных потребителей данных о траектории ВС.

Методы второй группы основаны на процедуре подтверждения данных АЗН-В на основе некоторой дополнительной информации о траектории движения ВС, полученной от других систем авиационного наблюдения, таких как первичные и вторичные локаторы, многопозиционные системы наблюдения (MLAT) и др. [2, 3].

Рассмотрим более подробно методы второй группы (рисунок 2).

*Верификация на основе данных мультilaterационной системы (MLAT).* Система *MLAT* представляет собой распределенную многопозиционную систему синхронизированных приемных пунктов, связанных линиями связи с центром обработки [2, 3]. Принцип работы системы основан на использовании разностно-дальномерного позиционного метода навигации. Сигнал АЗН-В от конкретного ВС принимается множеством наземных приемных пунктов, передается в центр обработки, где вычисляется разность времен прихода сигнала на различные приемные пункты. Упрощенный состав и информационные связи системы мультilaterации показаны на рисунке 4 [3].

Данный метод верификации данных в настоящее время считается наиболее рациональным, так как обладает высокой достоверностью при относительно низкой стоимости оборудования по сравнению с первичными и вторичными локаторами. Системы *MLAT* уже эксплуатируются в США, в Европе и в РФ. Достоинствами мультilaterации являются высокая точность определения местоположения и параметров движения ВС, возможность использования для решения указанных задач радиоизлучений штатных бортовых средств ВС. Таким образом, не требуются специальное дооборудования ВС, что выгодно с экономической точки зрения. Дальнейшим развитием мультilaterационных систем является создание широкозонной мультilaterации на основе применения спутниковой группировки.





Рисунок 2. Классификация методов защиты данных АЗН-В от спуфинга

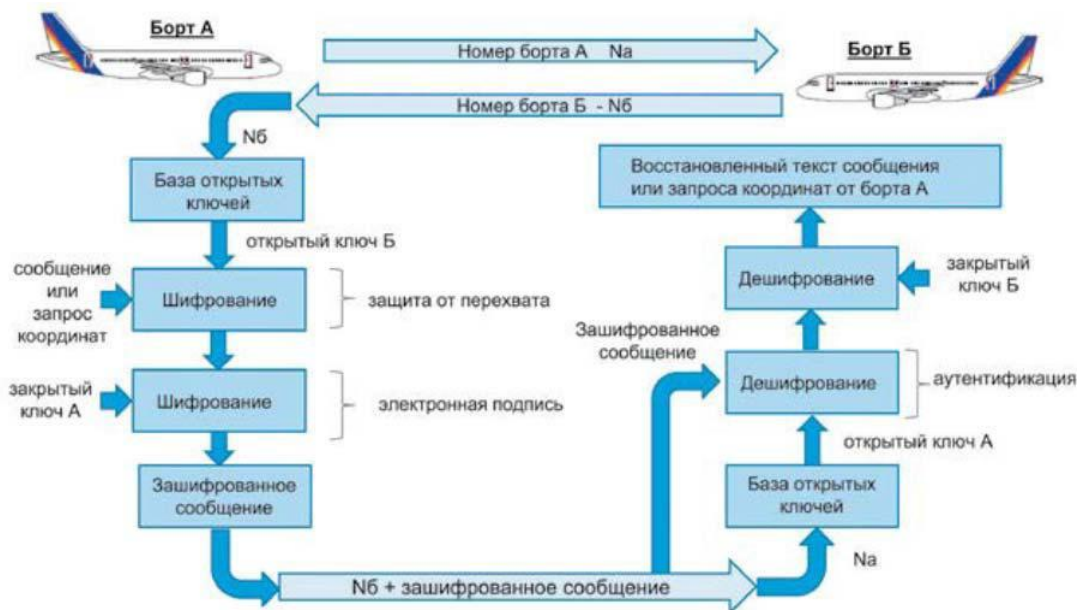


Рисунок 3. Процесс обмена зашифрованными сообщениями [3]

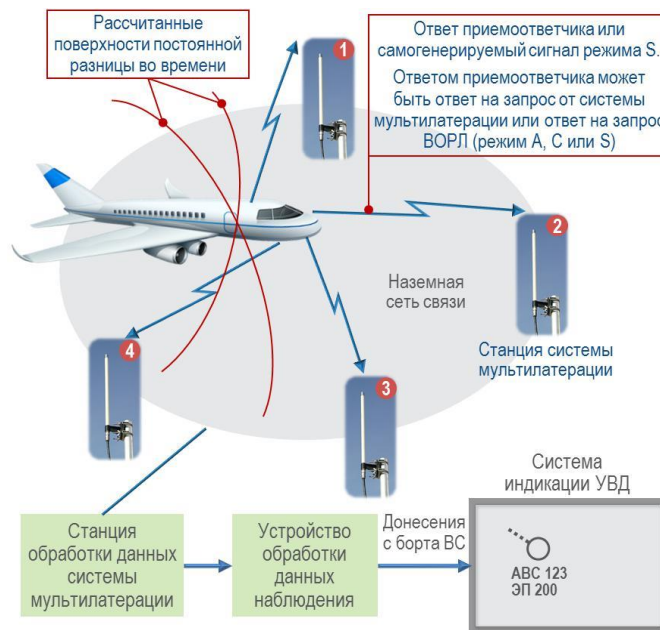


Рисунок 4. Упрощенная структура и взаимодействие элементов мультilaterационной системы [3]

В качестве недостатков мультilaterационных систем следует отметить их восприимчивость к многолучевому распространению, необходимость решения задачи идентификации сигнала, принадлежащего конкретному ВС, на всех приемных пунктах, требование наличия отдельной линии связи между центральной станцией обработки и разнесенными в пространстве приемниками, обязательность высокоточной синхронизации шкал времени всех приемных пунктов и центральной станции обработки [3, 6].

*Верификация на основе угломерно-энергетических измерений.* Данный метод основан на применении классического угломерно-дальномерного позиционного метода определения местоположения ВС, за исключением того, что дальность до ВС определяется на основе энергетического метода, например, как в работе [7]. Угловые измерения могут быть выполнены с использованием остронаправленной антенны со сканирующим лучом или с использованием секторной антенны, например, применяемой в аппаратуре АЗН-В «Пульсар-Н». Идея энергетического метода измерения дальности основана на измерении разности мощностей принимаемого сигнала в различные моменты времени, соответствующие различным положениям в пространстве ВС. При этом вводятся допущения о равномерном и прямолинейном движении ВС с известной скоростью [7]. и неизменностью значения излучаемой мощности бортового передатчика ВС.

Результатом применения угломерно-энергетического метода являются данные о пространственном положении ВС или данные о его местоположении – положении на поверхности, которое сравнивается с данными, полученными по каналам АЗН-В. По результатам сравнения с использованием принятого критерия принимается решение о верификации данных АЗН-В.

Один из методов определения дальности до ВС на основе энергетических измерений рассмотрен в работе [7]. Геометрическая постановка задачи определения дальности до цели (Ц) на основе измерений мощности принимаемого сигнала, приведена на рисунке 5.

На рисунке 5 точки  $Ц_i$ ,  $Ц_j$  и  $Ц_k$  обозначают положения цели в различные моменты времени:  $t_i$ ,  $t_j$  и  $t_k$ , при этом принимается ограничение, что  $\Delta t_{ij} = |t_j - t_i| = |t_k - t_j| = \Delta t_{jk}$ . Также принимается допущение об известности скорости движения ВС  $v$  [7]. Из рисунка 5 видно, что так как  $v\Delta t_{ij} = v\Delta t_{jk}$ , прямая  $ОЦ_j$  является медианой треугольника  $ОЦ_iЦ_k$ . На

основе этого предположения, и с учетом вида выражения для мощности принимаемого сигнала, следующего из уравнения радиосвязи

$$p = \mu r^{-2}, \quad r = \|r\|, \quad \mu(t) = \mu = \text{const} \forall t \in [0, T],$$

получено выражение для оценки дальности до цели [7]

$$r_k = \left[ 2p_i p_j s_{ij}^2 (p_i p_j + p_j p_k - 2p_i p_k)^{-1} \right]^{\frac{1}{2}},$$

где  $s_{ij} = v\Delta t_{ij} = v\Delta t_{jk} = s_{jk}$ ,  $p_i, p_j, p_k$  – мощность сигнала, излучаемого ВС и наблюдаемого на входе приемного устройства измерительной системы в моменты времени  $t_i, t_j, t_k$ , соответственно.

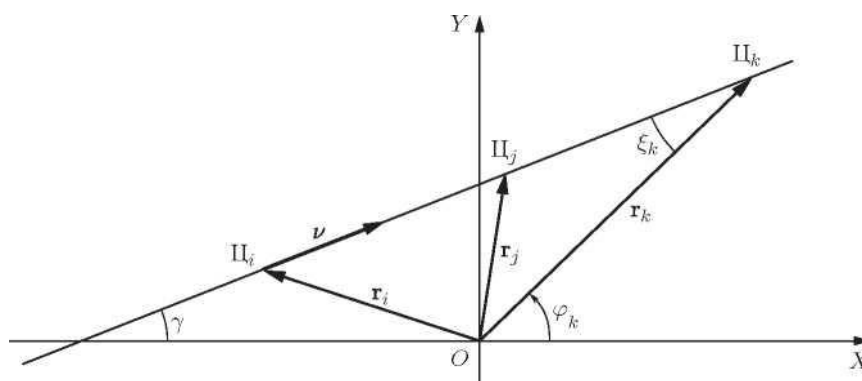


Рисунок 5. Геометрическая постановка задачи определения дальности до цели [7]

Следует отметить, что основными ограничениями данного метода являются условие прямолинейного движения ВС и необходимость знания его скорости.

*Верификация на основе данных мультистатического первичного обзорного лоатора (MSPSR [2]).* Системой MSPSR называют сеть из нескольких передающих и приемных пунктов (в предельном случае система является бистатической и содержит один передатчик и один приемник с направленной антенной, рисунок 6). Такой лоатор в отечественной литературе принято называть полуактивным лоатором [8]. При этом, координаты передающих и приемных пунктов полагаются известными, что позволяет на каждой приемной позиции, на основе приема отраженного от ВС сигнала передатчика «подсвета», определить бистатическую дальность, которой соответствует эллипсоид. Тогда пересечение трех эллипсоидов определяет область вероятного расположения ВС. В таких системах в качестве передатчиков, являющихся источником сигналов «подсвета», могут использоваться сторонние, то есть не входящие в штатный состав передатчики, например, станции радио- и телевизионного вещания и базовые станции мобильной телефонной связи, или передатчики, специально установленные для того, чтобы не зависеть от источников излучения третьих сторон [8, 9]. Использование сторонних передатчиков позволяет существенно упростить структуру и уменьшить стоимость MSPSR, кроме того, в отличие от MLAT, появляется возможность определять местоположение ВС даже при их переходе в режим «радиомолчания». В качестве недостатка MSPSR следует отметить сложность разделения прямого сигнала (линия DC на рисунке 6), принимаемого направленной антенной приемника непосредственно от передатчика «подсвета», и отраженного от ВС сигнала, принимаемого этой же антенной.

Несмотря на указанный недостаток, следует отметить, что в настоящее время существует относительно большое число примеров практической реализации MSPSR различного назначения [8, 9]. Так, например, 14 мая 2013 г. чешская фирма ERA («ERA Systems Corporation»), известная своими разработками в области пассивной локации, официально представила

демонстрационную версию полуактивной системы, мобильная версия которой получила условное название Silent Guard (рисунок 7).

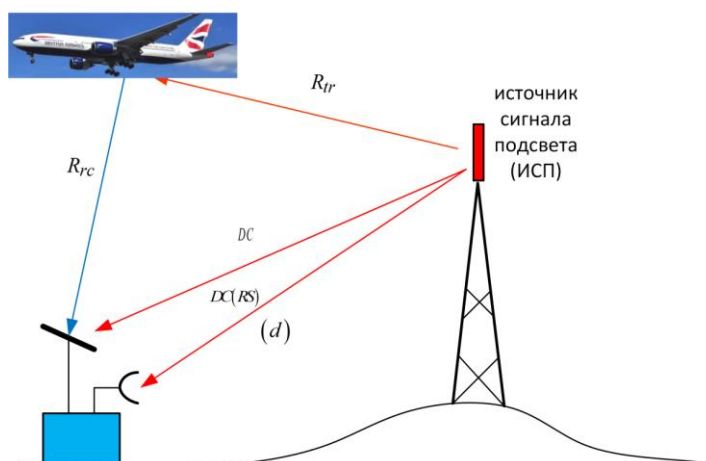


Рисунок 6. Пример структуры бистатического первичного обзорного локатора (MSPSR) на основе когерентной обработки сигналов

*Верификация на основе использования алгоритмов фильтрации Калмана.* Алгоритм фильтра Калмана, в общем случае, состоит из двух матричных уравнений – уравнения оценки вектора состояния и уравнения оценка корреляционной матрицы ошибок фильтрации [3, 10, 11]. Данные уравнения построены на основе математической модели движения воздушного судна и уравнения измерений наблюдаемых параметров, что позволяет учитывать в фильтре особенности динамики воздушного судна, его возможности по маневрированию и др. Таким образом, в любой момент времени с помощью фильтра формируются оценка вектора состояния и оценка корреляционной матрицы ошибок фильтрации. Полученные оценки позволяют осуществить верификацию данных АЗН-В путем их сравнения с результатами фильтрации по принятому критерию, так, например, Калмановская фильтрация позволяет обнаруживать фиктивные маневры воздушного судна, что значительно усложняет организацию эффективного спуфинга [3, 11]. Пример алгоритма фильтрации, устойчивого к сингулярным ошибкам, рассмотрен в работе [11].



Рисунок 7. Бистатический локатор «Silent Guard»: а – общий вид мобильного варианта; б – антенная система [9]

*Групповая верификация.* Данный метод верификации основан на использовании мультилатерационного метода определения местоположения, когда в качестве приемных пунктов, которых должно быть не менее четырех, выступают ВС, находящиеся во взаимной радиовидимости [3]. При этом, в большинстве случаев, для установления взаимного доверия потребуется аутентификация ВС, входящих в группу. Мультилатерация

выполняется посредством взаимного радиообмена между членами группы измерительной информацией. Следует отметить, что практическая реализация данного способа потребует решения задачи помехозащищенной передачи данных между ВС, выполняющими роль приемных позиций мультilaterационной системы, и ВС, выполняющим роль центра обработки данных. При этом также необходимо решить задачу разработки методики включения и исключения ВС из группы.

Проведенный анализ известных и предлагаемых методов верификации данных АЗН-В позволяет сделать вывод, что такие методы как верификация на основе данных мультilaterационной системы, на основе угломерно-энергетических измерений, на основе мультистатического локатора и на основе групповой верификации требуют создания и развертывания как на земной поверхности, так и на борту воздушных судов, как, например, для случая групповой верификации, специального оборудования. Данный фактор существенно усложняет решение задачи верификации и снижает её экономическую привлекательность. По этой причине, с точки зрения соотношения цена/качество, для решения задачи верификации может быть целесообразным использование способа на основе применения алгоритмов фильтрации Калмана [10, 11]. Однако, для обеспечения высокого уровня достоверности верификации данных АЗН-В, целесообразно использовать комплексированные процедуры, объединяющие несколько из рассмотренных на рисунке 2 методов.

#### СПИСОК ЛИТЕРАТУРЫ

1. Рабочий документ ИКАО А39-WP/2961 TE/125 26/8/16. Наблюдение дистанционно пилотируемых воздушных судов и вопросы кибербезопасности // [Электронный ресурс]. URL: <http://www.icao.int> (дата обращения: 20.10.2023).
2. Aeronautical Surveillance Manual. Doc 9924 AN/474. 2<sup>nd</sup> ed. ICAO. Montreal, 2017.
3. Косьянчук В.В., Сельвесюк Н.И., Хамматов Р.Р. Обзор основных путей повышения безопасности системы АЗН-В // Научный Вестник МГТУГА. – 2019, Т.22, №1, С. 40-50.
4. Strohmeier M. On perception and reality in wireless air traffic communication security / M. Schäfer, R. Pinheiro, V. Lenders, I. Martinovic // IEEE Transactions on Intelligent Transportation Systems. – 2017, Vol. 18, Iss. 6, Pp. 1338–1357.
5. Фальков Э.Я. Интеграция беспилотных авиационных систем в общее воздушное пространство: ключевые проблемы и возможные пути решения // Крылья Родины. – 2016, № 6, С. 26–32.
6. Алипов И.В. Проблемы внедрения вещательного автоматического зависимого наблюдения (АЗН-В) в Российской Федерации // Научный вестник ГосНИИ ГА. – 2015, №7. С. 86-92.
7. Булычев Ю.Г., Ивакина С.С., Мозоль А.А., Насенков И.Г. Анализ модификации энергетического метода пассивной дальнометрии // Автометрия. – 2016, Т.52, №1, С. 37-44.
8. Семашко П.Г., Пархоменко Н.Г., Охрименко А.Е. Перспективы полуактивной радиолокации в связи с развитием служб цифрового радиовещания // Успехи современной радиоэлектроники. – 2010, №7, С. 38-46.
9. Бархатов А.В., Веремьев В.И., Воробьев Е.Н., Коновалов А.А., Ковалев Д.А., Кутузов В.М., Михайлов В.Н. Пассивная когерентная радиолокация. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», – 2016, 163с.
10. Елисеев А.В., Ануфриев К.В., Погорелов Р.А., Рубайло Д.Э. Алгоритм адаптивной настройки параметров линейного дискретного фильтра с использованием нечеткой экспертной системы // Радиотехника. – 2019, Т.83, № 7(9), С. 89-102.
11. Елисеев А.В. Алгоритм линейной фильтрации, устойчивый к сингулярным ошибкам // Изв. ВУЗов. Радиоэлектроника. – 2005, №10, С. 20-28.

---

**А.В. Елисеев<sup>1,2</sup>, А.Г. Жуковский<sup>2</sup>, М.Я. Клименко<sup>1</sup>, М.Р. Разыкова<sup>1</sup>**

**ОБОСНОВАНИЕ СТРУКТУРЫ СОВРЕМЕННОЙ ГИБРИДНОЙ  
РАДИОТЕХНИЧЕСКОЙ СИСТЕМЫ ПОИСКА ТЕРПЯЩИХ БЕДСТВИЯ  
ТРАНСПОРТНЫХ СРЕДСТВ**

Донской государственной технической университет, Ростов-на-Дону, Россия<sup>1</sup>  
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: гибридная радиотехническая система поиска, космические аппараты, беспилотные летательные аппараты, аварийный радиомаяк.

Рассмотрена задача обоснования структуры современной региональной системы поиска терпящих бедствие транспортных средств. Предложена структура системы поиска, содержащая аварийные радиомаяки, сеть беспилотных летательных аппаратов, сеть низкоорбитальных космических аппаратов, ретранслятор на высокоорбитальном космическом аппарате.

**A.V. Eliseev<sup>1,2</sup>, A.G. Zhukovsky<sup>2</sup>, M.Y. Klimenko<sup>1</sup>, M.R. Razykova<sup>1</sup>**

**SUBSTANTIATION OF THE STRUCTURE OF A MODERN HYBRID RADIO  
ENGINEERING SEARCH SYSTEM FOR VEHICLES IN DISTRESS**

Don State Technical University, Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: hybrid radio engineering search system, spacecraft, unmanned aerial vehicles, emergency beacon.

The problem of substantiating the structure of a modern regional search system for vehicles in distress is considered. The structure of the search system containing emergency beacons, a network of unmanned aerial vehicles, a network of low-orbit spacecraft, a repeater on a high-orbit spacecraft is proposed.

Современная экономика и социальная жизнь развитых стран характеризуется высокой динамикой перемещения как предметов хозяйственной деятельности, так и населения на различных видах транспорта: наземного, морского и воздушного. Особую роль при этом играет воздушный транспорт, обеспечивающий высокую оперативность и глобальность решения задач перевозки грузов и пассажиров. Одним из важнейших требований к авиационной деятельности предприятий гражданской авиации является безопасность полетов. Под безопасностью полетов понимается такое состояние, при котором риски, связанные с авиационной деятельностью, относящейся к эксплуатации воздушных судов или непосредственно обеспечивающей такую эксплуатацию, снижены до приемлемого уровня и контролируются [1, 2]. В настоящее время, в мире достигнут относительно высокий уровень безопасности полетов, вероятность погибнуть в самолете гораздо ниже, чем при путешествии на железнодорожном или автомобильном транспорте, что иллюстрируется данными на рисунке 1 [2].



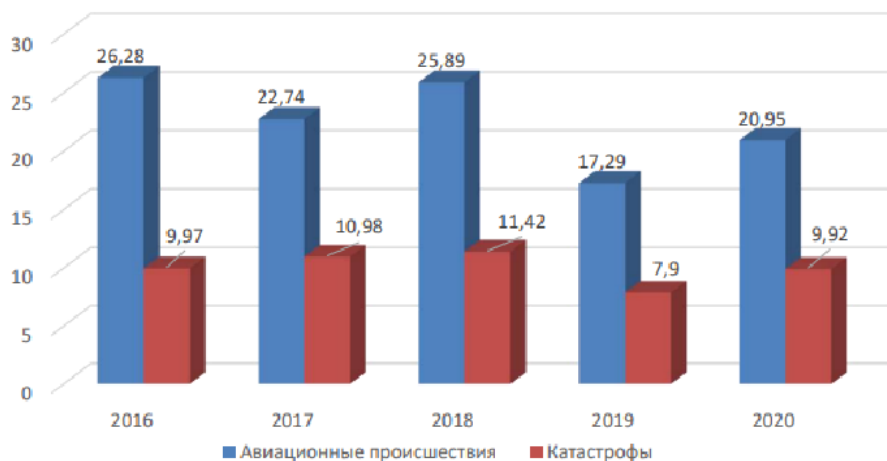


Рисунок 1. Количество авиационных происшествий и катастроф на один миллион вылетов всех воздушных судов гражданской авиации государств-участников Соглашения

Несмотря на относительно малое число авиационных происшествий и катастроф на один миллион вылетов по-прежнему актуальна задача своевременного обнаружения факта наступления авиационного происшествия и проведения аварийно-спасательных работ, так как от эффективности решения этих задач зависит тяжесть наступивших последствий.

Авиационные подразделения поиска и спасения (АПСС) использует, как правило, следующие источники информации: результаты радиолокационного контроля с помощью систем авиационного наблюдения, полученные до момента аварии, данные международной системы поиска и спасения *COSPAS-SARSAT*, результаты приема сигналов аварийных радиомаяков (АРМ), аварийных радиостанций (АРС), а также результаты оптико-электронного наблюдения с борта специализированных космических аппаратов или спасательных воздушных судов АПСС [3-5].

Основой современной радиотехнической системы поиска и спасения является международная космическая система поиска и спасения *COSPAS-SARSAT*, созданная в период 1978-1987 гг. в результате совместных усилий СССР, США, Канады и Франции [5].

Первоначально, система *COSPAS-SARSAT* включала в свой состав два типа космических аппаратов: низкоорбитальные - для приема сигналов АРМ и последующего определения их местоположения на основе эффекта Доплера и геостационарные – для ретрансляции сигналов от низкоорбитальных спутников в наземный центр обработки. Недостатком такой космической группировки является дискретность решения задачи поиска в пределах конкретного района, обусловленная фиксированным временем радиовидимости спутника из зоны бедствия по причине ограниченного числа спутников. Для устранения данного недостатка современная система *COSPAS-SARSAT* содержит спутники низкоорбитального сегмента (LEOSAR), спутники геостационарного сегмента (GEOSAR) и спутники среднеорбитального сегмента (MEOSAR), которые обрабатывают и/или ретранслируют сигналы, передаваемые аварийными радиобуями (рисунок 2) [5].

Наличие трех типов космических аппаратов позволяет решать следующие задачи:

- спутники геостационарного сегмента (GEOSAR) обеспечивают передачу в реальном времени в центр обработки сигналов бедствия от АРМ, содержащих данные о принадлежности радиомаяка и его координатах, полученных от спутниковой системы навигации;
- спутники низкоорбитального сегмента (LEOSAR) обеспечивают определение координат АРМ на основе эффекта Доплера, в том числе и в приполярных районах, где спутники GEOSAR не решают свои задачи;
- спутники среднеорбитального сегмента (MEOSAR) предназначены для расширения зоны действия системы, в том числе и в приполярных районах, а



также для повышения точности определения координат АРМ на основе использования многопозиционной системы наблюдения, состоящей из сети навигационных спутников, с расположенными на их борту ретрансляторами сигналов АРМ.

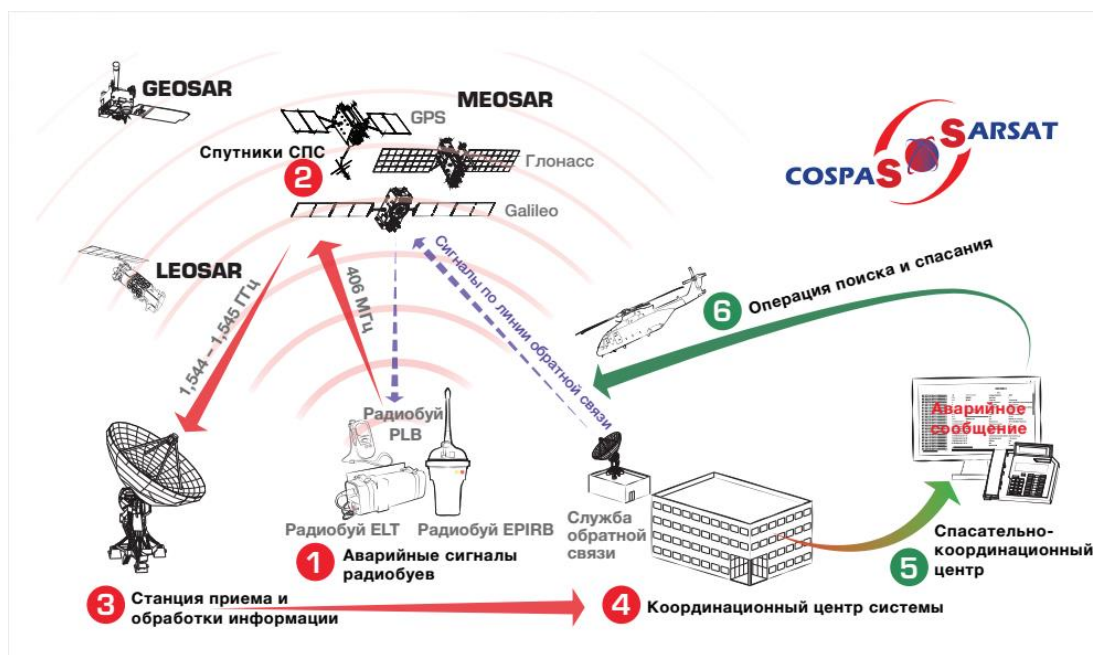


Рисунок 2. Состав и информационные потоки современной системы COSPAS-SARSAT [5]

Наряду с рассмотренными выше достоинствами системы *COSPAS-SARSAT* следует отметить и её особенности, в ряде случаев превращающиеся в её недостатки:

- геостационарный сегмент решает задачу определения координат АРМ только если в сигнале АРМ присутствует информация о его координатах;
- низкоорбитальный сегмент характеризуется значительной задержкой во времени по определению координат АРМ, что обусловлено конечным периодом обращения космического аппарата вокруг Земли и ограниченной по количеству группировкой космических аппаратов;
- среднеорбитальный сегмент требует более сложного наземного многоканального оборудования;
- с 01 февраля 2009 года прекращена спутниковая обработка сигналов АРМ на частотах 121,5/243 МГц, спутниковой группировкой выполняется прием только на частоте 406 МГц. Известно, что бортовой АРМ воздушных судов излучает аварийный сигнал на частоте 406 МГц в течении 24 часов [4]. Кроме того, следует отметить, что эта система является не национальной, а международной, что в современных политических условиях может привести к её ограниченным возможностям на территории России.

По этой причине целесообразно обосновать структуру региональной радиотехнической системы поиска транспортных средств, терпящих бедствие.

Предлагается создание гибридной системы поиска (рисунок 3), имеющей следующий состав:

- аварийные радиомаяки и аварийные радиостанции, размещенные на борту транспортного средства;
- сеть беспилотных летательных аппаратов (БЛА) различных типов с размещенной на их борту аппаратурой пеленгации сигналов АРМ 121,5/243 МГц, аппаратурой ретрансляции сигналов 406 МГц, содержащих координатную

информацию, на приемные пункты АПСС, аппаратурой приема и измерения времени прихода сигнала от АРМ для реализации разностно-дальномерного метода определения местоположения терпящего бедствие транспортного средства, аппаратуру спутниковой связи для передачи данных на борт низкоорбитальных космических аппаратов;

- сеть низкоорбитальных космических аппаратов системы «Гонец» [6], обеспечивающих передачу информации от БЛА или непосредственно в АПСС или через спутник ретранслятор, находящийся на высокой орбите, например – космический ретранслятор «Луч»;
- космический ретранслятор «Луч», обеспечивающий передачу в реальном времени результатов поиска в АПСС.

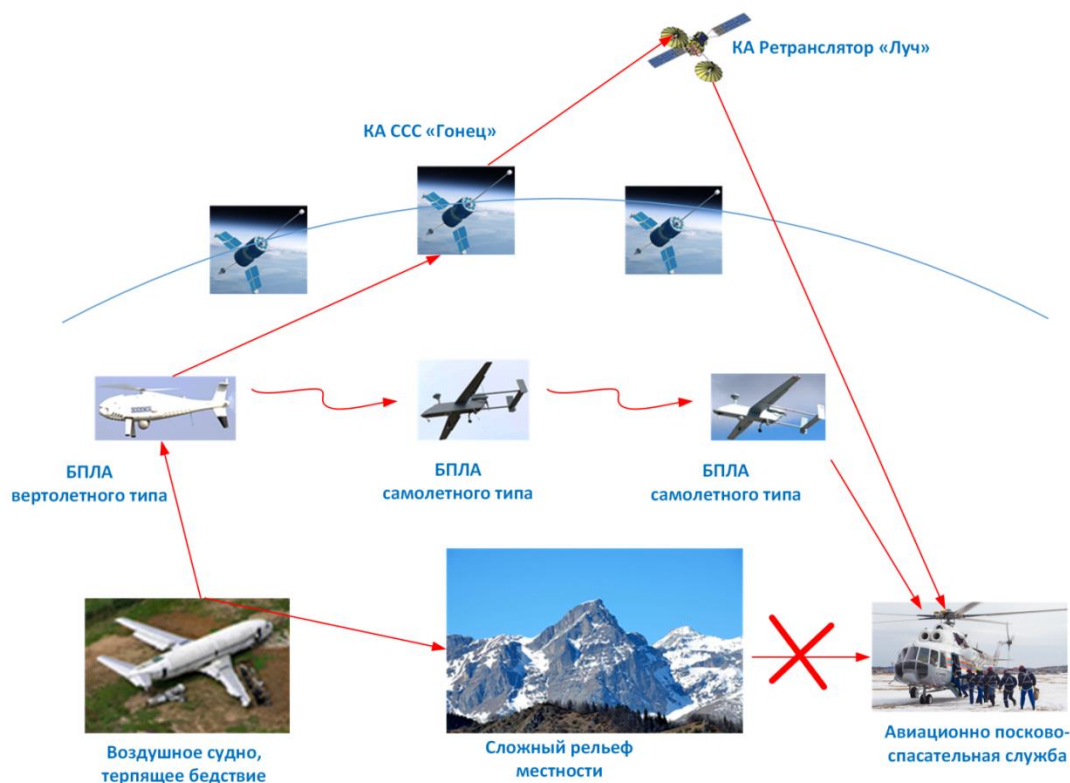


Рисунок 3. Структура современной гибридной радиотехнической системы поиска терпящих бедствия транспортных средств

Рассмотрим функционирование многопозиционной системы наблюдения (МПСН), реализованной на основе БЛА. Каждый БЛА будем рассматривать как приемную позицию МПСН,  $RS_i, i = \overline{1, N_{RS}}$ ,  $N_{RS}$  – количество БЛА. В случае обнаружения источника радиоизлучения, под которым будем понимать терпящее бедствие (рисунок 3) радиоизлучающее воздушное судно  $Trg_k, k \in \overline{1, M_{Trg}}$ , на каждой приемной позиции  $RS_i, i = \overline{1, N_{RS}}$  принимается сигнал  $S_{i,k}, i = \overline{1, N_{RS}}, k \in \overline{1, M_{Trg}}$ , где  $M_{Trg}$  – число воздушных судов, находящихся в рабочей зоне МПСН. Сигналы  $S_{i,k}$  передаются по линиям передачи данных в центр обработки, под которым будем понимать или один из БЛА, или наземный центр обработки, где определяется время их приема на соответствующем приемном пункте  $(\tau_{i,k}, i = \overline{1, N_{RS}})$  в единой шкале времени. Далее, для реализации разностно-дальномерного метода [7], вычисляется разность времен приема сигнала от  $k$  –

го воздушного объекта на  $i$ -ом приемном пункте  $(\tau_{i,k}, i = \overline{2, N_{RS}})$  и приемном пункте, принятом за опорный, например, на первом приемном пункте  $(\tau_{1,k})$ :

$$\Delta\tau_{i,1,k} = \tau_{i,k} - \tau_{1,k}. \quad (1)$$

Разностям времен  $\Delta\tau_{i,1,k}$ ,  $i = \overline{2, N_{RS}}$  соответствуют разности расстояний, проходящих сигналом от радиоизлучающего воздушного судна до каждого БЛА-приемного пункта:

$$d_{i,1,k} = c\Delta\tau_{i,1,k} = R_{t,i,k} - R_{t,1,k}, i = \overline{2, N_{RS}}, \quad (2)$$

где

$c$  – скорость распространения электромагнитной волны;

$R_{t,i,k}$  – расстояние между  $k$ -ым радиоизлучающим воздушным судном с координатами  $\mathbf{X}_{trg,k} = [x_{t,k}, y_{t,k}, z_{t,k}]^T$  и приемным пунктом  $RS_i, i \in \overline{1, N_{RS}}$ :

$$R_{t,i,k} = \sqrt{(x_i - x_{t,k})^2 + (y_i - y_{t,k})^2 + (z_i - z_{t,k})^2}. \quad (3)$$

Таким образом, можно сказать, что вектор измерений разностно-дальномерной МПСН содержит множество измерений разностей дальностей:

$$\mathbf{Z}_k(t_j) = \mathbf{Z}_k(j) = [d_{2,1,k}, d_{3,1,k}, \dots, d_{(N_{RS}-1),1,k}, d_{N_{RS},1,k}]^T, \quad (4)$$

где

$\mathbf{Z}_k(t_j)$  – вектор измерений, соответствующий  $k$ -му радиоизлучающему воздушному судну в моменты времени  $t_j, j = 1, 2, 3, \dots$

Для перехода от вектора координат вида (4), содержащему оценки разностей дальностей, к вектору прямоугольных координат  $\mathbf{X}_{t,k} = [x_{t,k}, y_{t,k}, z_{t,k}]^T$ , заданных в местной топоцентрической системе координат, центр которой совмещен, например, с местом расположения АПСС, запишем уравнения связи между элементами этих векторов:

$$\begin{aligned} d_{2,1,k} &= R_{t,2,k} - R_{t,1,k} = \sqrt{(x_2 - x_{t,k})^2 + (y_2 - y_{t,k})^2 + (z_2 - z_{t,k})^2} - \\ & - \sqrt{(x_1 - x_{t,k})^2 + (y_1 - y_{t,k})^2 + (z_1 - z_{t,k})^2}, \\ d_{3,1,k} &= R_{t,3,k} - R_{t,1,k} = \sqrt{(x_3 - x_{t,k})^2 + (y_3 - y_{t,k})^2 + (z_3 - z_{t,k})^2} - \\ & - \sqrt{(x_1 - x_{t,k})^2 + (y_1 - y_{t,k})^2 + (z_1 - z_{t,k})^2}, \\ d_{N_{RS},1,k} &= R_{t,N_{RS},k} - R_{t,1,k} = \sqrt{(x_{N_{RS}} - x_{t,k})^2 + (y_{N_{RS}} - y_{t,k})^2 + (z_{N_{RS}} - z_{t,k})^2} - \\ & - \sqrt{(x_1 - x_{t,k})^2 + (y_1 - y_{t,k})^2 + (z_1 - z_{t,k})^2}. \end{aligned} \quad (5)$$

Система уравнений (5) является нелинейной и для нахождения её корней необходимо использовать численные методы, корректность решения при этом существенно зависит от выбора начального приближения, кроме того, итерационность процедуры решения снижает оперативность нахождения оценки местоположения объекта.

С учетом этого, необходимо линеаризовать систему уравнений (5) по аналогии [7]. Представим каждое уравнение системы (5) в виде

$$R_{t,i,k} = d_{i,1,k} + R_{t,1,k}, \quad i = \overline{2, N_{RS}}, \quad (6)$$

и возведем обе части в квадрат, получим:

$$(x_i - x_1)x_{t,k} + (y_i - y_1)y_{t,k} + (z_i - z_1)z_{t,k} + d_{i,1,k}R_{t,1,k} = 0.5(R_i^2 - R_1^2 - d_{i,1,k}^2), \quad (7)$$

$$i = \overline{2, N_{RS}},$$

где

$R_i = \sqrt{x_i^2 + y_i^2 + z_i^2}$  – расстояние от  $i$ -го БПЛА-приемника до начала декартовой системы координат.

Систему (7) можно представить в матричном виде:

$$\mathbf{A}_k \mathbf{X}_k^* = \mathbf{B}_k, \quad (8)$$

где

$$\mathbf{X}_{t,k}^* = [x_{t,k}, y_{t,k}, z_{t,k}, R_{t,1,k}]^T, \quad (9)$$

$$\mathbf{A}_k = \begin{bmatrix} x_2 - x_1 & y_2 - y_1 & z_2 - z_1 & d_{2,1,k} \\ x_3 - x_1 & y_3 - y_1 & z_3 - z_1 & d_{3,1,k} \\ \vdots & \vdots & \vdots & \vdots \\ x_{N_{RS}} - x_1 & y_{N_{RS}} - y_1 & z_{N_{RS}} - z_1 & d_{N_{RS},1,k} \end{bmatrix}_{(N_{RS}-1) \times 4},$$

$$\mathbf{B}_k = 0.5 \begin{bmatrix} R_2^2 - R_1^2 - d_{2,1,k}^2 \\ R_3^2 - R_1^2 - d_{3,1,k}^2 \\ \vdots \\ R_{N_{RS}}^2 - R_1^2 - d_{N_{RS},1,k}^2 \end{bmatrix}_{(N_{RS}-1) \times 1}.$$

Из выражения (8) с использованием процедуры псевдообращения можно определить оценку вектора  $\mathbf{X}_k^*$ :

$$\widehat{\mathbf{X}}_{t,k}^* = (\mathbf{A}_k^T \mathbf{W} \mathbf{A}_k)^{-1} \mathbf{A}_k^T \mathbf{W} \mathbf{B}_k, \quad (10)$$

где

$\mathbf{W}$  – матрица весовых коэффициентов.

Так как вектор (9) является расширенным вектором координат, то для перехода к вектору оценок декартовых координат терпящего бедствие радиоизлучающего воздушного судна используем преобразование:

$$\widehat{\mathbf{X}}_{t,k} = \begin{bmatrix} \widehat{x}_{t,k} \\ \widehat{y}_{t,k} \\ \widehat{z}_{t,k} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \left( \mathbf{A}_k^T \mathbf{W} \mathbf{A}_k \right)^{-1} \mathbf{A}_k^T \mathbf{W} \mathbf{B}_k. \quad (11)$$

Дальнейшая обработка вектора  $\widehat{\mathbf{X}}_{t,k}$  может быть выполнена на основе алгоритмов динамической фильтрации [7-9].

Таким образом, на основе анализа существующей радиотехнической системы поиска и спасения терпящих бедствие транспортных средств, предложена гибридная радиотехническая система, включающая такие компоненты как сеть БЛА, оснащенных радиопеленгаторами и приемниками разностно-дальномерной системы, низкоорбитальные космические аппараты связи и высокоорбитальный спутник-ретранслятор. Применение БЛА позволит организовать поиск в труднодоступной местности, например, в ущельях, где сигналы АРМ могут быть недоступны для спутникового сегмента системы COSPAS-SARSAT. Кроме того, применение измерительной структуры на основе БЛА позволит создать адаптивную МПЧН, изменяющую свою пространственную структуру в зависимости от решаемых задач.

#### СПИСОК ЛИТЕРАТУРЫ

1. Система управления безопасностью полетов // [Электронный ресурс]. URL: <http://www.favt.gov.ru/dejatelnost-bezopasnost-poletovsubp> (дата обращения: 10.09.2023).
2. Состояние безопасности полетов в гражданской авиации государств-участников соглашения о гражданской авиации и об использовании воздушного пространства в 2020 г. // [Электронный ресурс]. URL: [https://www.МАК\\_Otchet-za-2020-ro-ВР](https://www.МАК_Otchet-za-2020-ro-ВР). (дата обращения: 09.09.2023).
3. Авиационные аварийные радиомаяки системы КОСПАС-САРСАТ. Проблемы и пути их решения // [Электронный ресурс]. URL: <http://https://ppt-online.org/86252> (дата обращения: 09.09.2023).
4. Системы связи и телекоммуникации на воздушном транспорте: учебник / под ред. Э.А. Болелова. – М.: ИД Академии Жуковского, 2020. – 160с.
5. Система Коспас-Сарсат // [Электронный ресурс]. URL: <https://cospas-sarsat.int> (дата обращения: 09.09.2023).
6. Спутниковая система «Гонец» // [Электронный ресурс]. URL: <https://gonets.ru/rus/> (дата обращения: 09.09.2023).
7. Черняк В.С. Многопозиционная радиолокация. М.: Радио и связь, 1993. – 416с.
8. Елисеев А.В., Ануфриев К.В., Погорелов Р.А., Рубайло Д.Э. Алгоритм адаптивной настройки параметров линейного дискретного фильтра с использованием нечеткой экспертной системы // *Радиотехника*. – 2019, Т.83Б №7 (9), С. 89-102.
9. Елисеев А.В. Алгоритм линейной фильтрации, устойчивый к сингулярным ошибкам // *Изв. ВУЗов. Радиоэлектроника*. – 2005, №10, – С. 20-28.

**ЛОКАЛЬНАЯ ЭЛЕКТРОЭНЕРГЕТИЧЕСКАЯ СИСТЕМА С ИСПОЛЬЗОВАНИЕМ  
ВОЗОБНОВЛЯЕМЫХ ИСТОЧНИКОВ ДЛЯ ЭЛЕКТРОСНАБЖЕНИЯ  
АВТОНОМНЫХ ОБЪЕКТОВ СВЯЗИ**

Федеральное государственное бюджетное образовательное учреждение  
высшего образования «Донской государственный технический университет»,  
г. Ростов-на-Дону, Россия<sup>1</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: электроснабжение, автономные объекты связи, потенциал возобновляемой энергии, технические требования, локальная электроэнергетическая система.

В статье рассмотрены рекомендации по созданию локальной электроэнергетической системы с использованием возобновляемых источников энергии для электроснабжения автономных объектов связи. Выполнен анализ ресурсов возобновляемых источников энергии России. Сделан вывод о целесообразности создания локальной электроэнергетической системы на основе гибридных энергетических станций с использованием энергии ветра, солнца и других видов возобновляемой энергии для электроснабжения автономных объектов связи. Сформулированы основные технические требования к проектируемой локальной электроэнергетической системе. Основные из них: бесперебойность, модульность структуры и адаптивность управления. Предложена структурная схема локальной электроэнергетической системы, удовлетворяющей указанными требованиями. Сформулированы общие принципы её функционирования, обеспечивающие экономию ресурса аккумуляторных батарей, бесперебойность и требуемое качество электроэнергии.

**N.V. Rudenko<sup>1</sup>, V.V. Ershov<sup>2</sup>, A. E. Vasiliev<sup>1</sup>**

**LOCAL ELECTRIC POWER SYSTEM USING  
RENEWABLE SOURCES FOR ELECTRIC SUPPLY  
AUTONOMOUS COMMUNICATION OBJECTS**

Federal State Educational Institution of Higher Education "Don State Technical  
University", Rostov-on-Don, Russia<sup>1</sup>

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: power supply, autonomous communication facilities, renewable energy potential, technical requirements, local electrical power system.

The article discusses recommendations for creating a local electric power system using renewable energy sources for power supply of autonomous communication facilities. An analysis of Russia's renewable energy resources was carried out. A conclusion is drawn about the feasibility of creating a local electric power system based on hybrid power plants using wind, solar and other types of renewable energy to supply power to autonomous communication facilities. The basic technical requirements for the designed local electric power system are formulated. The main ones are: uninterrupted operation, modular structure and adaptability of management. A block diagram of a local electric power system that satisfies the specified requirements is proposed. The general principles of its operation are formulated, ensuring savings in battery life, uninterrupted operation and the required quality of electricity.

## **Введение.**

Надежное функционирование инфокоммуникационных систем должно обеспечиваться бесперебойным электроснабжением. Однако развитие этих систем ограничено из-за того, что значительная часть России, около 2/3 её территории, не имеет непосредственной связи с сетями Единой или региональных электроэнергетических систем. В локальных, автономных, электроэнергетических системах используются преимущественно дизель-генераторы (ДГ), экономичность и экологичность многочисленных устаревших ДГ низки [1].

В России, большое количество населенных пунктов остается без сотовой связи, не говоря уже об интернете. Основная часть – это Сибирь и Дальний Восток. Именно там развитие сотовой связи довольно слабое, относительно центральных районов. Это касается как магистральных каналов связи с выходом в единую сеть страны, так и информационной инфраструктуры населенных пунктов [2]. Однако, главой государства был поставлен чёткий ориентир – к 2030 году довести до 97% долю домохозяйств, которым созданы возможности широкополосного доступа к интернету. Это один из основных показателей достижения национальных целей развития. [3].

В указанных регионах есть автономные объекты связи, но нет стабильного источника электроснабжения, однако в этих местах можно использовать возобновляемые источники энергии (ВИЭ). Кроме этого, необходимо учитывать тот факт, что базовые станции сотовой связи размещаются на ограниченной территории и могут быть связаны единой локальной электрической сетью.

Таким образом, разработка рекомендаций по созданию локальной электроэнергетической системы (ЛЭЭС) с использованием ВИЭ для электроснабжения автономных объектов связи (АОС) является актуальной задачей.

## **Результаты исследования.**

Анализ потенциала возобновляемой энергии России выполнен авторами в работах [4, 5, 6]. На его основе можно сделать вывод о целесообразности создания локальной электроэнергетической системы на основе гибридных энергетических станций с использованием энергии ветра, солнца и других видов возобновляемой энергии для электроснабжения автономных объектов связи. Одновременное использование различных видов альтернативной энергетики гарантируют производство достаточного количества энергии и надежность электроснабжения.

## **Предложения по выбору основных технических требований к ЛЭЭС.**

Можно сформулировать предложения по выбору основных технических требований к ЛЭЭС. К ним относятся следующие:

- обеспечение бесперебойности (это требует применения множества ВИЭ (ветроэнергетические установки (ВЭУ), солнечные энергетические установки (СЭУ), волновые электростанции (ВоЭС), миниГЭС и др. (в зависимости от конкретной территории), также использования аккумуляторных батарей (АБ));
- необходимость учета случайного характера поступления энергии от ВИЭ, также низкую плотность потока этой энергии, а также случайный характер изменения нагрузки;
- модульность структуры;
- необходимость создания системы управления на основе алгоритмов адаптивного управления в зависимости от текущих потоков энергии, текущей нагрузки и приоритета подключения нагрузки.

## **Предложение по выбору структурной схемы ЛЭЭС.**

Проведенный анализ источников [1, 7, 8] позволил предложить структурную схему ЛЭЭС, удовлетворяющую указанным требованиям (рисунок 1).



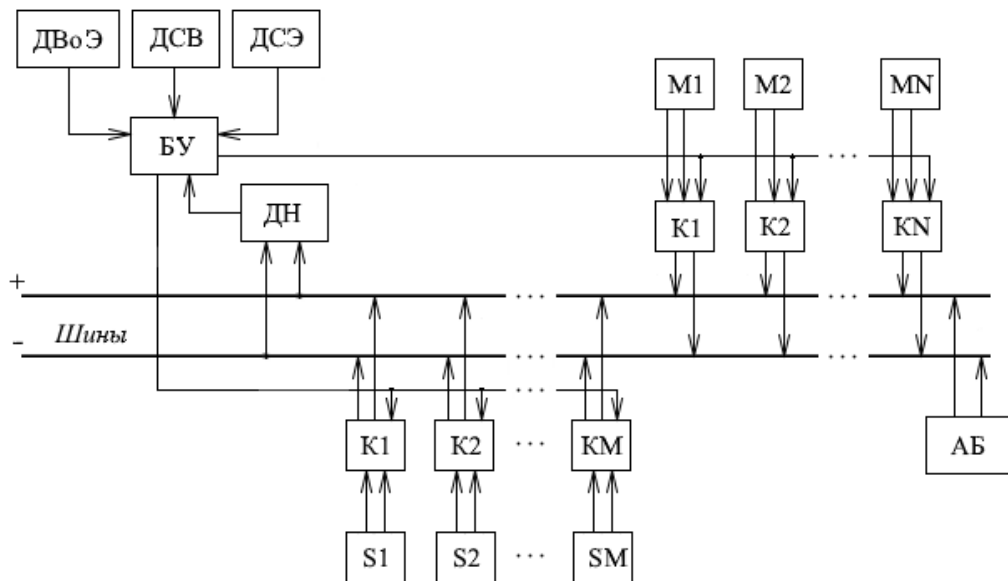


Рисунок 1. Структурная схема ЛЭЭС

ЛЭЭС содержит следующие элементы управления, на которые поступают сигналы с блока управления (БУ):

- M1, M2, ..., MN – модули ВИЭ;
- S1, S2, ..., SM – распределенная нагрузка, например, нагрузка БССС;
- K1, K2, ..., KN и K1, K2, ..., KM – ключи для коммутации элементов с шинами питания.

ЛЭЭС содержит следующие элементы обратной связи:

- ДВоЭ – датчик волновой энергии;
- ДСВ – датчик скорости ветра;
- ДСЭ – датчик солнечной энергии;
- ДН – датчик нагрузки.

Вариант структурной схемы модуля ВИЭ представлен на рисунке 2. Она содержит следующие источники энергии:

- ВоЭС – волновая электростанция;
- СБ – солнечная батарея;
- ВЭУ – ветроэнергетическая установка;
- В1 и В2 – выпрямители;
- АБ – аккумуляторная батарея.

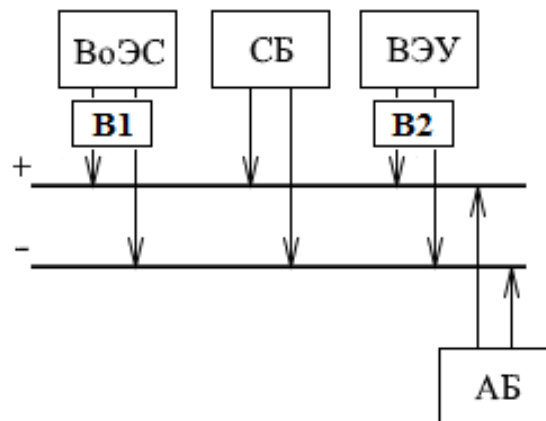


Рисунок 2. Вариант структурной схемы модуля ВИЭ (для прибрежных районов)

---

**Работа ЛЭЭС** осуществляется с учетом случайного характера нагрузки и с учетом текущих условий потоков энергии, обусловленных окружающей средой. При этом всегда выполняется баланс генерируемой мощности  $\sum P_m$  и мощности нагрузки  $\sum P_s$ , т.е.

$$\sum P_m = \sum P_s.$$

Работа ЛЭЭС осуществляется следующим образом. К шине питания подключаются нагрузка АОС. Датчик нагрузки ДН измеряет потребляемый ток, в блоке управления БУ вычисляется потребляемая мощность, а также средняя мощность, вырабатываемая модулем ВИЭ по данным с датчиков ДВоЭ, ДСВ и ДСЭ и выдаются сигналы на ключи для подключения требуемого количества модулей ВИЭ.

В случае превышения мощности нагрузки генерируемой мощности часть нагрузки отключается с учетом принятого приоритета для обеспечения условия баланса мощностей. При этом аккумуляторные батареи выбираются так, чтобы при полном отсутствии энергии ВИЭ они должны обеспечивать наиболее приоритетную нагрузку.

В случае превышения генерируемой мощности требуемой мощности нагрузки часть модулей отключается для обеспечения условия баланса мощностей. При этом достигается экономия ресурса. Бесперебойность электроснабжения обеспечивается работой аккумуляторных батарей АБ, как в отдельных модулях, так и вне их.

Таким образом, адаптивный алгоритм управления обеспечивает экономию ресурса АБ, бесперебойность и требуемое качество электроэнергии.

#### **Выводы:**

1. Анализ потенциала возобновляемой энергии России позволяет сделать вывод о целесообразности построения локальной электроэнергетической системы на основе гибридных энергетических станций с использованием энергии ветра, солнца и других видов возобновляемой энергии для электроснабжения автономных объектов связи.
2. Сформулированы основные технические требования к проектируемой локальной электроэнергетической системе. Основные из них: бесперебойность, модульность структуры и адаптивность управления.
3. Предложена структурная схема локальной электроэнергетической системы, удовлетворяющей указанными требованиями. Сформулированы общие принципы её функционирования, обеспечивающие экономию ресурса аккумуляторных батарей, бесперебойность и требуемое качество электроэнергии.

#### **СПИСОК ЛИТЕРАТУРЫ**

1. Солоницын А.Г. Локальные электроэнергетические системы с широким использованием возобновляемых источников. Автореферат диссертации на соискание ученой степени кандидата технических наук // [Электронный ресурс] URL: [www.dissercat.com/content/lokalnye-elektroenergeticheskie-sistemy-s-shirokim-ispolzovaniem-vozobnovlyaemykh-istochniko](http://www.dissercat.com/content/lokalnye-elektroenergeticheskie-sistemy-s-shirokim-ispolzovaniem-vozobnovlyaemykh-istochniko) (дата обращения 15.10.2023 г.)
2. Минвостокразвития: у 10% населения Дальнего Востока нет доступа к качественной связи // [Электронный ресурс] Рамблер / URL: <https://auto.rambler.ru/other/40531325-minvostokrazvitiya-u-10-naseleniya-dalnego-vostoka-net-dostupa-k-kachestvennoy-svyazi/> (дата обращения 15.10.2023 г.)
3. Портал Правительство России. Новости. Михаил Мишустин провёл стратегическую сессию по развитию отрасли связи до 2035 года // [Электронный ресурс] URL: <http://government.ru/news/48806/> (дата обращения 15.10.2023 г.).

4. Rudenko N.V., Ershov V.V., Evstafiev V.V. Improvement of ecological and resource-consumption properties of hybrid power supply plants of mobile base stations//Proc. International Conf. on Industrial Eng., Application. and Manufact. (ICIEAM). 16-19 May 2017, St.-Petersburg, Russia. DOI: 10.1109/ICIEAM.2017.8076240.
5. Rudenko N.V., Ershov V.V., Konshina N. Energy Conservation in High-Rise Buildings Based on Environmentally-Friendly Renewable Energy Sources // IOP Conf. Series: Earth and Environmental Science. 2019. V. 224 (1). [electronic media] // URL: <http://iopscience.iop.org/article/10.1088/1755-1315/224/1/012020/pdf> (data of application: 20.10.2023).
6. Руденко Н.В., Евстафьев В.В., Бойко Ю.Ю. Анализ возможности использования волновой энергии для электроснабжения автономных объектов связи // Труды Северо-Кавказского филиала Московского технического университета связи и информатики - Ростов-на-Дону.: ПЦ «Университет» СКФМТУСИ, 2022. С. 70-74.
7. Виноградов А.В., Сейфуллин А.Ю. Перспективные источники энергии для микросетей систем сельского электроснабжения // [Электронный ресурс] URL: <http://https://cyberleninka.ru/article/n/perspektivnye-istochniki-energii-dlya-mikrosetey-sistem-selskogo-elektrosnabzheniya> (дата обращения 15.10.2023 г.).
8. Бык Ф.Л., Мышкина Л.С. Эффекты интеграции локальных интеллектуальных энергосистем // Известия высших учебных заведений. ПРОБЛЕМЫ ЭНЕРГЕТИКИ. 2022. Т. 24. № 1. С. 3-15. doi:10.30724/1998-9903-2022-24-1-3-15.

**И.А. Алферова<sup>2</sup>, И.А. Енгибарян<sup>1</sup>, И.В. Решетникова<sup>1</sup>,  
О.А. Сафарьян<sup>2</sup>, В.И. Юхнов<sup>1</sup>**

## **ПОГРЕШНОСТЬ ФОРМИРОВАНИЯ ЧАСТОТЫ В ЦИФРОВЫХ КАНАЛАХ ПЕРЕДАЧИ ДАННЫХ, ОБУСЛОВЛЕННАЯ ЭФФЕКТОМ ДЖИТТЕРА**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Донской Государственный Технический университет, Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: гармонический сигнал, частотно-временные параметры сигналов, джиттер, нестабильность частоты сигнала.

В статье рассматриваются вопросы, связанные с влиянием джиттера на стабильность частотно-временных параметров сигнала. На примере цифровых синтезаторов частоты получены оценки, определяющие параметры джиттера (среднеквадратичного отклонения момента формирования сигнала) с абсолютной и относительной нестабильностью частоты. Приведены результаты численного моделирования, подтверждающие правильность полученных теоретических результатов и основные физические закономерности.

**I.A. Alferova<sup>2</sup>, I.A. Engibaryan<sup>1</sup>, I.V. Reshetnikova<sup>1</sup>,  
O.A. Safaryan<sup>2</sup>, V.I. Yukhnov<sup>1</sup>**

## **FREQUENCY GENERATION ERROR IN DIGITAL DATA TRANSMISSION CHANNELS DUE TO THE JITTER EFFECT**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Don State Technical University, Rostov-on-Don, Russia<sup>2</sup>

---

Keywords: harmonic signal, time-frequency parameters of signals, jitter, signal frequency instability.

The article discusses issues related to the influence of jitter on the stability of the time-frequency parameters of the signal. Using the example of digital frequency synthesizers, estimates are obtained that determine the parameters of the jitter (RMS deviation of the moment of signal formation) with absolute and relative frequency instability. The results of numerical modeling are presented, confirming the correctness of the theoretical results obtained and the basic physical laws.

Кратковременная стабильность частоты является одним из важнейших факторов, определяющих вероятность битовой ошибки при передаче информации и данных в каналах связи. Известно достаточно большое число работ, в которых анализируются вопросы влияния нестабильности частотно-временных параметров (ЧВП) сигналов на вероятность битовой ошибки в каналах связи при использовании *M-QAM* и *OFDM*-сигналов. В частности, здесь можно отметить работы [1-12]. Однако в указанных работах, как правило, не рассматриваются вопросы, связанные с причинами возникновения нестабильности частоты сигнала.

Наиболее актуальным при анализе возникновения нестабильности ЧВП сигналов является рассмотрение влияния эффектов джиттера в цифровых синтезаторах частоты на стабильность частоты формируемых сигналов. Последнее определяется все более широким использованием цифровых методов синтеза сигналов с заданными значениями частоты или изменяющихся по заданному закону.

Целью доклада является анализ взаимосвязи джиттера и нестабильности частоты в цифровых синтезаторах частоты.

Рассмотрим представление идеального сигнала в канале связи

$$V^{(0)}(t) = V_0 \cdot \cos[\omega_0(t) \cdot t + \varphi_0], \quad (1)$$

в котором  $V_0$  - заданная амплитуда сигнала;  $\omega_0(t)$  - мгновенное значение частоты в соответствии с законом ее изменения;  $\varphi_0$  - начальная фаза сигнала.

В реальном канале связи представление сигнала должно учитывать возникновение флуктуаций амплитуды, частоты и фазы от номинальных значений, определяемых требованиями к частоте несущей излучаемого сигнала, выделенной полосе частот и виду манипуляции параметров сигнала. С учетом отмеченных требований представим реальный сигнал в виде:

$$V(t) = [V_0 + \Delta V(t)] \cdot \cos[(\omega_0 + \Delta\omega(t)) \cdot t + \varphi_0 + \Delta\varphi(t)] + n_u(t), \quad (2)$$

где  $\Delta V(t)$ ,  $\Delta\omega(t)$ ,  $\Delta\varphi(t)$  описывают соответственно флуктуации амплитуды, частоты и установки начальной фазы сигнала;  $n_u(t)$  - аддитивный белый гауссовский шум (АБГШ).

При цифровом синтезе частот в заданные моменты времени  $t_k$  ( $k = 1, \dots, K$ ) формируются требуемые значения сигнала

$$V_k^{(0)} = V^{(0)}(t_k). \quad (3)$$

Требуемые значения  $V_k$  задаются с высокой точностью. Наиболее значимым

фактором, влияющим на точность формирования сигнала, является джиттер, в результате которого формирование значения  $V_k$  происходит не в момент времени  $t_k$ , а в момент времени  $t_k \pm \delta t_k$ . Графическая интерпретация влияния джиттера на формируемый сигнал приведена на рисунке 1.

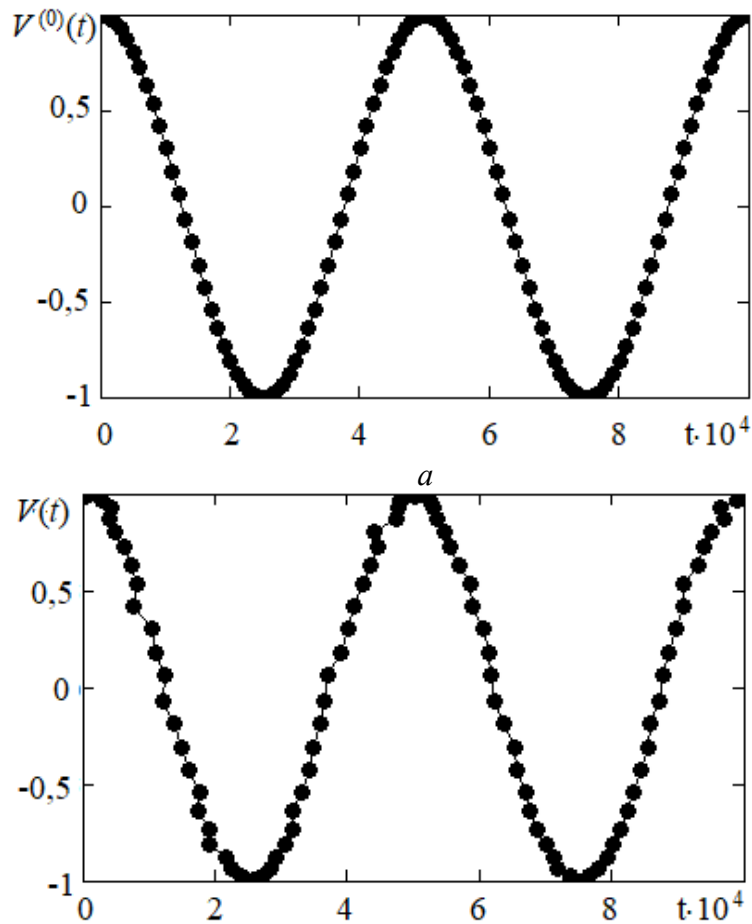


Рисунок 1. Представление формируемого сигнала:  
*a* – идеального; *б* – при наличии эффекта джиттера.

Для количественной оценки влияния эффекта джиттера представим соотношение (1) следующим образом

$$V^{(0)}(t) = V_0 \cdot \cos[\Phi_k^{(0)}], \quad (4)$$

В выражении (4)  $\Phi_k^{(0)}$ , представляющее фазу сигнала в момент времени  $t_k$ , определяется следующим образом

$$\Phi_k^{(0)} = \int_0^{t_k} \omega_0(\tau) d\tau + \varphi_0, \quad (5)$$

где  $\Phi_k^{(0)} = \int_0^{t_k} \omega_0(\tau) d\tau + \varphi_0$  - фаза сигнала в момент времени  $t_k$ .

С учетом эффекта джиттера данное значение сигнала будет сформировано в момент

времени  $t_k \pm \delta t_k$ . Таким образом, значение фазы сигнала будет получено не в момент времени  $t_k$ , а в момент времени  $t_k \pm \delta t_k$ . Это позволяет представить приращение фазы на интервале  $[t_{k-1}, t_k]$  в виде

$$\Delta\Phi_k^{(0)} = \int_{t_{k-1}}^{t_k} \omega_0(\tau) d\tau. \quad (6)$$

Мгновенное значение частоты определяется соотношением

$$\omega(t) = \frac{\int_{t_{k-1}}^{t_k} \omega_0(\tau) d\tau}{t_k - t_{k-1} \pm \delta t_k \pm \delta t_{k-1}}. \quad (7)$$

При условии  $\delta t_k \ll t_k - t_{k-1}$  и  $\delta t_{k-1} \ll t_k - t_{k-1}$  (указанное условие всегда выполняется на практике) выражение (7) может быть линеаризовано и приведено к виду

$$\omega(t) = \omega_0(t) \cdot \left( 1 \mp \frac{\delta t_k}{t_k - t_{k-1}} \mp \frac{\delta t_{k-1}}{t_k - t_{k-1}} \right), \quad t \in [t_{k-1}, t_k] \quad (8)$$

Соотношение (8) является основным для анализа взаимосвязи параметров джиттера (математического ожидания и среднеквадратического отклонения) с параметрами нестабильности частоты формируемого сигнала.

Соотношение (8) позволяет оценить статистические характеристики мгновенного значения частоты  $\omega(t)$  и связать их с параметрами джиттера. Будем считать, что случайные значения  $\delta t_k$  подчиняются нормальному закону распределения [13-19]

$$p(\delta t_k) = \frac{1}{\sqrt{2\pi D_{\delta t}}} \exp\left(-\frac{(\delta t_k)^2}{2D_{\delta t}}\right), \quad (9)$$

где  $D_{\delta t}$  - дисперсия случайной величины  $\delta t_k$ .

Кроме того, предположим, что значения случайной величины представляют случайный процесс, любые два значения которого являются некоррелированными.

Математическое ожидание мгновенного значения частоты  $\omega(t)$  определим следующим выражением

$$M[\omega(t)] = M\left[\omega_0(t) \cdot \left( 1 \mp \frac{\delta t_k}{t_k - t_{k-1}} \mp \frac{\delta t_{k-1}}{t_k - t_{k-1}} \right)\right], \quad t \in [t_{k-1}, t_k], \quad (10)$$

где  $M[\square]$  - обозначение операции нахождения математического ожидания случайной величины.

Случайный характер распределения имеют только  $\delta t_k$  и  $\delta t_{k-1}$ . Это позволяет преобразовать формулу (10) к виду [20]

$$M[\omega(t)] = \omega_0(t) \cdot \left( 1 \mp \frac{M[\delta t_k]}{t_k - t_{k-1}} \mp \frac{M[\delta t_{k-1}]}{t_k - t_{k-1}} \right), \quad t \in [t_{k-1}, t_k]. \quad (11)$$

С учетом принятого закона распределения (9) получаем, что  $M[\omega(t)] = \omega_0(t)$ , т.е. среднее значение частоты  $\omega(t)$  совпадает с заданным значением.

Дисперсия значений частоты формируемого сигнала определяется с учетом последнего результата с использованием следующего выражения

$$D[\omega(t)] = M \left[ \omega_0^2(t) \cdot \left( \mp \frac{\delta t_k}{t_k - t_{k-1}} \mp \frac{\delta t_{k-1}}{t_k - t_{k-1}} \right)^2 \right], \quad t \in [t_{k-1}, t_k]. \quad (12)$$

Преобразуя выражение (11), запишем

$$D[\omega(t)] = \omega_0^2(t) \cdot \left[ \frac{M[(\delta t_k)^2]}{(t_k - t_{k-1})^2} + \frac{M[(\delta t_{k-1})^2]}{(t_k - t_{k-1})^2} \pm 2 \frac{M[\delta t_k \cdot \delta t_{k-1}]}{(t_k - t_{k-1})^2} \right], \quad t \in [t_{k-1}, t_k]. \quad (13)$$

Числители первых двух слагаемых в правой части выражения (12) представляют собой дисперсии случайных значений, связанных с джиттером. Третье слагаемое в правой части (12) равно нулю с учетом некоррелированности значений случайного процесса, описывающего джиттер в устройстве формирования сигналов. Таким образом, взаимосвязь дисперсии частоты формируемого сигнала с параметрами джиттера можно представить в виде

$$D[\omega(t)] = \omega_0^2(t) \cdot \left[ \frac{D[(\delta t_k)]}{(t_k - t_{k-1})^2} + \frac{D[(\delta t_{k-1})]}{(t_k - t_{k-1})^2} \right], \quad t \in [t_{k-1}, t_k]. \quad (14)$$

Считая, что параметры джиттера являются стационарными, т.е.  $D[(\delta t_k)] = D_{\Delta t}$ ,  $k = 1, \dots, K$ , получаем

$$D[\omega(t)] = 2\omega_0^2(t) \cdot \frac{D_{\Delta t}}{(t_k - t_{k-1})^2}, \quad t \in [t_{k-1}, t_k]. \quad (15)$$

Приведенное значение в общем случае полностью определяет взаимосвязь погрешности формирования частоты в цифровых каналах передачи данных, обусловленной эффектом джиттера, с параметрами самого джиттера.

На рисунке 2 для частного случая формирования гармонических сигналов приведена зависимость допустимой величины джиттера от частоты  $\omega_0$ . При проведении исследований допустимая погрешность формирования сигнала принималась равной  $10^{-6}$ .



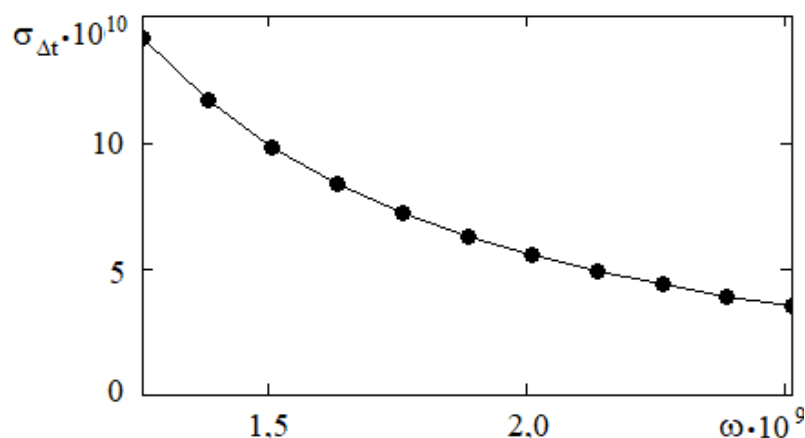


Рисунок 1. Представление формируемого сигнала:  
*a* – идеального; *б* – при наличии эффекта джиттера.

Приведенная зависимость погрешности формирования частоты от сигнала от частоты показывает квадратичную зависимость уменьшения величины джиттера с ростом частоты. Кроме того, приведенные результаты показывают допустимые значения джиттера, которые составляют единицы наносекунд.

#### СПИСОК ЛИТЕРАТУРЫ

1. Джулиан Данн. Джиттер. Теория. Часть 1 // <https://www.ixbt.com/proaudio/jitter-theory-part1.shtml>.
2. Бакланов И.Г., Лебедев А.Г., Сондак С.Ю. Несколько серьезных слов о джиттере // Метрология и измерительная техника в отрасли связб. №2, 2005.
3. Исследование влияния джиттера тактового сигнала на цифро-аналоговое преобразование. *AdvanteX Research Lab, 2004*. Теоретические основы и результаты эксперимента.
4. Сергиенко А. Б. Цифровая обработка сигналов. [Текст] – СПб.: Питер, 2003. – 604 с.: ил.
5. Ричард Лайонс. Цифровая обработка сигналов: Второе издание. Пер. с англ. [Текст] – М.: ООО «Бином-Пресс», 2006 г. – 656с.: ил.
6. Гуменюк А.С., Бочаров Ю.И. Устройства выборки-хранения быстродействующих АЦП. [Текст] Микροэлектроника, 2007, том 36, №5, с. 390-400.
7. Мерфи Е., Слеттери К. Все о синтезаторах DDS. [Текст] Пер. с англ.
8. Власенко А. // Компоненты и технологии. 2005. № 1. 32с.
9. Галкин В.А. Цифровая мобильная радиосвязь. [Текст] - М.: Горячая линия-Телеком, изд. 2-е, 2012.
10. Кестер У. Аналого-цифровое преобразование. [Текст] - М.: Техносфера, 2007.
11. Carlos Azeredo-Leme, Clock Jitter Effect on Sampling. IEEE Circuits and systems magazine. 2011, pp. 26-37.
12. Юхнов В.И., Енгибарян И.А., Сафарьян О.А., Пилипенко И.А. Аналитические зависимости для оценок отклонения частоты и длительности формируемых сигналов в информационно телекоммуникационных системах. Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 59-62.
13. Сафарьян О.А., Алферова И.А., Енгибарян И.А., Юхнов В.И. Стабилизация частоты на основе первично-фундаментальных свойств больших систем. Научные технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 26-32.
14. Dai L., Harjani R. CMOS Switched-Op-Amp-Based Sample-and-Hold Circuit // IEEE J. Solid-State Circuits. 2000. V. 35. № 1. P. 109-113.

- 
15. Исследование влияния джиттера тактового сигнала на цифро-аналоговое преобразование. Теоретические основы и результаты эксперимента.// Advantex Research Lab, 2004.
  16. T. M. Fortier, C. W. Nelson, A. Hati, F. Quinlan, J. Taylor, H. Jiang, C. W. Chou, T. Rosenband, N. Lemke, A. Ludlow, D. Howe, C. W. Oates, and S. A. Diddams. Sub-femtosecond absolute timing jitter with a 10 GHz hybrid photonic-microwave oscillator // Applied physics letters. 2012. № 100.
  17. Bar-Giora Goldberg, The Effects of Clock Jitter on Data Conversion Devices. *RF Design*, August 2002, pp. 26-32, <http://www.rfdesign.com>.
  18. Joseph V. Adler. Clock-Source Jitter: A Clear Understanding Aids Oscillator Selection. *EDN*, February 18, 1999, pp. 79-86, <http://www.ednmag.com>.
  19. Neil Roberts. Phase Noise and Jitter – A Primer for Digital Designers. *EEDesign*, July 14, 2003, <http://www.eedesign.com>.
  20. Корн Г., Корн Т. Справочник по математике (для научных сотрудников и инженеров). – М.: Наука. Гл. ред. физ.-мат. лит., 1977. – 832 с.

**И.А. Алферова<sup>2</sup>, Ю.Д. Безуглов<sup>1</sup>, И.А. Енгибарян<sup>1</sup>,  
О.А. Сафарьян<sup>2</sup>, В.И. Юхнов<sup>1</sup>**

### **ВЛИЯНИЕ НЕСТАБИЛЬНОСТИ ЧАСТОТЫ НА ВЕРОЯТНОСТЬ БИТОВОЙ ОШИБКИ ПРИ ПЕРЕДАЧЕ М-КАМ-СИГНАЛОВ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Донской Государственный Технический университет, Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: радиоэлектронная система, М-КАМ-сигналы, стабильность частоты сигнала, вероятность битовой ошибки.

В докладе рассматриваются вопросы, связанные с влиянием долговременной и кратковременной нестабильности несущей частоты и частоты гетеродина на вероятность битовой ошибки при передаче М-КАМ-сигналов. Показано, что как долговременная, так и кратковременная нестабильность частоты приводит к уменьшению отношения сигнал/шум на выходе корреляционного устройства и соответственно к «размыванию» положения точки сигнального созвездия, соответствующей сигналу. Кроме того, долговременная нестабильность частоты приводит к повороту сигнального созвездия на угол, величина которого определяется как величиной рассогласования частот принимаемого сигнала, так и длительностью импульса. Совокупное влияние указанных факторов приводит к росту вероятности битовой ошибки, зависящему от величины и дисперсии отклонения частоты сигнала и основания кода используемого М-КАМ-сигнала. Приведены результаты математического моделирования, подтверждающие правильность полученных теоретических результатов и основные отмеченные закономерности.

## THE EFFECT OF FREQUENCY INSTABILITY ON THE PROBABILITY OF BIT ERROR IN THE TRANSMISSION OF M-CAM SIGNALS

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Don State Technical University, Rostov-on-Don, Russia<sup>2</sup>

**Keywords:** electronic system, M-CAM signals, signal frequency stability, probability of bit error.

The report discusses issues related to the influence of long-term and short-term instability of the carrier frequency and the frequency of the heterodyne on the probability of bit error in the transmission of M-CAM signals. It is shown that both long-term and short-term frequency instability leads to a decrease in the signal-to-noise ratio at the output of the correlation device and, accordingly, to a «blurring» of the position of the signal constellation point corresponding to the signal. In addition, long-term frequency instability leads to a rotation of the signal constellation by an angle, the magnitude of which is determined both by the magnitude of the frequency mismatch of the received signal and the duration of the pulse. The combined influence of these factors leads to an increase in the probability of a bit error, depending on the magnitude and variance of the deviation of the signal frequency and the basis of the code of the M-CAM signal used. The results of mathematical modeling are presented, confirming the correctness of the theoretical results obtained and the main patterns noted.

В настоящее время для обеспечения передачи сигналов между объектами, в частности, взаимодействия пилотируемых летательных аппаратов (ПЛА) и наземной структурой сетей передачи данных обслуживающих организаций широко применяются каналы различных частотных диапазонов. Использование указанных каналов позволяет абонентскому оборудованию объекта функционировать в мобильном режиме связи. В этом случае абонент представляет собой удаленный элемент некоторой внутренней системы передачи цифровых данных. Технической основой такой организации обмена данными являются каналы, в том числе и радиоканалы, передачи сигналов. Широкое распространение при организации высокоскоростных, устойчивых к воздействию внешних неблагоприятных факторов находят М-КАМ-сигналы [1-3].

Наиболее неблагоприятными факторами, приводящими к снижению скорости передачи данных, увеличению вероятности битовой ошибки, являются долговременная и кратковременная нестабильность частоты. Так, в настоящее время относительная нестабильность частоты характеризуется значениями  $10^{-8}$  –  $10^{-9}$  и выше [3, 4]. Указанные значения нестабильности частоты удовлетворяют, как правило, большинству практических приложений. Однако с внедрением сетей 5 G и 6 G требования к стабильности частоты будут только возрастать, что определяется использованием М-КАМ сигналов с более высоким значением основания алфавита, обеспечивающим повышение скорости передачи данных. При этом с увеличением плотности расположения абонентов и повышения их мобильности будут усиливаться массогабаритные ограничения на используемую аппаратуру связи [5-15]. Отмеченные тенденции, заключающиеся в повышении требований к стабильности частоты сигналов и ограничений на массогабаритные параметры аппаратуры мобильных терминалов, определяют актуальность темы доклада.

Целью доклада является анализ влияния нестабильности частоты на вероятность битовой ошибки при передаче М-КАМ-сигналов.

Представим синфазную и квадратурную составляющие принимаемого высокочастотного сигнала на входе устройства корреляционной обработки следующим образом [16-21]

$$\begin{aligned} s_I &= s_I^{(0)} \cdot \cos \left[ (\omega_0 + \Delta\omega) \cdot t + \varphi_0^{(I)} \right] + \zeta_I, \\ s_Q &= s_Q^{(0)} \cdot \sin \left[ (\omega_0 + \Delta\omega) \cdot t + \varphi_0^{(Q)} \right] + \zeta_Q, \end{aligned} \quad (1)$$

где  $s_I^{(0)}$  и  $s_Q^{(0)}$  - амплитуды синфазной и квадратурной составляющих сигнала соответственно;  $\Delta\omega$  - отклонение частоты сигнала, обусловленное нестабильностью частоты сигнала;  $\varphi_0^{(I)}$  и  $\varphi_0^{(Q)}$  - начальные фазы синфазной и квадратурной составляющих сигнала, определяемые передаваемой в данном бите информацией, соответственно;  $\zeta_I$  и  $\zeta_Q$  - аддитивный белый гауссовский шум (АБГШ) в синфазном и квадратурном каналах соответственно.

Будем считать, что аппаратура синфазного и квадратурного каналов идентична, что позволяет в выражении (1) при дальнейшем рассмотрении ограничиться условием  $\varphi_0^{(I)} = \varphi_0^{(Q)} = \varphi_0$ .

На выходе устройства корреляционной обработки, в котором проводится перемножение синфазной и квадратурной составляющих с соответствующим сигналом гетеродина, и последующая низкочастотная фильтрация, формируются синфазная и квадратурная составляющие на промежуточной частоте

$$\begin{aligned} v_I &= v_I^{(0)} \cdot \cos \Delta\varphi - v_Q^{(0)} \cdot \sin \Delta\varphi + \zeta_I, \\ v_Q &= v_Q^{(0)} \cdot \cos \Delta\varphi + v_I^{(0)} \cdot \sin \Delta\varphi + \zeta_Q, \end{aligned} \quad (2)$$

где  $v_I^{(0)}$  и  $v_Q^{(0)}$  - амплитуды синфазной и квадратурной составляющих сигнала на выходе устройства корреляционной обработки соответственно;  $\Delta\varphi = \int_0^T \Delta\omega(\tau) d\tau + \varphi_0$ , в котором  $\int_0^T \Delta\omega(\tau) d\tau$  - составляющая изменения фазы сигнала при корреляционной обработке, обусловленное нестабильностью частоты сигнала в течение импульса  $T$ .

Представим отклонение частоты  $\Delta\omega(\tau)$  в виде двух слагаемых, первое из которых  $\Delta\omega_1(\tau)$ , обусловленное долговременной нестабильностью, имеет постоянное значение на интервале передачи/приема всего сигнала, второе  $\Delta\omega_2(\tau)$ , обусловленное кратковременной нестабильностью, является постоянным в течение импульса, но меняет свои значения случайным образом между импульсами.

Рассмотрим проявление долговременной нестабильности частоты. На первом этапе пренебрежем влиянием шумовых составляющих  $\zeta_I$  в синфазной и  $\zeta_Q$  квадратурной составляющих. Выделение информационной составляющей посылки, передаваемой с использованием М-КАМ-модуляции, проводится путем сравнения в решающем устройстве оценки фазы принятого сигнала со значениями фаз посылок, образующих алфавит.

Появление дополнительного слагаемого сигналов  $\Delta\varphi_1 = \int_0^T \Delta\omega(\tau) d\tau$  может приводить к возникновению неправильной демодуляции принятого сообщения.

Пусть на передающей стороне сформирована информационная посылка, которой соответствует начальная фаза сигнала  $\varphi_{nep}^{(m)}$ , ( $m=1, \dots, M$ ). Правильной демодуляции соответствует, как показано в работах [21-27], получение оценки фазы сигнала  $\varphi_{np}^{(m)}$ , значение которой удовлетворяет условию

$$|\varphi_{np}^{(m)} - \varphi_{nep}^{(m)}| < 2\pi/M, \quad (m=1, \dots, M). \quad (3)$$

Ошибка демодуляции возникает при нарушении указанного условия, что может быть записано следующим образом

$$|\varphi_{np}^{(m)} - \varphi_{nep}^{(m)}| \geq 2\pi/M. \quad (4)$$

При этом, если  $\varphi_{np}^{(m)} - \varphi_{nep}^{(m)} \geq 2\pi/M$ , то переданная  $m$ -я комбинация будет принята как  $(m+1)$ -я комбинация. В случае  $|\varphi_{np}^{(m)} - \varphi_{nep}^{(m)}| \leq -2\pi/M$  переданная  $m$ -я комбинация будет принята как  $(m-1)$ -я комбинация.

Условие, при котором долговременная нестабильность сигнала не приводит к возникновению ошибки демодуляции, определяется следующим выражением

$$\Delta\omega \cdot T \leq 2\pi/M, \quad (5)$$

что эквивалентно следующему ограничению на величину отклонения частоты

$$\Delta\omega \leq \frac{2\pi}{T \cdot M}, \quad (6)$$

Выражение (6) определяет допустимое значение долговременной нестабильности частоты сигнала. Геометрическая интерпретация указанных условий для случая сигнала 8PSK приведена на рисунке 1. Символами  $\bullet$  показаны элементы сигнального созвездия при отсутствии отклонений частоты, символами  $\odot$  - при наличии отклонения частоты. Наличие сдвига фазы обуславливает, как приведено на рисунке 1, поворот сигнального созвездия на угол  $\Delta\varphi_1$ .

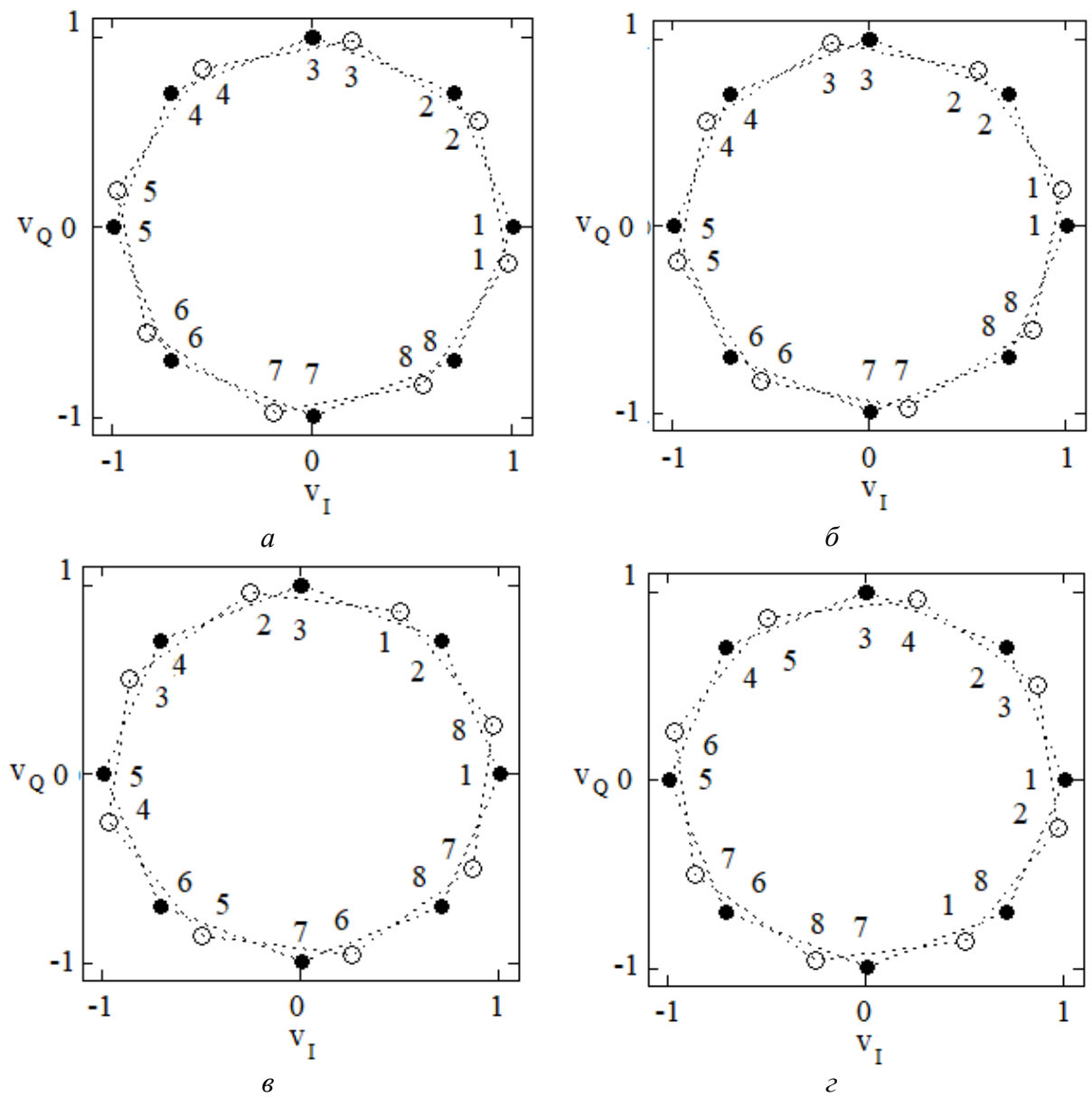


Рисунок 1. Созвездия 8PSK-сигнала:  
*a* -  $\Delta\varphi_1 = \pi/16$ ; *б* -  $\Delta\varphi_1 = -\pi/16$ ; *в* -  $\Delta\varphi_1 = \pi/6$ ; *г* -  $\Delta\varphi_1 = -\pi/16$ .

Наличие сдвига фазы обуславливает, как приведено на рисунке 1, поворот сигнального созвездия на угол  $\Delta\varphi_1$ , в зависимости от величины которого возможно появление ошибок демодуляции. Необходимо отметить, что долговременная нестабильность частоты одинаково проявляется при передаче всех бит информационной посылки.

При анализе влияния кратковременной нестабильности частоты вновь воспользуемся соотношениями (3)-(6). Однако принципиальным отличием является то, что отклонение частоты  $\Delta\omega$ , в отличие от долговременной составляющей, принимает случайные значения. С учетом этого при приеме информационных сообщений может наблюдаться как событие (3), так и событие (4), т. е. как правильная, так и неправильная демодуляция принятого сообщения.

Для анализа влияния кратковременной нестабильности частоты на передачу М-КАМ-сигналов рассмотрим наиболее широко распространенный на практике случай, при котором отклонения частоты  $\Delta\omega$  подчиняются нормальному закону распределения

$$p(\Delta\omega) = \frac{1}{\sqrt{2\pi \cdot D_{\Delta\omega}}} \exp\left(-\frac{\Delta\omega^2}{2D_{\Delta\omega}}\right), \quad (7)$$

где  $D_{\Delta\omega}$  - дисперсия случайного процесса, описывающего кратковременную нестабильность частоты.

С учетом соотношений (6) и (7) вероятность ошибочного приема  $P_{ош}$  может быть представлена, как вероятность, что величина  $\Delta\omega$  превысит значение  $2\pi/(T \cdot M)$ . Последнее условие может быть представлено в виде

$$P_{ош} = \frac{2}{\sqrt{2\pi \cdot D_{\Delta\omega}}} \int_{2\pi/(T \cdot M)}^{+\infty} \exp(-\Delta\omega^2/2D_{\Delta\omega}) d(\Delta\omega). \quad (8)$$

На рисунке 2 приведены зависимости  $P_{ош}$  для различных значений дисперсии частоты сигнала при частоте несущей сигнала 1 ГГц.

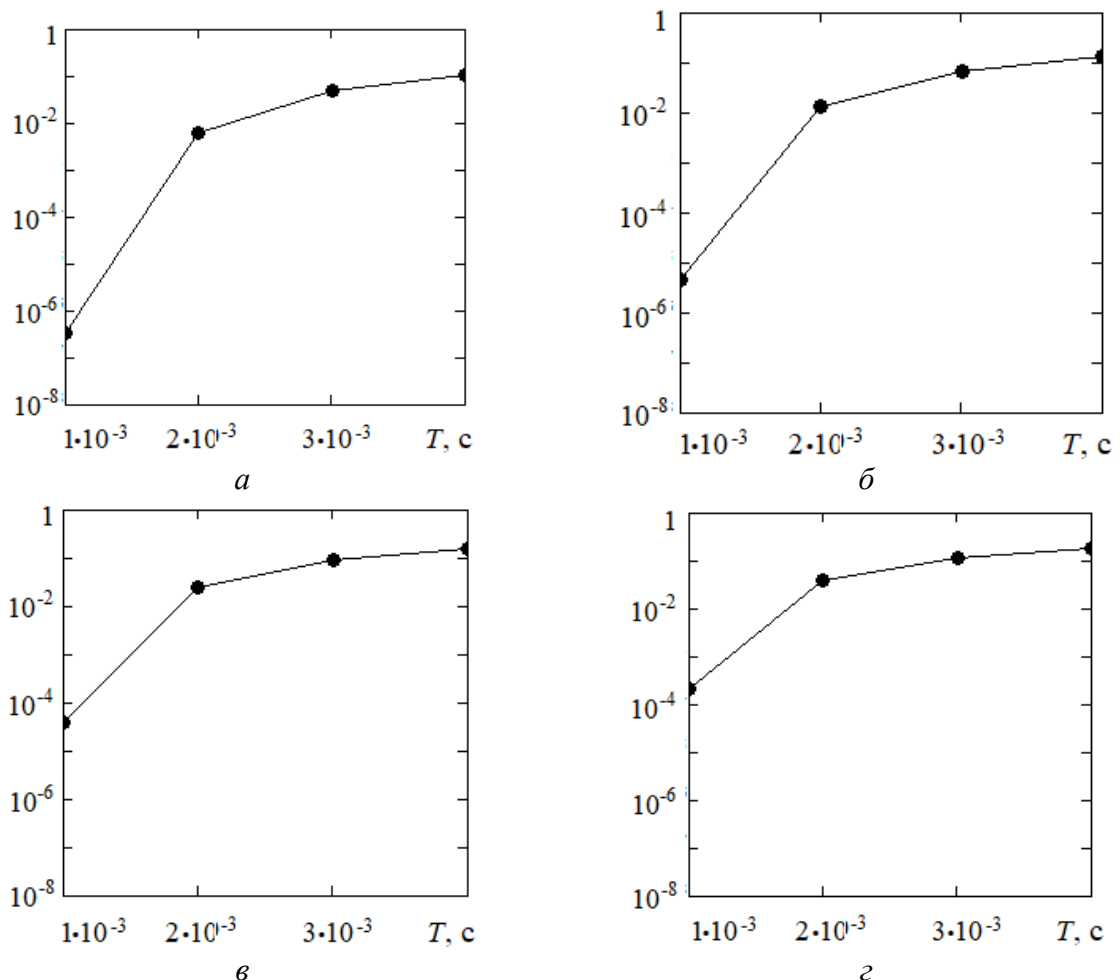


Рисунок 2. Зависимость  $P_{ош}$  от длительности импульса:

$a - D_{\Delta\omega} = 10^4$ ;  $б - D_{\Delta\omega} = 2 \cdot 10^4$ ;  $в - D_{\Delta\omega} = 3 \cdot 10^4$ ;  $г - D_{\Delta\omega} = 4 \cdot 10^4$ .

Приведенные результаты имеют простую физическую трактовку. С увеличением нестабильности частоты сигнала и соответственно дисперсии, увеличивается вероятность появления в случайном процессе значений частоты сигнала, превышающих границу

---

$2\pi/(T \cdot M)$ ). Кроме того, можно отметить, что с увеличением длительности импульса значение частоты, при котором происходит ошибка демодуляции принятого сообщения, уменьшается.

Приведенные результаты показывают:

Влияние как долговременной, так и кратковременной нестабильности частоты сигнала с математической точки зрения описывается одними и теми же соотношениями. Влияние обоих факторов проявляется в ошибке демодуляции.

Однако для долговременной нестабильности частоты, проявляющейся на временных интервалах более суток, характерным является появление ошибок демодуляции для всех принимаемых информационных посылок. В случае кратковременной нестабильности частоты, проявляющейся на интервалах длительностью единицы секунд, величина отклонения частоты принимает случайные значения. Такой характер поведения отклонения частоты приводит к тому, что ошибка демодуляции наблюдается не для всех, а только для части битов передаваемой информации.

Результаты моделирования показали, что вероятность битовой ошибки, обусловленная кратковременной нестабильностью частоты, возрастает как с увеличением длительности импульсов, так и основания кода М-КАМ-сигналов.

#### СПИСОК ЛИТЕРАТУРЫ

1. *Глотов А.Ф.* Интеллектуализация информационных систем: подходы и направления.// «Геоматика»-2015, с.18-24.
2. *David B. Lesson.* Oscillator Phase Noise: A 50-Year Review // IEEE Transactions on Ultrasonics, Ferroelectrics and Frequencies control.-2016, № 8. p. 1208-1225.
3. *Demir, A. Mehrotra, J. Roychowdhure.* Phase noise in oscillators: A unifying theory and numerical methods for characterization // IEEE Trans. Circuits Syst. I. Fundam. Theory Appl., May 2000, vol. 47, no. 5, p. 655-674.
4. *Zheng T., Chen L., Chen T., Wei S.M.,* Virtual synchronous generator technology and prospects// Autom. Electric Power Syst. -2015, № 39 (21) p.165–175.
5. *Shao H., Li P., Fu W.B., Yang G.H.,* Wind-solar grid-connected technology based on virtual synchronous generator control strategy// Electr. Autom. – 2018, № 40 (5) p.16–18.
6. *Ling Y.L.,* Adaptive control of distributed power inverter based on VSG// Energy Conserv. – 2020 № 39 (4) p. 5–9.
7. *Ren D.J., Wei Y.B., Xi Z.F., Zhang J.,* Control strategy of inverter power sharing based on VSG// Power Electron. Technol – 2020, №54 (2) p. 28–31.
8. *Huo X.X., Wu P., Huang X., Yan J.J., Wang K.Y., Xu K., Yao C., Chen P.Y.,* Microgrid Stability Control Based on Adaptive Parameter Virtual Synchronous Machine// Electric Power Construct - 2019, № 40 (2), p. 79–86.
9. *Cheng G., Shao X., Wang G.,* Adaptive control strategy for virtual synchronous generator parameters// Renewable Energy - 2021, № 39 (12) p.1655–1661.
10. *Lu Z., Sheng W., Zhong Q., Liu H., Zeng Z.,* Virtual synchronous generator and its applications in micro-grid// Proc. CSEE - 2014, № 34 (16) p.2591–2603.
11. *Zhao D.M., Zhang N., Liu Y.H., Zhang X.,* Integrated control strategy for smooth switching of microgrid and island operation mode based on energy storage// Power Syst. Technol - 2013, № 37 (2),p.301–306.
12. *Li P., Zhang X.S., Zhao B., Wang Z.L., Sun J.R.,* Microgrid design and mode switching control strategy of multi-microgrid and multi-grid point structure// Autom. Electric Power Syst. - 2015, № 39 (9), p.172–178.
13. *Wang J.S., Tang C.H., Chen N., Tan K., Mao J.X.,* A microgrid on-off and off-grid smooth switching control strategy based on self-recognition of operating mode// Autom. Electric Power Syst - 2015, № 39 (9), p.185–191.



- 
14. *Yang Y.C., Zhou Z.G.*, Distributed power grid-connected inverter seamless switching control strategy// *J. Electric Power Syst. Autom.* - 2016, № 28 (8), p.91–97.
  15. *Shi R.L., Zhang X., Xu H.Z., Liu F., Hu C., Yu Y.*, Seamless switching control strategy of microgrid operation mode based on virtual synchronous generator// *Autom. Electric Power Syst.* - 2016, №40 (10), p. 16–23.
  16. *Wang C.S., Xiao Z.X., Wang S.X.*, Integrated control and analysis of microgrid// *Autom. Electric Power Syst* - 2008, № 7, p.98–103.
  17. *Bai W., Liu L.Q., Zhang C.M., Ma L.Q.*, Seamless switching control technology of virtual synchronous generator// *Autom. Instrument* - 2017, №38 (12), p. 13–17.
  18. *Gu B.S., Wang J.H., Luo F.F., Ji Z.D., Lv Z.P., Gu W., Wang T.*, Three phase four leg virtual synchronous generator pre synchronization, multi loop control and load imbalance control method// *Acta Electrotech. Sinica* - 2017, №32 (S1) p. 138–150.
  19. *Wan X.F., Zhan Z.L., Liao Z.P., Xi R.X.*, Research on seamless switching strategy of virtual synchronous generator on and off grid// *J. Electron. Measure. Instrument* - 2018, №32 (5) p.33–40.
  20. *Ji Y., Su J., Ding B.*, Microgrid inverter VSG off-grid switching and fault handling// *Control Eng* - 2021, № 28 (7), p.1496–1504.
  21. *Li B., Zhou L., Yu X.R., Zheng C., Liu J.H.*, A microgrid inverter secondary frequency modulation scheme based on improved virtual synchronous generator algorithm// *Power Syst. Technol* - 2017, №41 (8), p/ 2680–2687.
  22. *Safaryan O.A., Pilipenko I.A., Boldyrikhin N.V., Yukhnov V.I.*, Multidimensional likelihood function in the problem of estimating time-frequency parameters of signals// *Conference Proceedings - 2021 Radiation and Scattering of Electromagnetic Waves, RSEMW 2021*, pp. 393-396
  23. *Safaryan O.A., Pilipenko I.A., Saharov I.A.*, Features of Frequency Generators Stabilization in Distributed Information-Measuring Systems// *Conference Proceedings - 2019 Radiation and Scattering of Electromagnetic Waves, RSEMW 2019* - 2019, pp. 208-211.
  24. *Сафарьян О.А., Алферова И.А., Енгибарян И.А., Юхнов В.И.* Стабилизация частоты на основе первично-фундаментальных свойств больших систем. *Научно-технические технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 26-32.*
  25. *Сафарьян О.А., Пилипенко И.А.* Метод оценивания параметров стабильности генераторов // *РАДИОЛОКАЦИЯ, НАВИГАЦИЯ, СВЯЗЬ / сборник трудов XXVI Международной научно-технической конференции: в 6 т. Воронеж - 2020, с.204-211.*
  26. *Юхнов В.И., Енгибарян И.А., Сафарьян О.А., Пилипенко И.А.* Аналитические зависимости для оценок отклонения частоты и длительности формируемых сигналов в информационно телекоммуникационных системах. // *Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 59-62.*
  27. *Safaryan O.A., Pilipenko I.A.*, Prerequisites and Theoretical Foundations of the Statistical Method of Frequency Stabilization in Information and Telecommunication Systems// *Electronics* - 2022, №11(18), p 1-9.

## **ВЛИЯНИЕ КРАТКОВРЕМЕННОЙ НЕСТАБИЛЬНОСТИ ЧАСТОТЫ НА ОТНОШЕНИЕ СИГНАЛ/ШУМ В КАНАЛАХ СВЯЗИ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Донской Государственный Технический университет, Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: сигнал, отношение сигнал/шум, кратковременная нестабильность частоты.

В статье рассмотрены вопросы, связанные с влиянием кратковременной нестабильностью частоты в канале связи на отношение сигнал/шум (ОСШ) при передаче сигнала с известными параметрами. Анализ влияния нестабильности частоты сигнала проведен в приближении воздействия аддитивного белого гауссовского шума. Значения шумового процесса считаются некоррелированными между собой и со значениями отсчетов передаваемого сигнала. Полученные результаты позволяют сформулировать требования к кратковременной нестабильности частоты сигнала в зависимости от требований вероятности битовой ошибки при использовании M-QAM и OFDM-сигналов.

**I.A. Alferova<sup>2</sup>, I.A. Engibaryan<sup>1</sup>, I.V. Reshetnikova<sup>1</sup>,  
O.A. Safaryan<sup>2</sup>, V.I. Yukhnov<sup>1</sup>**

## **THE EFFECT OF SHORT-TERM FREQUENCY INSTABILITY ON THE SIGNAL-TO-NOISE RATIO IN COMMUNICATION CHANNELS**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Don State Technical University, Rostov-on-Don, Russia<sup>2</sup>

Keywords: signal, signal-to-noise ratio, short-term frequency instability.

The article discusses issues related to the influence of short-term frequency instability in the communication channel on the signal-to-noise ratio (SNR) when transmitting a signal with known parameters. The analysis of the effect of signal frequency instability was carried out in the approximation of the effect of additive white Gaussian noise. The values of the noise process are considered uncorrelated with each other and with the values of the samples of the transmitted signal. The results obtained allow us to formulate requirements for short-term instability of the signal frequency depending on the requirements of the probability of bit error when using M-QAM and OFDM signals.

Одним из подходов при анализе влияния кратковременной нестабильности частотно-временных (ЧВП) сигналов является представление мгновенной частоты сигнала  $f(t)$  в виде

$$f(t) = f_0 + \frac{1}{2\pi} \frac{d\varphi_N(t)}{dt}. \quad (1)$$

Данный подход может быть использован при анализе взаимосвязи параметров кратковременной нестабильности частоты сигнала и изменения отношения сигнал/шум. С понятием и определением кратковременной нестабильности частоты связано второе

слагаемое в соотношении (1), описывающее кратковременную нестабильность частоты сигналов на коротком временном интервале, например, в пределах одного импульса. Кратковременная нестабильность ЧВП сигналов, период следования которых составляет порядка единиц-десятков миллисекунд, определяет, например, для систем связи изменение фазы сигнала между излучаемыми импульсами, что наиболее важно для случая передачи данных с использованием *M-QAM*-технологии [1-10].

Флуктуация средней частоты сигнала радиолокатора  $f(t)$ , описываемая выражением (1), приводит к изменению фазы принимаемого сигнала, что при проведении когерентной обработки принимаемого сигнала обуславливает снижению уровня автокорреляционной функции (АКФ). Случайные отклонения частоты излучаемого на передающей стороне сигнала приводят к появлению в принимаемом сигнале дополнительного фазового сдвига, имеющего случайное значение. В случае систем связи и передачи данных принимаемый сигнал представляет собой сигнал, содержащий информацию, передаваемую абонентом.

При обработке принимаемых сигналов указанные случайные значения фазы приводят к случайным отклонениям мгновенных отсчетов принимаемых сигналов, что обуславливает, в свою очередь, появление случайной составляющей сигнала на выходе устройства обработки [11-29].

Рассмотрим радиосигнал вида

$$V(t) = [V_0 + \Delta V(t)] \cdot \cos[(\omega_0 + \Delta\omega(t)) \cdot t + \varphi_0 + \Delta\varphi(t)] + n_u(t), \quad (2)$$

излученный в момент времени  $t$ , и поступивший на обработку на вход устройства формирования синфазной и квадратурной составляющих в момент времени  $t + \tau$ . В отсутствие кратковременной нестабильности частоты изменение фазы сигнала должно было составить величину  $\Delta\varphi(\tau) = 2\pi f_0 \cdot \tau$ . Однако из-за наличия флуктуаций ЧВП сигнала его частота, определяемая соотношением (1), отличается от  $f_0$ , и приращение фазы определяется следующим выражением

$$\Delta\varphi_N(\tau) = 2\pi \int_t^{t+\tau} (f_0 + (2\pi)^{-1} d\varphi_N(t)/dt) dt. \quad (3)$$

Если  $\varphi_N$  имеет симметричный закон распределения, то математическое ожидание и дисперсия дополнительной составляющей фазы (1.25) соответственно равны

$$M[\Delta\varphi_N(\tau)] = 2\pi f_0 \cdot \tau, \quad (4)$$

$$D[\Delta\varphi_N(\tau)] = 4\pi^2 M \left[ \left( f_0 \cdot \tau - \int_t^{t+\tau} (f_0 + (2\pi)^{-1} d\varphi_N(t)/dt) dt \right)^2 \right]. \quad (5)$$

Графическое представление случайных отклонений фазы при излучении и последующем приеме  $n$  импульсов, определяемых влиянием шумовой составляющей, приведено на рисунке 1.

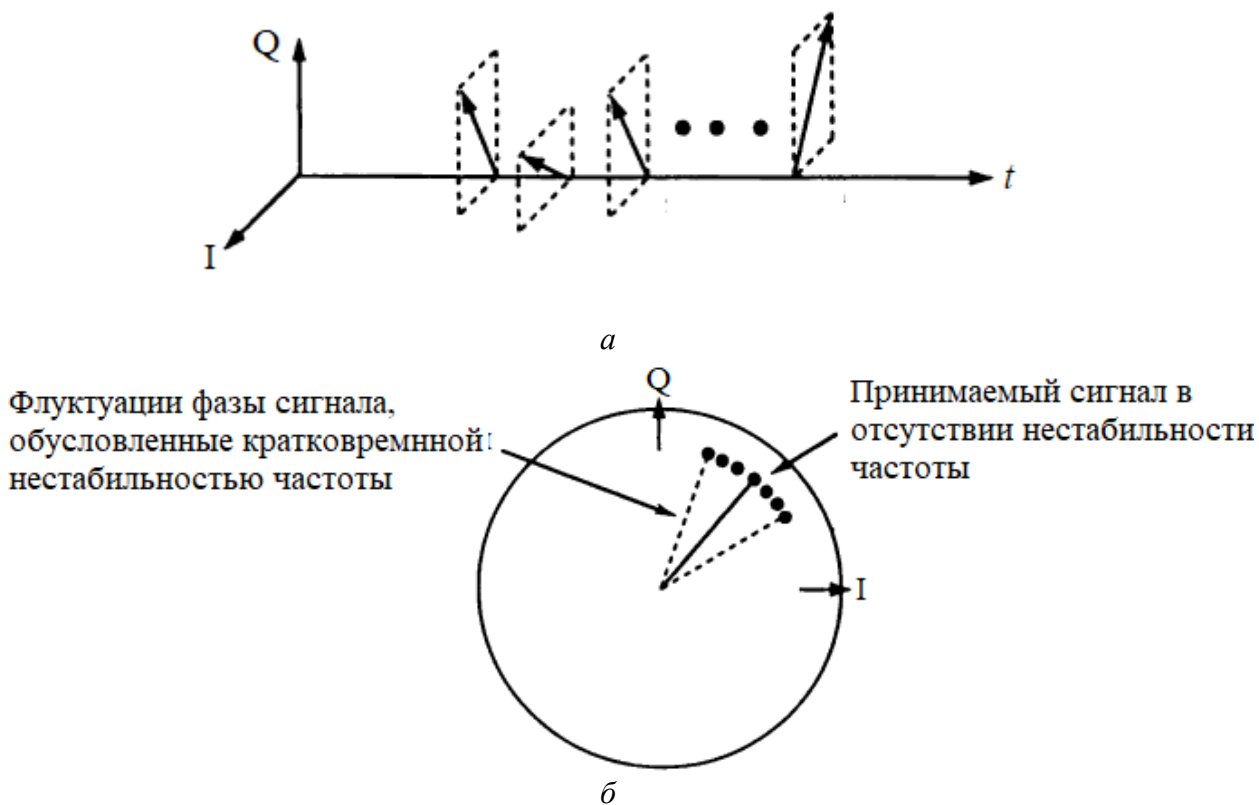


Рисунок 1. Влияние нестабильности частоты на сигнал [11]:  
 а – изменение синфазной и квадратурной составляющей при распространении сигнала;  
 б – графическое представление флуктуации фазы принятого сигнала, обусловленное кратковременной нестабильностью частоты

Для определения среднего отклонения частоты представим  $p$ -й сигнал в комплексной форме с помощью следующего соотношения [11]

$$G_p = A \exp[j(\psi - \nu \cdot \Delta f_i)], \quad p = 0, 1, 2, \dots, n-1, \quad (6)$$

где  $A$  и  $\psi$  - соответственно амплитуда и фаза сигнала в отсутствии нестабильности частоты;  $\nu \cdot \Delta f_i$  - составляющая случайной фазовой ошибки за время распространения сигнала  $\tau$ , обусловленная случайным отклонением частоты  $\Delta f_i$ ;  $\nu = 2\pi\tau$  рад/Гц.

Среднее отклонение частоты несущей  $\Delta f_i$  сигнала для  $i$ -го импульса является средним значением частоты за интервал  $\tau$  и определяется как

$$\Delta f_i = \frac{\Delta \varphi_N(\tau)}{\tau}. \quad (7)$$

Сигнал на выходе устройства дискретного преобразования Фурье, входящего в состав схемы, показанной на рисунке 1.4, при обработке сигнала (1) может быть определен следующим выражением [11]

$$M[H_i(\Delta f_i)] = A \cdot n \cdot C_j, \quad (8)$$

а его дисперсия - формулой

$$\sigma_H^2 = A^2 \cdot n \cdot M \cdot (1 - C_j^2). \quad (9)$$

В соотношениях (8), (9)  $C_j$  представляет характеристическую функцию, определяемую соотношением

$$C_j = \exp(-\nu^2 \sigma^2 / 2) \quad (10)$$

для СКО частоты  $\Delta f_i$  [11].

Необходимо отметить, что для идеально стабильного сигнала (сигнала без флуктуаций ЧВП) из (8) и (9) следуют, что  $C_j = 1$ . В этом случае для математического ожидания и дисперсии соответственно получаются следующие равенства  $M[H_i(\Delta f_i)] = A \cdot n$ ,  $\sigma_H^2 = 0$ .

Получаемое на основании соотношения (10) значение представляет нижнюю границу оценки дисперсии ЧВП сигнала, которая пропорциональна мощности сигнала. Указанный вывод является важным, так как показывает, что увеличение мощности сигнала при сохранении ЧВП не приводит к увеличению ОСШ

Указанное значение во многом определяет разрешение начальной фазы сигнала. В частности, это, как отмечалось выше, является важным в системах связи с М-QAM сигналами для оценивания начальной фазы сигнала, определяющей положение в сигнальном созвездии. Последнее определяется тем, что принимаемый сигнал может быть ниже уровня спектральных составляющих сигнала, одновременно принимаемого сигнала более высокого уровня мощности. Интегральная величина СКО спектральных составляющих фазовых шумов определяется как  $\sigma_c = \nu \cdot \sigma$ .

Результаты исследований взаимосвязи СКО фазовых ошибок с уменьшением мощности сигнала и соответствующим снижением ОСШ приведены в таблице 1 [11]. Для приведенных в таблице 1 результатов СКО фазовой ошибки определялось с использованием соотношения

Таблица 1. Потери мощности сигнала и снижение ОСШ, обусловленные кратковременной нестабильностью частоты

СКО фазовой ошибки $\sigma_c$	Уменьшение мощности сигнала		$\frac{nC_j^2}{1-C_j^2}$	Отношение мощности сигнала к мощности шумов, $S/\sigma_H^2$ , дБ			
	$C_j^2$	$C_j^2$ , дБ		$n = 64$	$n = 128$	$n = 256$	$n = 512$
0,01	0,9999	-0,0	$10.000 \cdot n$	58	61	64	67
0,02	0,9990	-0,0	$2.500 \cdot n$	52	55	58	61
0,05	0,9980	-0,0	$400 \cdot n$	44	47	50	53
0,1	0,9900	-0,0	$101 \cdot n$	38	41	44	47
0,2	0,9610	-0,2	$26 \cdot n$	32	35	38	41
0,5	0,7790	-1,1	$4,52 \cdot n$	25	28	31	34
1,0	0,3680	-4,3	$1,58 \cdot n$	20	23	26	29
2,0	0,0180	-17,4	$1,02 \cdot n$	16	21	24	27

Для приведенных в таблице 1 результатов СКО фазовой ошибки определялось с использованием соотношения

$$\sigma_{\Delta\varphi} = \sigma_{\Delta f} \cdot \tau, \quad (11)$$

где  $\sigma_{\Delta f}$  дисперсия частоты, обусловленная кратковременной нестабильностью.

Как и в случае *M-QAM*-модуляция с большими индексами, так и в случае с ортогональным мультиплексированием (использованием *OFDM*-сигналов) критическим параметром приемо-передающей аппаратуры РЭС является интегральный уровень спектральных составляющих сигнала. Появление паразитных спектральных составляющих несущей при *QAM*-модуляции может приводить к увеличению СКО оценки начальной фазы несущей дискретного состояния, что в приемном устройстве будет приводить к росту вероятности ошибок при приеме каждого бита информации и соответственно ухудшению качества связи [17-21].

## СПИСОК ЛИТЕРАТУРЫ

1. *Шорин О.А.* Оценка влияния скорости перемещения абонентов на удельную интенсивность потока потерь соединений в сетях с *OFDM*-сигналами // *Электросвязь*. 2017. № 1. С. 35-39.
2. *Шорин О.А.* Методы оптимального распределения частотно-временного ресурса в системах подвижной радиосвязи // Диссертация на соискание ученой степени д.т.н. – М.: МТУСИ, 2005. – 263 с.
3. *Бельчиков С.* Фазовый шум: как спуститься ниже –120 дБн/Гц на отстройке 10 кГц в диапазоне частот до 14 ГГц, или Борьба за децибелы. // *Компоненты и технологии*. 2009. № 5 С. 139-146.
4. *Артеменко А.А., Рубцов А.Е.* // *Вестник ННГУ. Серия Радиофизика*. Н. Новгород: Изд-во ННГУ, 2005. Вып. 1(3). С. 127–134.
5. *Артеменко А.А., Мальцев А.А., Рубцов А.Е.* Влияние неточности оценивания фазы несущей на вероятность битовых ошибок в *M-QAM* системах передачи данных // *Вестник ННГУ. Серия Радиофизика*. Н. Новгород: Изд-во ННГУ, 2007. Вып. 2(3). С. 81–87.
6. *Hanzo L.* Quadrature Amplitude Modulation: Basics to Adaptive Trellis-Coded, Turbo-Equalised and Space-Time Coded *OFDM*, *CDMA* and *MC-CDMA* Systems. - Wiley-IEEE Press, 2004.
7. *Prasad R., van Nee R.* *OFDM Wireless Multimedia Communications*. – L: Artech House, 2000. – 275 p.
8. *Lindsey W.C. and Chie C.M.* // *Proc. IEEE*. Apr. 1981. V. 69. P. 410–431.
9. *Старых Н.* Ослабление фазового шума в радарах и системах связи. // *Электронные компоненты*. 2018. № 7. С. 6-7.
10. *Мальцев А.А., Масленников Р.О., Хоряев А.В.* Влияние фазового шума на *OFDM*-системы передачи данных // *Известия вузов. Радиофизика*. 2010. Том LIII. № 8. С. 528-542.
11. *С.А. Гоголева, А.Я. Демидов, Н.А. Каратаева, Д.Ю. Майков, Е.П. Ворошилин.* Оценка влияния частотной расстройки на вероятность битовой ошибки в *OFDMA* системах связи // *Доклады ТУСУРа*, часть 1, декабрь 2011. № 2 (24), С. 45-48.
12. *Юхнов В.И., Енгибарян И.А., Сафарьян О.А., Пилипенко И.А.* Аналитические зависимости для оценок отклонения частоты и длительности формируемых сигналов в информационно телекоммуникационных системах // *Труды Северо-Кавказского филиала Московского технического университета связи и информатики*. 2020. № 1. С. 59-62.

- 
13. Сафарьян О.А., Алферова И.А., Енгибарян И.А., Юхнов В.И. Стабилизация частоты на основе первично-фундаментальных свойств больших систем. Научные технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 26-32.
  14. Donald R. Wehner. High-Resolution Radar – 2nd ed. ARTEC HOUSE, Inc. 1995. – 593 p.
  15. Исследование влияния джиттера тактового сигнала на цифро-аналоговое преобразование. AdvanteX Research Lab, 2004. Теоретические основы и результаты эксперимента.
  16. Сергиенко А. Б. Цифровая обработка сигналов. [Текст] – СПб.: Питер, 2003. – 604 с.: ил.
  17. Ричард Лайонс. Цифровая обработка сигналов: Второе издание. Пер. с англ. [Текст] – М.: ООО «Бином-Пресс», 2006 г. – 656с.: ил.
  18. Гуменюк А.С., Бочаров Ю.И. Устройства выборки-хранения быстродействующих АЦП. [Текст] Микроэлектроника, 2007, том 36, №5, с. 390-400.
  19. Мерфи Е., Слеттери К. Все о синтезаторах DDS. [Текст] Пер. с англ.
  20. Власенко А. // Компоненты и технологии. 2005. № 1. 32с.
  21. Галкин В.А. Цифровая мобильная радиосвязь. [Текст] - М.: Горячая линия-Телеком, изд. 2-е, 2012.
  22. Кестер У. Аналого-цифровое преобразование. [Текст] - М.: Техносфера, 2007.
  23. Carlos Azeredo-Leme, Clock Jitter Effect on Sampling. IEEE Circuits and systems magazine. 2011, pp. 26-37.
  24. Dai L., Harjani R. CMOS Switched-Op-Amp-Based Sample-and-Hold Circuit // IEEE J. Solid-State Circuits. 2000. V. 35. № 1. P. 109-113.
  25. Бельчиков С. Фазовый шум. [Текст] // Компоненты и технологии. 2009. №5. с. 139-146.
  26. J. Bahl and P. Bharti. Microwave Solid State Circuit Design, Second Edition. – John Wiley & Sons Inc., Hoboken, NJ, 2003.
  27. J. A. Scheer and J. Kurtz, Coherent Radar Performance Estimation. Artech House, Boston, MA, 1993.
  28. R. H. Walden, IEEE J. 1999. Sel. Commun. 17, P. 539.
  29. J. Kim, J. A. Cox, J. Chen, and F. X. Kartner, Nat. Photonics. 2008. № 2, P. 733.

**Фан Гуан Ань**

## **МОДЕЛИРОВАНИЕ И АНАЛИЗ ПИК-ФАКТОРА И КОЭФФИЦИЕНТА ОШИБОК СИМВОЛОВ ДЛЯ АМПЛИТУДНО-ФАЗОВОЙ МОДУЛЯЦИИ**

Ордена Трудового Красного Знамени федеральное государственное Бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», Москва, Россия

Ключевые слова: амплитудно-фазовая модуляция, помехоустойчивость, энергоэффективность, пик-фактор, коэффициент ошибок, коэффициенты, соотношение сигнал/шум.

В данной статье рассматриваются моделирование и анализ пик-фактора (PAPR – Peak to Average Power Ratio) и коэффициента ошибок символов (SER - Symbol error ratio) в системах связи, использующих амплитудно-фазовую модуляцию (APSK - Amplitude Phase Shift Keying). Методы модуляции амплитуды и фазы используются в многих стандартах, которые позволяют передавать радиосигналы на большие расстояния с более высокой

---

скоростью передачи данных. В последнее время наблюдается рост интереса бизнеса к использованию режимов, выходящих за рамки модуляции APSK. Двумя фундаментальными требованиями оптимизации для методов проектирования созвездий APSK являются минимизация значений пик-фактора и минимизация коэффициента ошибок символов в системах связи. В данной работе рассматриваются алгоритмы для модуляции APSK, а также анализ значения пик-фактора в случаях изменения параметров в модуляции APSK. Исследуется зависимость коэффициента ошибок символов от параметров созвездия. Наконец, проводится сравнительный анализ достигнутых результатов с вниманием на помехоустойчивость и энергоэффективность. Моделирование модуляции APSK в системе связи в пакете «Матлаб» является основным направлением данной работы. По результатам моделирования можно увидеть коэффициент ошибок символов в канале Рэлеевского замирания и значение пик-фактора в системе связи на одной несущей множественного доступа с частотным разделением SC-FDMA (Single Carrier - frequency-division multiple access). В заключение результаты этих зависимостей наглядно представлены, сопоставлены и объяснены. Для того чтобы оценить эффективность системы, мы должны учитывать как значения пик-фактора, так и коэффициента ошибок символов. Для достижения оптимальной производительности эти показатели необходимо комбинировать, чтобы получить оптимальный вариант для системы связи.

**Phan Tuan Anh**

## **SIMULATION AND ANALYSIS OF THE PAPR AND SER IN THE M-APSK MODULATION**

Moscow Technical University of Communications and Informatics, Moscow, Russia

**Keywords:** M-APSK, Noise immunity, Power efficiency, Peak to Average Power Ratio (PAPR), Symbol error ratio (SER), signal to noise ratio (SNR)

This paper explores the simulation and analysis of the PAPR (Peak-to-Average Power Ratio) and SER (Symbol error ratio) in communication systems using the M-APSK (Amplitude Phase Shift Keying) modulation. The M-APSK modulation methods are used in the aforementioned standards, which allow radio signals to be transmitted over greater distances with higher data rates. There has been a rise in business interest in using modes beyond M-APSK. The two fundamental optimization requirements for APSK constellation design techniques are minimizing the PAPR (Peak-to-Average Power Ratio) values and minimizing the SER (symbols error ratio) in the communication systems. This work discusses algorithms for M-APSK modulation, as well as analyzing the PAPR value in cases where APSK parameter changes are made. The dependencies of SER on constellation parameters are examined. Finally, the comparative analysis of results achieved is made with a focus on noise immunity and power efficiency. The implementation of the M-APSK modulation in the communication system in MATLAB is the focus of this work. It is possible to see the SER in the fading Rayleigh channel and PAPR at the results of the simulation. In conclusion, the results of these dependencies are clearly presented, compared and explained. In order to evaluate the efficiency of a system, we must consider both PAPR and SER. To achieve optimal performance, these indicators must be combined in order to provide an accurate picture.



---

## Введение.

Важнейшим требованием системы передачи данных является обеспечение высокой энергоэффективности при минимизации потерь на использование спектра, чтобы системы связи были адаптированы специально для современных приложений. Используя методы помехоустойчивой модуляции и эффективные канальные коды, вещательные компании могут добиться надежной передачи даже в сложных условиях. Методы модуляции, обеспечивающие более высокую спектральную эффективность, необходимы для систем связи, поскольку они должны передавать данные с большей скоростью. Однако в результате этого снижается помехоустойчивость канала [1, 2].

Современные автогенераторы реализованы для использования в схемах в ГУН (генератор, управляемый напряжением) и можно использовать также в качестве усилителей СВЧ сигналов сложной формы. Это позволяет повысить стабильность автогенераторов, снизить его шумы и обеспечить постоянство амплитуды выходного напряжения [3 - 6].

Взросший спрос на системы связи, способные передавать больше данных, требует использования методов модуляции с более высокой спектральной эффективностью. При использовании метода модуляции более высокого порядка увеличивается как спектральная эффективность, так и скорость передачи данных. Однако это увеличение производительности сопровождается снижением помехоустойчивости канала. Системы модуляции высшего порядка, такие как M-аричная фазовая модуляция (PSK - phase shift keying), становятся все более популярными в спутниковой связи благодаря своим превосходным характеристикам по сравнению с традиционными схемами, такими как квадратурная фазовая модуляция (QPSK- quadrature phase shift keying). При использовании этой технологии необходимо применять эффективные методы кодирования и оптимизированные спектрально и энергоэффективные алгоритмы модуляции для достижения наиболее благоприятных результатов [7, 8]. Эти технологии лучше всего использовать в конкретных условиях связи. Эти технологии модуляции обычно используются в различных приложениях, когда отношение сигнал/шум в приемнике является достаточным.

Если PSK является единственной используемой схемой модуляции, то количество возможных фазовых состояний будет большим. Это затруднит реализацию PSK, так как будет много возможностей для кодирования данных. Однако если мы объединим амплитудной модуляции с волновой функцией, то количество фазовых состояний уменьшится, поскольку мы будем делить на группы амплитуд. Это означает, что одно и то же фазовое состояние (т.е. в определенной точке пространства) может иметь разные амплитуды, а также разные фазы в зависимости от того, какая группа амплитуд задействована. APSK — это метод модуляции, который сочетает в себе как амплитудную, так и фазовую модуляцию для цифровых систем передачи [9-11].

Схемы модуляции высшего порядка, вероятно, будут выгодны для будущих наблюдательных миссий, требующих скорости нисходящей передачи данных более 1 Гбит/с. Эти схемы могут обеспечить высокую пропускную способность, необходимую для различных цифровых мультимедийных приложений и других приложений с высокой скоростью передачи данных, таких как доступ к Интернету "точка-точка" через сеть позвоночника. По сравнению с другими методами модуляции, APSK выделяется как привлекательный вариант для цифровой передачи по нелинейным каналам связи благодаря своей энергетической и спектральной эффективности. Кроме того, он устойчив к нелинейным искажениям, что делает его желательным выбором в данном контексте. Модуляция M-APSK хорошо известна своей устойчивостью к нелинейным искажениям в радиоканалах [12]. Методы модуляции 16- и 32-APSK используются в некоторых настоящих стандартах, которые позволяют передавать радиосигналы на большие расстояния с более высокой скоростью передачи данных. Схема модуляции 4-12-APSK и 4-12-16-APSK была предложена в стандарте DVB-S2, и были проведены обширные исследования для оценки их производительности в различных условиях канала, в том числе

---

с усилителями высокой мощности (HPA - High Power Amplifiers) [13]. В частности, DVB-S2 использует 16-APSK и 32-APSK для повышения отношения сигнал/шум (SNR – signal to noise ratio). Для получения высококачественных широкополосных сигналов через спутник, системы связи должны использовать методы модуляции, которые могут противостоять шумовым помехам. Спутник находится довольно далеко от Земли, поэтому уровень сигнала очень низок, и помехи легко нарушают его на приемном оборудовании. Для борьбы с этой проблемой в цифровых системах связи часто используется модуляция со сдвигом амплитуды и сдвигом фазы, которая известна как APSK. Модуляция APSK также может использоваться для потребительских устройств, таких как многоручевые спутники или цифровое видеовещание, которые требуют большей эффективности использования спектра.

В последние годы наблюдается рост интереса бизнеса к использованию режимов, выходящих за рамки 16- и 32-APSK. Это особенно актуально для профессиональных приложений, где требуется более высокий уровень шума. Системы связи сталкиваются с двумя общими проблемами: шумом и помехами. Однако нелинейность канала представляет собой дополнительную проблему. Нелинейные искажения сигнала, вызванные шумом и помехами, со временем привели к увеличению числа ошибок, поэтому важно соблюдать меры предосторожности при работе со сложными системами. Нелинейность сигнала возникает в результате того, что плата усилителя мощности настроена на работу в наиболее эффективной точке, близкой к насыщению. Схемы модуляции высшего порядка M-APSK подвержены колебаниям огибающей сигнала, вызванным транспондерами, что может привести к нелинейности канала. Усилитель высокой мощности (HPA) и цифро-аналоговый преобразователь (DAC – Digital to Analog converter) искажают сигнал при прохождении через них, что приводит к снижению среднего уровня мощности (высокое отношение пиковой мощности к средней (пик-фактор)). Это ограничение можно обойти, увеличив мощность сигнала, но это нарушит некоторые нормы регулирования, ограничивающие мощность передачи. Два основных требования к оптимизации методов проектирования созвездий APSK — это минимизация значений пик-фактора (PAPR) и максимизация помехоустойчивости (минимизация коэффициента ошибок символов (SER)) в системах связи. Для того чтобы оценить эффективность системы, мы должны учитывать как значение пик-фактор (PAPR), так и показатель ошибок символов (SER). Для достижения оптимальной производительности эти показатели необходимо комбинировать, чтобы получить оптимальное значение.

Остальная часть данной работы организована следующим образом: Первый раздел содержит краткое объяснение алгоритма, используемого для модуляции APSK, одновременно представляя параметры, необходимые для анализа и моделирования M-APSK. Во втором разделе представлен функция CCDF (Complementary Cumulative Distribution Function) для значения PAPR, полученный в результате моделирования методом Монте-Карло. В 3-ом разделе представлены графические зависимости коэффициента ошибок символов (SER) от параметров модуляции 16-APSK. После этого результаты анализируются и обсуждаются.

### **Обзор модуляции APSK.**

Этот обзор модуляции APSK дает понимание того, как она работает, и ее потенциальных применений. После завершения этапов адаптации и кодирования выход канального перемежителя отображается на диаграмму созвездий выбранной схемы модуляции. Модуляция M-APSK широко используется в современных системах передачи информации. Во время модуляции входные биты сопоставляются один к одному с одним из  $M=2^B$  волновых форм в следующем наборе.

$$S = \{S_1, S_2, \dots, S_M\} \quad (1)$$

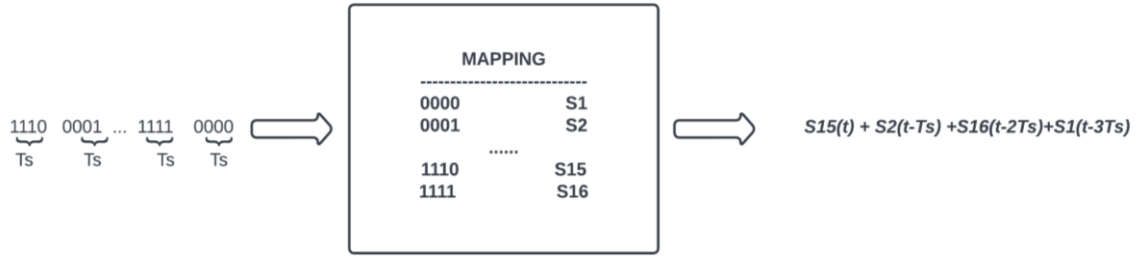


Рисунок 1. Пример процесса сопоставления 16-APSK

Созвездие APSK состоит из  $N$  числа концентрических окружностей, каждая из которых имеет  $n_k$  сигнальных точек (т.е.  $k$ -я окружность в созвездии имеет  $n_k$  сигнальных точек), а радиус и первичный фазовый сдвиг для этой окружности -  $r_k$ ,  $\varphi_k$ . В общем случае созвездие APSK может быть описано следующим образом [4]:

$$x = \left\{ \begin{array}{l} r_1 \cdot e^{j(\varphi_1 + \frac{2\pi}{n_1}n)} \quad n = 0, 1, \dots, n_1 - 1 \\ \dots \dots \dots \\ r_k \cdot e^{j(\varphi_k + \frac{2\pi}{n_k}n)} \quad n = 0, 1, \dots, n_k - 1 \\ \dots \dots \dots \\ r_N \cdot e^{j(\varphi_N + \frac{2\pi}{n_N}n)} \quad n = 0, 1, \dots, n_N - 1 \end{array} \right\} \quad (2)$$

где,  $k=1, 2, \dots, N$ .

Из математической модели следует, что основными параметрами созвездий APSK являются число состояний каждого круга  $n_k$ , вектор сигнала каждого состояния с амплитудой  $r_k$  и первой фазовый сдвиг точек символа  $\varphi_k$ . Чтобы было удобнее, вместо радиусов будем использовать их отношения относительно радиуса самой внутренней окружности  $\gamma_k = \frac{r_{k+1}}{r_k}$ . Модуляцию APSK обычно называют  $n_1$ - $n_2$ -...- $n_N$ -APSK. Примеры созвездий 4-12-APSK и 4-12-16-APSK показаны ниже.

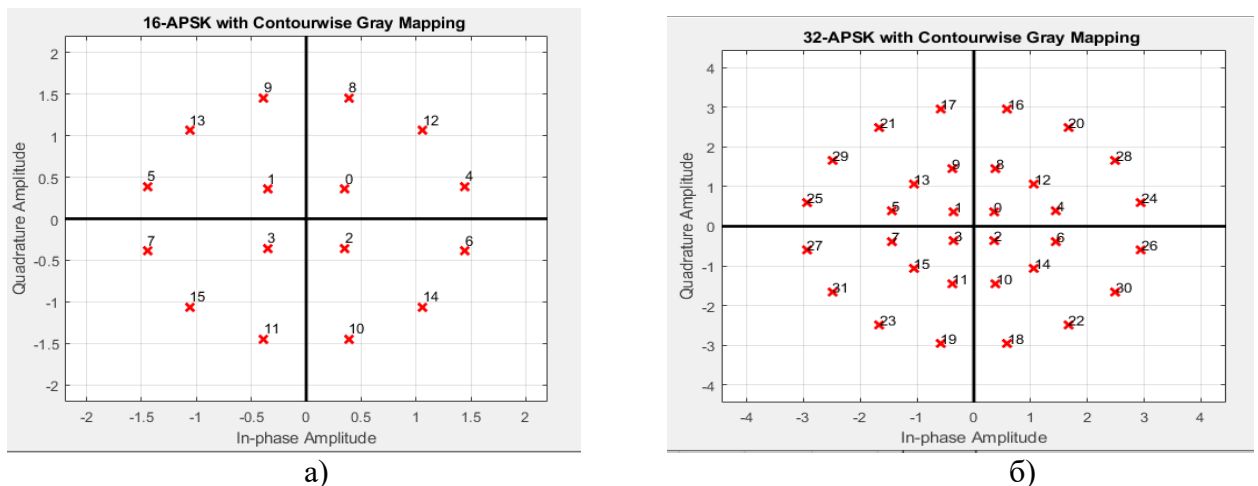


Рисунок 2. Созвездия M-APSK:  
а) 4-12-APSK    б) 4-12-16-APSK.

Параметры этих примеров созвездий следующие:

В случае 16-APSK:  $N=2$ ,  $n_1=4$ ,  $n_2=12$ ,  $\varphi_1 = \frac{\pi}{4}$ ,  $\varphi_2 = \frac{\pi}{12}$  и  $\gamma_1 = \frac{r_2}{r_1} = \frac{1.5}{0.5} = 3$ . В случае 32-APSK:  $N=3$ ,  $n_1=4$ ,  $n_2=12$ ,  $n_3=16$ ,  $\varphi_1 = \frac{\pi}{4}$ ,  $\varphi_2 = \frac{\pi}{12}$ ,  $\varphi_3 = 0$ ,  $\gamma_1 = \frac{r_2}{r_1} = \frac{1.5}{0.5} = 3$ ,  $\gamma_2 = \frac{r_3}{r_2} = \frac{3}{1.5} = 2$ .

Для простоты проведем исследование для 16-APSK модуляции, в которой одна из 16 форм волны отображается на 4 бита ( $M = 16$  и  $B = \log_2 M = 4$ ). Входная битовая последовательность состоит из 4-битовых непрерывающихся сегментов.

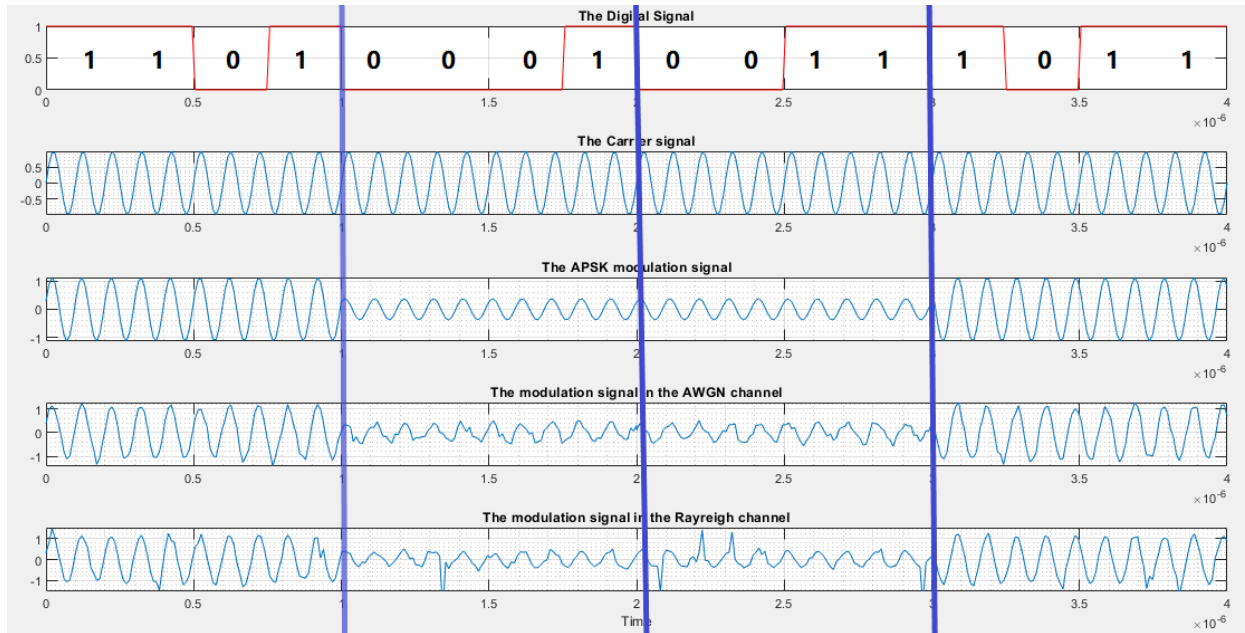


Рисунок 3. Модуляционные сигналы в 16-APSK модуляции

Как видно на рис.3, четыре бита, составляющие участок осциллограммы, соответствуют одной из 16 различных волн. Каждые  $T_s$  секунд генерируется новая волновая форма, соответствующая 4-битному символу. В результате предполагается, что период символа  $T_s$  будет измеряться в [с/символ], а соответствующая скорость передачи символов  $R_s$  будет установлена по следующей формуле:

$$R_s = \frac{1}{T_s} \text{ (symbols/s)} \quad (3)$$

Поскольку символ состоит из  $B$  бит, скорость передачи данных определяется как  $T_b = T_s/B$  [s/bit], а период передачи данных - как  $T_b = T_s/B$  [s/bit]. Следовательно, скорость передачи данных рассчитывается по следующей формуле:

$$R_b = \frac{1}{T_b} \text{ (bits/s)} \quad (4)$$

Математическая зависимость между скоростью передачи данных и скоростью передачи символов выглядит следующим образом:

$$R_b = B \cdot R_s \quad (5)$$

Для 16-APSK скорость передачи данных в четыре раза превышает скорость передачи символов.

В следующих разделах мы проведем простой метод моделирования для системы с использованием модуляции 16-APSK для анализа производительности радиосистем на основе измерений PAPR (пик-фактор) и SER (коэффициент ошибок символов). Вторая часть данной работы посвящена анализу влияния параметров модуляции APSK на значение PAPR системы SC-FDMA. В 3-ей части будет проведен анализ их влияния на SER при передаче по каналу с замираниями Рэлея. Для того чтобы исследовать влияние различных параметров созвездия 16-APSK, были использованы различные комбинации  $n_1$ ,  $n_2$ ,  $\varphi_1$ ,  $\varphi_2$  и

$\gamma_1$ . Параметры комбинации модуляции 16-APSK для каждого случая исследования приведены в таблице 1.

Таблица 1. Конфигурации исследуемых параметров модуляции APSK

Constellation Number (CN)	$\gamma_1$	$n_1$	$n_2$	$\phi_1$	$\phi_2$
CN0	2.5	8	8	15	15
CN1-1	2.5	8	8	0	15
CN1-2	2.5	8	8	10	15
CN1-3	2.5	8	8	20	15
CN1-4	2.5	8	8	30	15
CN2-1	2.5	8	8	15	0
CN2-2	2.5	8	8	15	10
CN2-3	2.5	8	8	15	20
CN2-4	2.5	8	8	15	30
CN3-1	2.5	4	12	15	15
CN3-2	2.5	12	4	15	15
CN4-1	1.5	8	8	15	15
CN4-2	2	8	8	15	15
CN4-3	3	8	8	15	15
CN4-4	3.5	8	8	15	15

Нулевой номер созвездия (CN0) будет использоваться в качестве опорного значения для сравнения с другими при моделировании. Легко заметить, что в случаях CN1-х изменяется значение первичного фазового сдвига первого круга. В то время как CN2-х выполняет изменение значения фазового сдвига второго круга. Случаи CN3-х изменяют значение числа состояний каждого круга. В то же время CN4-х изменяет значения коэффициентов относительно радиуса двух окружностей. Внесение этих изменений позволяет оценить влияние параметров APSK на значений PAPR и SER в системе связи. На основании этого результата мы можем оценить производительность системы.

#### **Влияние параметров модуляции APSK на значение пик-фактора.**

В этом разделе мы собираемся проанализировать значение пик-фактора (PAPR) в 16-APSK модуляции. На рисунке 4 показан ход моделирования простого расчета PAPR для систем модуляции APSK. Моделирование выполняется в программе MATLAB.

Для моделирования в данном исследовании мы анализируем значение PAPR для сигналов SC-FDMA с фильтром формирования импульсов. Основным преимуществом SC-FDMA является более низкий PAPR благодаря структуре с одной несущей [5]. Сравнивая две формы SC-FDMA, мы обнаружили, что локализованное FDMA (LFDMA - localized FDMA) имеет более высокий PAPR, чем чередующееся FDMA (IFDMA - interleaved FDMA). Поэтому мы будем использовать IFDMA для режима распределенного отображения поднесущих.

Заметно, что фильтр формирования импульсов увеличивает значение PAPR. В нашем исследовании мы используем импульс с повышенным косинусом, который является широко используемой формой импульса в беспроводной связи, определяемой следующим образом во временной области [6]:

$$r(t) = \text{sinc}\left(\pi \frac{t}{T}\right) \frac{\cos\left(\frac{\pi \alpha t}{T}\right)}{1 - \frac{4\alpha^2 t^2}{T^2}} \quad (6)$$

где  $\alpha$  - коэффициент свертывания, который находится в диапазоне от 0 до 1. В данном исследовании коэффициент свертывания будет равен 0,5.

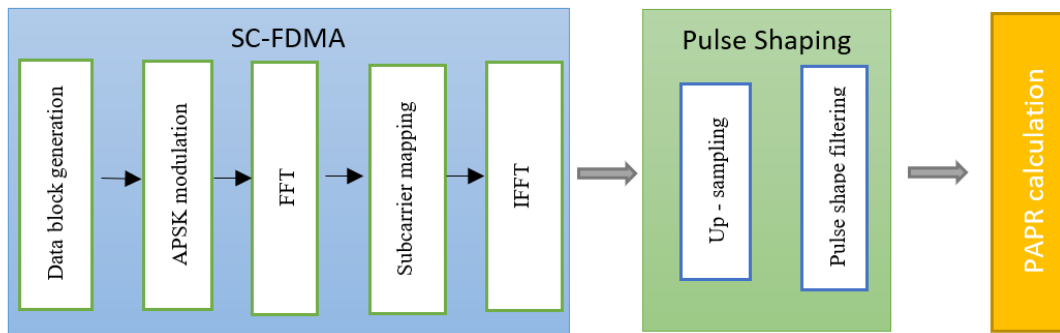


Рисунок 4. Блок-схема расчета пик-фактора для модуляции APSK в системах связи SC-FDMA

Для измерения мощной эффективности оценивается параметр PAPR (пик-фактор). Он измеряет отношение пиковой мощности к средней. Это отношение между максимальной и средней мощностью сигнала  $x(t)$  за период и представляется следующим выражением:

$$PAPR = \frac{\text{Peak power of } x(t)}{\text{Average power of } x(t)} = \frac{\text{Max}_{0 \leq t \leq T} |x(t)|^2}{\frac{1}{T} \int_0^T |x(t)|^2 dt} \quad (7)$$

Для численного анализа характеристик PAPR мы используем дополнительную кумулятивную функцию распределения (CCDF - Complementary Cumulative Distribution Function). Численные результаты функции CCDF распределения PAPR, которая представляет собой вероятность того, что PAPR больше определенного значения  $PAPR_0$  ( $\Pr\{PAPR > PAPR_0\}$ ), рассчитывается методом моделирования Монте-Карло [6]. На следующих рисунках представлены результаты моделирования функции CCDF для значения PAPR с использованием симуляторов, описанных на рисунках 4, с помощью программы Matlab.

На рисунке 5 показаны функции CCDF для значения PAPR в системе связи SC-FDMA с модуляцией 16-APSK для различных значений первичного фазового сдвига ( $\varphi_1$  и  $\varphi_2$ ). Видно, что значения PAPR не зависят от первичного фазового сдвига каждого круга.

Рисунок 6 представляет собой графические результаты CCDF функции для PAPR, когда количество состояний в каждом круге ( $n_1$  и  $n_2$ ) изменяется. Производительность значительно ухудшается при более высоком PAPR, когда  $n_1$  увеличивается. Результат показывает, что 4-12-APSK ( $n_1=4$  и  $n_2=12$ ) дает наилучшую производительность для значения пик-фактора. Это иллюстрирует критическую роль соответствующего выбора номера состояния каждого круга в системе связи с модуляцией M-APSK.

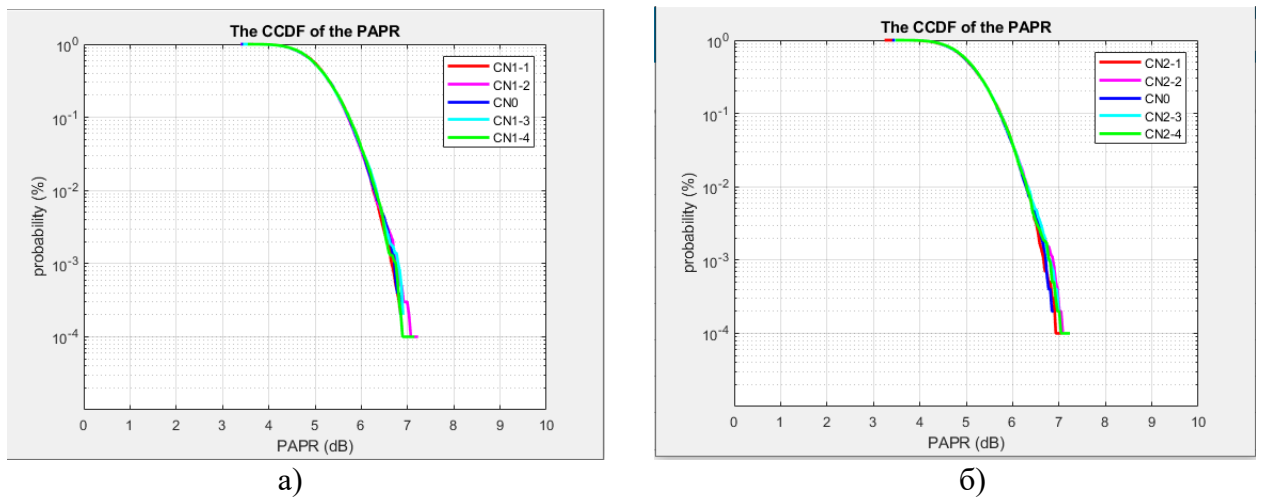


Рисунок 5. CCDF функция для PAPR в 16-APSK модуляции с различными значениями первичного фазового сдвига: а) первого круга, б) второго круга

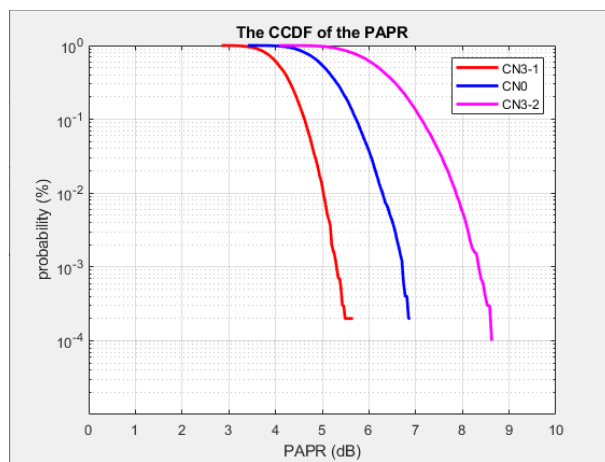


Рисунок 6. CCDF функция для PAPR в 16-APSK модуляции с различным количеством состояний в каждом круге

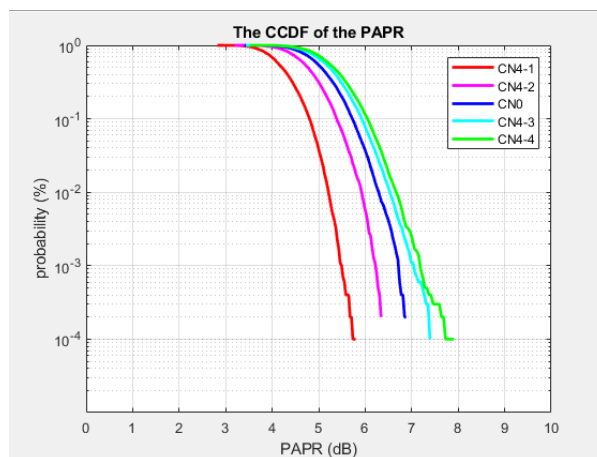


Рисунок 7. CCDF функция для PAPR в 16-APSK модуляции с различными соотношениями относительно радиуса двух окружностей

На рисунке 7 показаны результаты моделирования при изменении соотношения между радиусами двух окружностей  $\gamma_1$ . На основании этого результата установлено, что с увеличением отношения амплитуд между кольцами значение PAPR увеличивается. Результаты моделирования согласуются с теорией модуляции APSK. Кроме того, мы



видим, что при увеличении этого относительного соотношения скорость увеличения PAPR уменьшается.

Мы сравниваем значения пик-фактора, которые превышены с вероятностью менее 0,1% (или вероятность 99,99%) . Полное сравнение для различных случаев показано в таблице 2.

Таблица 2. Значения пик-фактора с вероятностью 99,99% при различных параметрах модуляции.

Constellation Number (CN)	CN0	CN1-1,2,3,4	CN2-1,2,3,4	CN3-1	CN3-2	CN4-1	CN4-2	CN4-3	CN4-4
PAPR	6.7 dB	6.7 dB	6.7 dB	5.2 dB	8.3 dB	5.5 dB	6.2 dB	7 dB	7.1 dB

Во-первых, в случае изменения числа состояния каждого круга, CN3-1 имеет более низкий значения пик-фактора, чем CN0 на 1,5 дБ, в то время как значение пик-фактор для CN0 ниже, чем CN3-2 на 1,6 дБ. При изменении соотношения между радиусами двух окружностей в случае CN0 значение пик-фактора ниже, чем в случае CN4-3 на 0,3 дБ и на 0,4 дБ для случая CN4-4, но выше, чем в случае CN4-1 на 1,2 дБ и на 0,5 дБ для CN4-2. Видно, что случай CN3-1 имеет самый низкий пик-фактор по сравнению с другими. Результаты в таблице 2 показывают расчетные значения параметра пик-фактора для оценки энергетической эффективности этих различных созвездий в системах связи.

Из приведенных выше результатов моделирования можно сделать следующие выводы, что характеристики PAPR в модуляции M-APSK не зависят от первичного фазового сдвига каждого круга. Функция CCDF значения пик-фактора остается неизменной при изменении  $\varphi_k$ . Но PAPR системы связи с модуляцией M-APSK зависит от числа состояния и соотношения радиусов между кругами. Когда число состояния первого круга увеличивается (число состояний других кругов уменьшаются), значение PAPR системы связи увеличивается. В то же время, при увеличении их отношения к радиусу самого внутреннего круга, значение PAPR также будет увеличиваться. Поэтому при выборе параметров модуляции M-APSK необходимо рассчитать  $\rho_k$  и  $\gamma_k$  для оптимизации значения PAPR (энергетической эффективности) системы с учетом других параметров системы. Важным параметром радиосистемы является помехоустойчивость. В следующем разделе мы проанализируем влияние параметра M-APSK на коэффициент ошибок символов (SER) систем связи.

### **Влияние параметров модуляции ASPK на коэффициент ошибок символов системы связи.**

Ключевым показателем для оценки любой схемы модуляции является коэффициент символьных ошибок (SER – symbol to error ratio) для соответствующей некодированной системы. Коэффициент символьных ошибок (SER) — это количество подсчитываемых символьных ошибок, встречающихся в потоке данных за определенный период времени. Общие причины символьных ошибок включают канальный шум, помехи сигнала, искажения и ошибки синхронизации часов передатчика и приемника. SER дает общее представление о том, когда можно ожидать появления ошибок в сигнале. Чем ниже SER, тем выше производительность системы.

В данном разделе представлены характеристики отношения ошибок символов (SER) при использовании 16-APSK созвездий и проведен сравнительный анализ полученных результатов. Моделирование расчета SER с различными параметрами модуляции 16-APSK выполнено в канале Fading Rayleigh. Алгоритм вычисления значения SER показан на рисунке 8 выше. Моделирование будем проводить в программе Matlab. Выбранный уровень SNR (signal to noise ratio) находится в диапазоне от -3 дБ до 40 дБ.

Для изучения влияния различных параметров созвездия 16-APSK на помехоустойчивость были использованы различные комбинации  $\rho_1$ ,  $\rho_2$ ,  $\varphi_1$ ,  $\varphi_2$  и  $\gamma_1$ .



Параметры комбинации модуляции 16-APSK для каждого случая исследования приведены в таблице 1. При моделировании вычисляется коэффициент ошибок символов (SER) для оценки производительности.

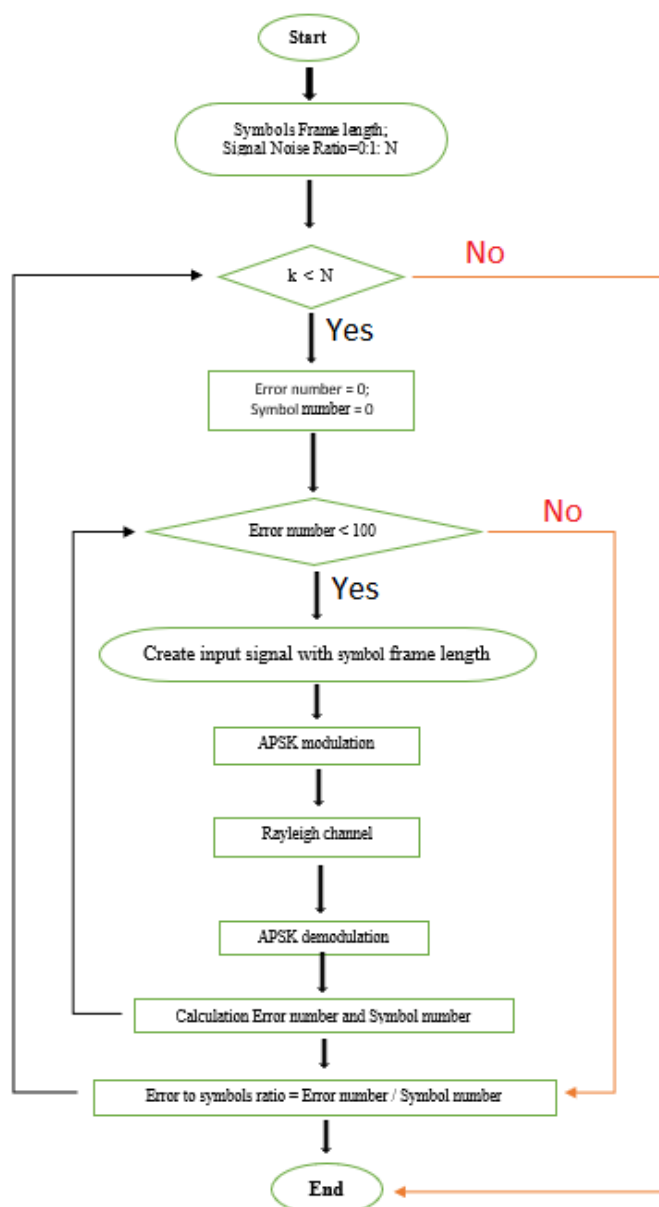
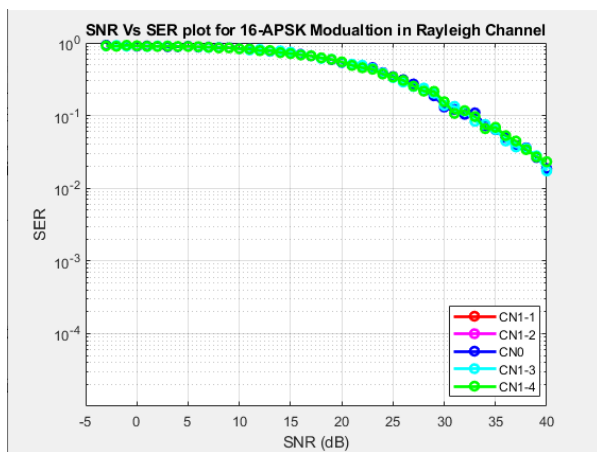


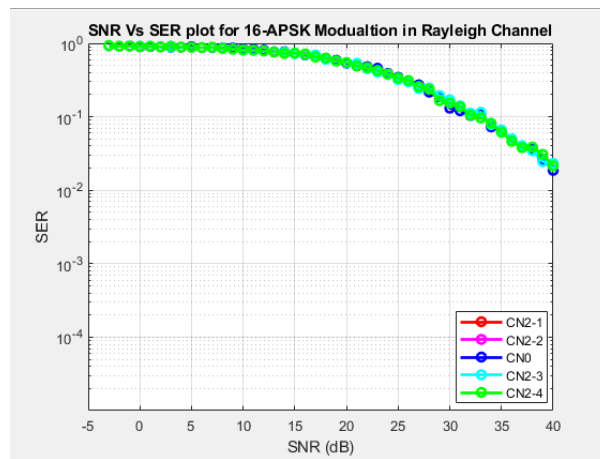
Рисунок 8. Алгоритм моделирования для расчета коэффициента символьных ошибок (SER) при модуляции M-APSK

Рисунок 10 представляет собой графические результаты вероятности ошибки символа при изменении количества состояний в каждом круге ( $n_1$  и  $n_2$ ). Результаты показывают, что при увеличении  $n_1$  и уменьшении  $n_2$  вероятность ошибки также увеличивается.

На рисунке 11 показаны результаты моделирования при изменении соотношения между радиусами двух окружностей  $\gamma_1$ . В данном случае сравнивается производительность SER между различными значениями  $\gamma_1$ . При увеличении относительного соотношения между радиусами двух окружностей вероятность ошибок при передаче уменьшается.



а)



б)

Рисунок 9. Зависимость SER от SNR в 16-APSK модуляции с различными значениями первичного фазового сдвига: а) первого круга, б) второго круга

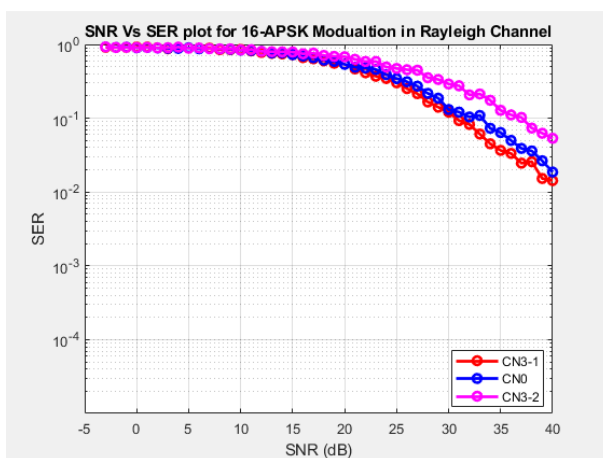


Рисунок 10. Зависимость SER от SNR в 16-APSK модуляции с различным количеством состояний в каждом круге

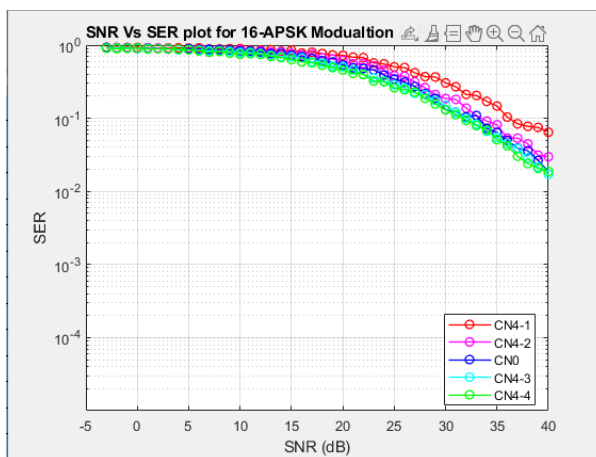


Рисунок 11. Зависимость SER от SNR в 16-APSK модуляции с различным соотношением относительно радиуса двух окружностей

В таблице 3 приведены зависимости SER от параметров созвездия 16-APSK для различных случаев. Эти зависимости были получены при отношении плотности мощности энергии сигнала к плотности мощности шума ( $E_s/N_0=25$  дБ). Эта таблица численно показывает влияние параметров 16-APSK модуляции на помехоустойчивость радиосистем.

Таблица 3. Значения SER при отношении сигнала на шум  $E_s/N_0=25$  дБ

Constellation Number (CN)	CN0	CN1-1,2,3,4	CN2-1,2,3,4	CN3-1	CN3-2	CN4-1	CN4-2	CN4-3	CN4-4
Symbol Error Ratio	0.12	0.12	0.12	0.119	0.135	0.15	0.14	0.116	0.114

Очевидно, что самая высокая помехоустойчивость радиоканала (минимальное значение SER) может быть обеспечена при использовании 16-APSK созвездия CN4-4.

Из приведенных выше результатов моделирования можно сделать следующие выводы, что производительность SER в модуляции M-APSK не зависит от первичного фазового сдвига каждого круга. Вероятность ошибки символа остается неизменной при изменении  $\varphi_k$ . Но вероятность ошибки символа в системе связи с модуляцией M-APSK зависит от количества состояний и соотношения радиусов между кругами. Когда число состояний первого круга увеличивается (номера состояний других кругов уменьшаются), значение SER системы связи увеличивается. В то же время, при увеличении их отношения к радиусу самого внутреннего круга, значение вероятности ошибки символа также уменьшается. Поэтому при выборе параметров модуляции M-APSK необходимо рассчитать  $n_k$  и  $\gamma_k$  для оптимизации помехоустойчивости системы с учетом других параметров системы.

#### Выводы.

Исследования значение пик-фактора в системе SC-FDMA и помехоустойчивости в затухающем рэлеевском канале, для формирования которого использовались изученные 16-APSK созвездия, показывают, что для оптимизации системы связи необходимо учитывать некоторые параметры M-APSK модуляции.

Мы проанализировали показатель PAPR сигналов SC-FDMA в случаях различных параметров 16-APSK модуляций. В частности, мы численно сравнивали характеристики PAPR, используя функцию CCDF. Характеристики PAPR в модуляции M-APSK не зависят от первичного фазового сдвига каждого круга. Но значение PAPR системы связи с модуляцией M-APSK зависит от чисел состояний и соотношения радиусов между кругами. При увеличении количества состояний первой из них, значение PAPR системы связи увеличивается. В то же время, когда их отношение к радиусу внутренней окружности увеличивается, значение PAPR также увеличивается.

Мы также проанализировали вероятность ошибки символов. Производительность SER в модуляции M-APSK не зависит от первичного фазового сдвига каждого круга. Но вероятность ошибки символа в системе связи с модуляцией M-APSK зависит от чисел состояний и соотношения радиусов между кругами. При увеличении число состояний первой из них, значение SER системы связи увеличивается. В то же время, когда их отношение к радиусу внутренней окружности увеличивается, значение вероятности ошибки символа также уменьшается.

Поэтому при выборе параметров модуляции M-APSK необходимо рассчитать  $n_k$  и  $\gamma_k$  для оптимизации помехоустойчивости и значения пик-фактора системы с учетом других показателей системы. Очевидно, что самая высокая помехоустойчивость радиоканала может быть обеспечена при использовании 16-APSK созвездия CN4-4, но в этом случае энергоэффективность системы очень низкая. Наилучшая энергоэффективность достигается при использовании созвездий CN3-1, но оно обеспечивает более низкую помехоустойчивость радиоканала, чем CN4-4. Это означает, что существует компромисс между показателями пик-фактора и помехоустойчивостью. Поэтому при выборе созвездия APSK необходимо найти оптимальный вариант между помехоустойчивостью и энергоэффективностью.

В данной работе мы проиллюстрировали методы моделирования модуляции APSK. Моделирование выполнено на программе MATLAB. Аналитические и графические результаты, представленные в данной работе, позволяют определить показатели системы

---

(PAPR и SER) при модуляции 16-APSK и их отображение. Эти зависимости могут быть использованы в любых других системах связи, в которых применяется модуляция M-APSK.

#### СПИСОК ЛИТЕРАТУРЫ

1. Смычек, М.А. Технологические сети и системы связи. // учеб. пособие. - 2-е изд. - Москва ; Вологда : Инфра-Инженерия, 2019, 400 с.
2. Marcelo S. Alencar, Valdemar Cardoso da Rocha Jr. Communication Systems // Third Edition. Springer 2022, 358p.
3. Logvinov V.V. and Anh P.T. Controlled Microwave Autogenerator on a Complementary Pair of Mosfet Transistors // 2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Arkhangelsk, Russian Federation, 2022.
4. Фан Т.А., Логвинов В.В. Исследование свойств синхронного свч усилителя, выполненного на комплементарной паре МОП транзисторов // Телекоммуникации и информационные технологии, 2023. Т. 10. № 1. С. 196-205.
5. Anh P.T. and Logvinov V.V. Analysis of the Synchronous Amplifier Properties Using Matlab and Simulation in Microcap Environment // 2023 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Pskov, Russian Federation, 2023.
6. Фан Т.А., Логвинов В.В. Управляемый СВЧ автогенератор на комплементарной паре МОП-транзисторов // Телекоммуникации и информационные технологии, 2022. Т. 9, № 2. С. 166-173
7. Дворкович В.П. Цифровые видеоинформационные системы (теория и практика) // М:Техносфера, 2022.
8. David R. Smith. Digital Transmission Systems // Springer Science & Business Media, 2013, 576 p.
9. D. Dupak, D. Kocur and J. Gazda. Optimization of 16-APSK modulation for SC-FDMA transmission system," 2013 23rd International Conference Radioelektronika (RADIOELEKTRONIKA), Pardubice, Czech Republic, 2013, pp. 249-254, doi: 10.1109/RadioElek.2013.6530926.
10. G. Qin, X. Lin, J. Cai, R. Jin, J. Shi and N. Chi. Capacity of Normal and Probability Shaping APSK/QAM in Visible Light Communication System," 2022 Asia Communications and Photonics Conference (ACP), Shenzhen, China, 2022, pp. 939-943, doi: 10.1109/ACP55869.2022.10088883.
11. T. Fan, W. Xu, L. Wang and L. Zhang. A New APSK-Based M-Ary Differential Chaos Shift Keying Modulation System," in IEEE Communications Letters, vol. 24, no. 12, pp. 2701-2704, Dec. 2020, doi: 10.1109/LCOMM.2020.3019105.
12. R. R. Muller, U. Wachsmann, J. B. Huber. Multilevel coding for peak power limited complex Gaussian channels. Proceedings of IEEE International «Symposium on Information Theory», Ulm, Germany, 1997, pp. 103-110.
13. Digital video broadcasting (DVB): Second generation framing structure, channel coding, and modulation systems for broadcasting, interactive services, news gathering and other broadband satellite applications [Web]. European Telecommunications Standards Institute. Дата обращения: 03.02.2023. URL: [https://www.etsi.org/deliver/etsi\\_en/302300\\_302399/30230702/01.02.01\\_20/en\\_30230702v010201a.pdf](https://www.etsi.org/deliver/etsi_en/302300_302399/30230702/01.02.01_20/en_30230702v010201a.pdf)

## ОСНОВНЫЕ ПОНЯТИЯ И СПОСОБЫ ПРИМЕНЕНИЯ API

Донской государственный технический университет,  
Ростов-на-Дону, Россия

Ключевые слова: API, приложения, микросервис, клиент-сервер, обмен, разработка, онлайн-платформа.

В статье проведено теоретическое исследование, включающее обзор на популярные программные интерфейсы. Описываются форматы API, принцип их работы и выделяются преимущества и недостатки, а также приводится пример работы с API социальной сетью Вконтакте. В результате за счет описания каждого программного интерфейса разработчики могут сделать выбор в пользу того или иного инструмента для создания собственного микросервиса.

A.S. Dvornichenko

## BASIC CONCEPTS AND WAYS OF USING THE API

Don State Technical University,  
Rostov-on-Don, Russia

Keywords: API, applications, microservice, client-server, exchange, development, online platform.

The article presents a theoretical study, including an overview of popular software interfaces. API formats are described, the principle of their operation and advantages and disadvantages are highlighted, as well as an example of working with the V Kontakte social network API is given. As a result, due to the description of each software interface, developers can make a choice in favor of one or another tool for creating their own microservice.

В современном мире разработка программного обеспечения стала неотъемлемой частью нашей жизни. Однако, с ростом количества программ и сервисов, возникает необходимость в их взаимодействии и обмене данными. В этом контексте, API (Application Programming Interface) играет важную роль, предоставляя набор методов и функций, которые позволяют программам взаимодействовать друг с другом и обмениваться информацией. Однако, многие разработчики сталкиваются с проблемой недостаточного знания основных понятий и способов применения API. Особенно это касается выбора подходящего формата интерфейса, который в дальнейшем помогает экономить не только силы и время, но также и деньги компании. В результате, возникают сложности при разработке и интеграции программного обеспечения.

Целью данной статьи является аналитический обзор основных понятий применения API. Задачей является рассмотрение основных принципов API, его ключевых понятий и преимуществ. Также, в задачи входит изучение варианта использования API на конкретном примере, таком как социальные сети.

API – это только интерфейс, предоставляемый неким программным обеспечением. Это абстракция базовой реализации (базовый код – это то, что на самом деле происходит внутри программного продукта при использовании API) [1]. В ходе теоретического исследования будет рассмотрено три популярных формата API: REST API, SOAP API, gRPC. API играет ключевую роль в интеграции и обмене данными между различными системами, ускоряя и упрощая разработку приложений. Каждый из трех форматов API - REST, SOAP и gRPC – имеют свои уникальные характеристики и предпочтительные

---

сценарии использования, такие как эффективность, скорость, масштабируемость и гибкость.

REST (Representational State Transfer) – это архитектурный стиль взаимодействия между компьютерными сетями, который был введен Роем Филдингом. REST-службы предоставляют доступ к текстовым представлениям ресурсов сети и позволяют манипулировать ими, используя единый, предопределенный набор операций [2]. REST API позволяет построить масштабируемые приложения с микросервисной архитектурой, разделяя большие части на более мелкие. Он также широко используется при работе с облачными вычислениями. Благодаря использованию кэша REST API обеспечивает повышенную производительность, что делает его подходящим для масштабирования сайтов и сервисов.

Применение REST API включает:

- разработку микросервисных приложений;
- внесение изменений в базу данных без вмешательства в логику приложения;
- предоставление доступа к программам сторонних поставщиков;
- использование в условиях ограниченной пропускной способности соединения с сервером.

REST API предоставляет доступ клиентским приложениям к данным на сервере через различные методы, такие как POST, GET, PUT и DELETE, используя протокола HTTP и HTTPS для обмена сообщениями.

Важной особенностью REST API является обмен сообщениями без сохранения состояния. Каждое сообщение содержит всю необходимую информацию для обработки и сервер не хранит результаты предыдущих сессий с клиентами. Это позволяет серверу быть гибким и масштабируемым, обеспечивает поддержку асинхронного взаимодействия и возможность реализации сложных алгоритмов обработки. REST API является универсальным, не зависящим от технологий на клиентской или серверной стороне и не привязывает разработчиков к определенному провайдеру.

REST API имеет несколько преимуществ, таких как простота, гибкость и поддержка различных протоколов. Однако, его производительность может быть ниже по сравнению с другими архитектурами, и он может не подходить для работы с большими объемами данных.

SOAP – это протокол, по которому веб-сервисы взаимодействуют друг с другом или с клиентами. Название происходит от сокращения Simple Object Access Protocol («простой протокол доступа к объектам»). SOAP API – это веб-сервис, использующий протокол SOAP для обмена сообщениями между серверами и клиентами. При этом сообщения должны быть написаны на языке XML в соответствии со строгими стандартами, иначе сервер вернет ошибку [3]. С ним связано несколько стандартов, регулирующих каждый аспект обмена данными. Ниже перечислены некоторые из них.

Web Services Security (WS-Security) определяет меры безопасности, такие как использование уникальных идентификаторов – токенов.

Web Services Addressing (WS-Addressing) требует включения маршрутной информации в виде метаданных.

WS-ReliableMessaging стандартизирует обработку ошибок в сообщениях SOAP.

Язык описания веб-сервисов (Web Services Description Language, WSDL) определяет область применения и функции веб-сервисов SOAP.

При отправке запроса в SOAP API необходимо обернуть HTTP-запрос в конверт SOAP. Это структура данных, которая изменяет базовый HTTP-контент в соответствии с требованиями к запросам SOAP. Благодаря конверту вы также можете отправлять запросы веб-сервисам SOAP с помощью других транспортных протоколов, таких как TCP или Протокол межсетевых управляющих сообщений (Internet Control Message Protocol, ICMP). Однако SOAP API и веб-сервисы SOAP всегда возвращают в своих ответах XML-документы.

---

Преимуществами SOAP API являются его структурированность – обеспечивающая четкое и предсказуемое взаимодействие между клиентом и сервером за счет строго определенной структуры, а также он поддерживает различные протоколы и представляет встроенную поддержку для различных механизмов безопасности, таких как шифрование или аутентификация.

Недостатками SOAP API являются его сложность из-за громоздкой структуры требующей большого объема кода для реализации. Также используется сложный формат передачи сообщения, требующий согласованности между клиентом и сервером.

gRPC – это система удаленного вызова процедур с открытым исходным кодом, разработанная компанией Google на основе RPC. RPC предлагает классический стиль API, разработанный достаточно давно и используемый и в настоящее время. gRPC осуществляет вызов процедур для запроса данных с удаленного сервера [4].

gRPC обеспечивает клиент-серверную структуру обмена данными. Открытый программный код фреймворка, несколько режимов обмена информацией между сервисами (как одно-, так и двунаправленные) и простота реализации коммуникационных взаимодействий позволяют обеспечить поддержку фреймворка в большинстве популярных систем разработки, включая NodeJS, C#, Go, Java и JavaScript. ряд преимуществ, среди которых высокая производительность, поддержка множества языков программирования, а также простота в использовании и настройке. Кроме того, gRPC позволяет создавать микросервисы с минимальным временем на разработку и поддержку.

К недостаткам gRPC можно отнести то, что он требует более глубоких знаний в области сетевых протоколов и Java, что может быть сложным для начинающих разработчиков. Кроме того, некоторые библиотеки и инструменты, необходимые для работы с gRPC, могут быть недоступны для всех языков программирования. Также стоит отметить, что gRPC может быть не лучшим выбором для небольших проектов или команд, которые не имеют опыта работы с микросервисами и RPC.

API используются в различных областях, включая веб-разработку, мобильные приложения, игры и даже в работе мессенджеров. Один из примеров использования API – это работа с мессенджерами. Мессенджеры, такие как Telegram, WhatsApp и другие, а также социальные сети, такие как Вконтакте, Одноклассники и другие, используют API для связи с серверами и обмена сообщениями между пользователями. API позволяет разработчикам создавать приложения, которые могут работать с сообщениями, фотографиями, видео и другими типами данных, отправленных через мессенджер.

Платформы социальных сетей получают выгоду от этой дополнительной функциональности без необходимости создавать новые функции самостоятельно. Разработчики получают выгоду от создания новых коммерческих приложений. А пользователи получают выгоду, получая доступ к функциям, создаваемым разработчиками, используя доступ к данным API [5]. Создание и внедрение разработчиками новых микросервисов, работающих с API, делает взаимодействие пользователей с мессенджерами более удобным.

Примером использования API является социальная сеть Вконтакте. Она не только предоставляет свои методы для использования разработчикам, но и сама пользуется методами других микросервисов.

Социальная сеть Вконтакте – одна из самых популярных платформ для общения и обмена контентом в России и странах ближнего зарубежья. Она активно использует API для обеспечения более широкой интеграции с другими сервисами и приложениями. Вконтакте предоставляет разработчикам доступ к разнообразным методам, что позволяет им создавать приложения и расширения, которые обогащают пользовательский опыт.

Одним из ярких примеров использования API Вконтакте является возможность авторизации на сторонних веб-сайтах или приложениях с использованием аккаунта Вконтакте. Это упрощает процесс регистрации и входа для пользователей, так как они

---

могут использовать свои существующие учетные записи Вконтакте. Это также позволяет разработчикам получить доступ к определенной информации пользователя, с их разрешения, для более персонализированного опыта.

Вконтакте также активно взаимодействует с методами других микросервисов. Например, они могут использовать API платежных систем для интеграции оплаты услуг и товаров непосредственно в приложении Вконтакте. Это обеспечивает удобство для пользователей, позволяя им совершать покупки без необходимости покидать социальную сеть.

Более того, Вконтакте предоставляет разработчикам доступ к методам для работы с данными, такими как новостная лента, сообщения, фотографии и видео. Это позволяет создавать приложения, которые интегрируются непосредственно с контентом, созданным пользователями Вконтакте.

Таким образом API играют ключевую роль в современном мире информационных технологий, и их важность продолжает расти с каждым днем. Сегодня API являются неотъемлемой частью множества онлайн-платформ, и одним из ярких примеров успешного использования API является социальная сеть Вконтакте.

Важно отметить, что API не только обогащают функциональность онлайн-платформ, но и способствуют сотрудничеству между различными сервисами. Они позволяют обмениваться данными и взаимодействовать с внешними системами, что содействует развитию новых технологий и инноваций. Благодаря API различные сервисы могут легко интегрироваться друг с другом, что повышает их конкурентоспособность и делает их более привлекательными для пользователей.

Современная цифровая экономика невозможна без API. Они обеспечивают гибкость и масштабируемость систем, позволяют быстро реагировать на изменяющиеся потребности рынка и создавать инновационные продукты и сервисы. Таким образом, API остаются актуальными и важными инструментами для усовершенствования онлайн-платформ, способствуя росту бизнеса, удовлетворению потребностей пользователей и развитию цифровой экономики в целом.

## СПИСОК ЛИТЕРАТУРЫ

1. Арно Лоре. Проектирование веб-API / Пер. с англ. Д. А. Беликова. – М.: ДМК Пресс, 2020.– 440 с.
2. Безрук П.А. Разработка системы распределенного мониторинга компьютерной сети на основе rest API // Актуальные проблемы авиации и космонавтики. – 2017. №13. с. 94-95.
3. SOAP API [Электронный ресурс] // skillfactory media : [сайт]. — URL: <https://blog.skillfactory.ru/glossary/soap-api/> (дата обращения: 01.10.2023).
4. Резединова, Е. Ю., Кыркунов, П. Н., Сергеев, А. В. Выбор сервис-ориентированной архитектуры для создания сервиса по благоустройству города / Е. Ю. Резединова, П. Н. Кыркунов, А. В. Сергеев // Системный анализ в проектировании и управлении. 2023. № 3. с. 168-177.
5. Объяснение API социальных сетей (простыми словами) [Электронный ресурс] // moyens : [сайт]. — URL: <https://ru.moyens.net/социальные-сети/179300/объяснение-апи-социальных-сетей-простым/> (дата обращения: 02.10.2023).



## **МНОГОЧАСТОТНЫЕ АНТЕННЫ СИСТЕМЫ СОТОВОЙ СВЯЗИ**

Военный учебно-научный центр ВВС «Военно-воздушная академия имени профессора  
Н.Е. Жуковского и Ю.А. Гагарина», Воронеж, Россия<sup>1</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: антенна, антенная решетка, многочастотные антенны.

В статье рассмотрен вариант построения антенной системы сотовой радиосвязи, которая обеспечит работу в двухчастотных диапазонах за счет задействования различных подрешеток излучателей, расположенных на одной несущей конструкции.

**V.V. Kharchenko<sup>1</sup>, S.V. Rudyy<sup>1</sup>, A.E. Vartazarova<sup>1</sup>, N.V. Boldyrikhin<sup>2</sup>**

## **MULTI-FREQUENCY ANTENNAS OF CELLULAR COMMUNICATION SYSTEMS**

Military educational scientific center air force "Air force Academy named after Professor N. E.  
Zhukovsky and Y. A. Gagarin", Voronezh, Russia<sup>1</sup>

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: antenna, antenna array, multi-frequency antennas.

The article considers a variant of constructing an antenna system of cellular radio communication, which will provide operation in two frequency ranges by using various sublattices of emitters located on the same supporting structure.

При организации радиосвязи часто возникает необходимость обеспечить возможность передачи информации в различных частотных диапазонах. Для решения такой задачи возможно использование совокупности антенно-фидерных устройств, каждое из которых обеспечит передачу информации в определенном диапазоне частот. Однако перспективным видится использование антенных систем, которые позволят реализовать функции нескольких антенн в одной антенной конструкции, что, несомненно, улучшит показатели надежности и экономическую эффективность комплексов связи в целом.

В условиях постоянно усложняющейся электромагнитной обстановки в районах эксплуатации большого числа радиотехнических средств антенные системы комплексов радиосвязи должны отвечать все более высоким требованиям, предъявляемым к ним. Улучшение показателей, по которым оценивается эффективность функционирования комплекса радиосвязи в целом, в большой степени зависит от характеристик антенных систем, структурно входящих в этот комплекс.

В последние годы в связи с развитием систем сотовой связи новых поколений возникла необходимость разработки многочастотных антенн для базовых станций в диапазонах 900, 1800, 2000 МГц и выше.

В частности, для повышения скорости передачи данных, пропускной способности канала связи, связанной с ней помехоустойчивостью и улучшения электромагнитной обстановки возможно применение многочастотных антенных решеток, которые позволят заменить целый ряд антенно-фидерных устройств, каждое из которых функционирует в своем частотном диапазоне [1].

В качестве многочастотной антенны системы сотовой связи может рассматриваться цилиндрическая антенная решетка щелевых излучателей, варианты построения которой представлены на рисунке. 1.

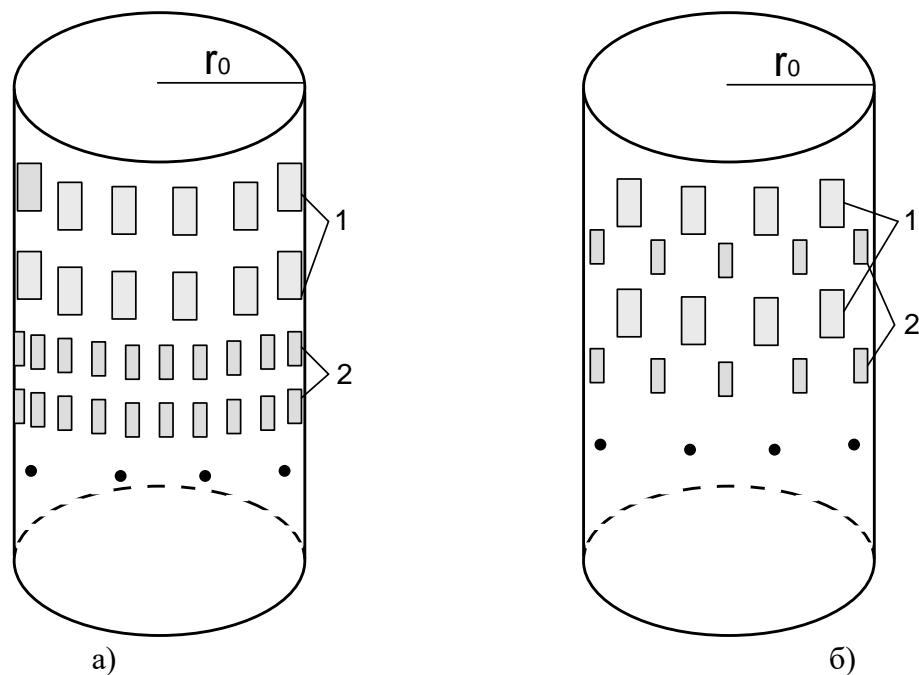


Рисунок 1. Варианты построения многочастотной антенны

Варианты построения многодиапазонной цилиндрической АР, представленные на рисунках 1а и 1б отличаются геометрическим расположением излучателей, формирующих кольцевые антенные решетки 1 и 2. Предполагается, что на одной несущей конструкции можно будет расположить 3-4 кольцевые антенные решетки, работающие в разных частотных диапазонах. При этом должны быть учтены все электродинамические особенности размещения излучателей в соседних решетках, и, в первую очередь, их взаимная связь в решетках.

В системах сотовой связи важным вопросом является возможность обеспечить передачу данных в заданном направлении. Причем в азимутальной плоскости антенной системы должна быть обеспечена передача в диапазоне углов от 0 до 360 градусов. Предлагаемая цилиндрическая конструкция антенны позволит это осуществить электрическим способом, при этом излучающая система находится на одной несущей поверхности в отличие от используемых в настоящее время секторных антенных систем.

Кроме того, известно [2, 3], что наиболее полно совокупности требований по обеспечению заданного сектора сканирования, возможности быстрого углового перемещения главного максимума диаграммы направленности (ДН), независимости характеристик излучения от направления сканирования удовлетворяет цилиндрическая антенная решетка (ЦАР). При этом, для снижения уровня бокового и заднего излучения в таких антеннах может быть использовано спадающее амплитудно-фазовое распределение в излучающем раскрытии антенной решетки (АР).

Особенностью электродинамического анализа предлагаемой модели многочастотной антенны является то, что рассмотренный в [4] подход хоть и является общим, для каждого диапазона будет отличаться значениями частотно-зависимых геометрических и электрофизических параметров антенной конструкции. Кроме того, при решении задач синтеза и анализа многочастотной антенны одним из основных вопросов будет являться оценка и учет взаимной связи излучателей не только в составе решетки (одного диапазона), но и в большей степени взаимного влияния излучателей кольцевых решеток различного диапазона.

---

## СПИСОК ЛИТЕРАТУРЫ

1. Пономарев Л.И., Степаненко В.И. Сканирующие многочастотные совмещенные антенные решетки // Под ред. Л.И. Пономарева. – М.: Радиотехника, 2009. – 328 с.
2. Габриэлян Д.Д., Звездина М.Ю., Лабунько О.С., Харченко В.В. Метод расчета проводимости щелей на круговом цилиндре под слоем магнетодиэлектрика. // Электромагнитные волны и электронные системы, 2005, вып. 5. – С. 24-29.
3. Инденбом М.В. Антенные решетки подвижных обзорных РЛС. Теория, расчет, конструкции // Монография. – М.: Радиотехника, 2015. – 416 с.
4. Петров Б.М. Электродинамика и распространение радиоволн // Учебник. М.: Горячая линия – Телеком, 2014. – 558с.

**Е.А. Карпенко, А.М. Коршун**

### **НЕЙРОСЕТЕВАЯ ВИДЕОАНАЛИТИКА КАК ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ РАЗВИТИЯ ВИДЕОНАБЛЮДЕНИЯ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: нейросетевая видеоаналитика, классическая видеоаналитика, безопасность, нейронная сеть.

В статье рассмотрены положительные и отрицательные стороны классической и нейросетевой видеоаналитики. Основные этапы работы и задачи, которые охватывает нейросетевая видеоаналитика, как составляющая комплексной безопасности и контроля технологического процесса.

**E.A. Karpenko, A.M. Korshun**

### **NEURAL NETWORK VIDEO ANALYTICS AS A PROMISING DIRECTION OF VIDEO SURVEILLANCE DEVELOPMENT**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: neural network video analytics, classical video analytics, security, neural network.

The article discusses the positive and negative aspects of classical and neural network video analytics. The main stages of work and tasks covered by neural network video analytics as a component of integrated security and process control.

На сегодняшний день обеспечение безопасности и контроля технологического процесса занимает значительное место в современном мире. Постоянный рост количества камер снижает человеческое восприятие, тем самым обработка видеопотока и принятие решения снижается в десятки раз. Решение данной проблемы стала внедрение видеоаналитики в системы видеонаблюдения. Это значительно повысило качество контроля видеопотока, так как по средствам детекторов видеоаналитики встроенных в камеру появилась возможность фиксировать нарушения. В данном случае значительно

---

улучшило качество безопасности объектов и технологического процесса, но тем самым оставило и нерешенные задачи, такие как:

Принятие решения зависит от человеческого фактора, что тоже снижает качество контроля и обеспечения безопасности;

Невозможность выполнения специфических или узких задач потребителей.

Решением данных проблем стало обучение интеллектуального видеонаблюдения правильной оценке видеопотока и самостоятельному принятию решения. Аппаратной реализацией данной проблемы являются нейросетевая видеоаналитика, где совокупность нейронных сетей и детекторов видеоаналитики обеспечат необходимый уровень оценке вероятности угрозы безопасности и принятия правильного решения по ее предоставлению.

Классический вид видеоаналитики можно применять для простых и четких задач, где не требуется ресурсоемкость оборудования. При более сложных задачах, где необходимо использовать универсальный метод можно использовать метод нейросетевой видеоаналитики. Для создания нейронной сети необходимо большое количество изображений, чтобы дальнейшее обучение и анализ работы проходил более эффективно. [1]

Весь материал выборки для обучения нейронной сети должен быть аналогичен условиям работы данной сети при реализации проекта. В противном случае работа данной сети будет некорректной, и выдавать низкий уровень эффективности работы.

Нейронная сеть представляет собой нейроны иерархически соединенные в сети, где выход одних нейронов является входом для других нейронов. Мы можем представить такие сети в виде соединенных слоев с узлами. Каждый узел принимает взвешенный вход, активирует активационную функцию для суммы входов и генерирует выход.

При разработке нейронной сети можно выделить 3 основных этапа:

1. Сбор материала и подготовка обучающей выборки. Подготовленный материал должен быть собран при аналогичных условиях работы нейросетевой видеоаналитики.
2. Обучение. Видео материал нарезается на отдельные видеоизображения в ручном режиме, происходит единообразная разметка объектов в кадре [2]
3. Анализ качества работы сети. Во время обучения выборка нейронной сети разбивается на текстовую и обучающую, и по окончании промежуточного этапа при запуске тестовой части выборки можно оценить качество работы нейронной сети

К задачам, которые на сегодняшний день может охватить нейросетевая видеоаналитика, относятся:

1. Обнаружение объектов. Нейросеть способна обнаружить объект, а также покадрово проследить перемещение и построить траекторию движения. Исходя из заданных параметров понять, что происходит с данным объектом и принять решение.
2. Движение человека. Нейросеть способна обнаруживать конечности и позы человека и из заданных параметров оценивать текущую ситуацию, а также считать это противоправными действиями или нет.

Также нейросетевая видеоаналитика способна выполнять более сложные и составные виды задач. К таким задачам можно отнести:

1. Обнаружение и фильтрация объекта и в итоге принятия решения о контроле действий
2. Обнаружение и классификация действий человека и в итоге принятия решения о его контроль

Следует отметить, что нейросетевая видеоаналитика хоть и может обеспечить решением большое количество сценариев безопасности и контроля технологического процесса, но также на данный момент остаются задачи, которые очень сложно решить данным методом. На сегодняшний день именно совокупность классического и

---

нейросетевого подхода видеоаналитики сможет охватить больше задач связанных с безопасностью и контролем технологического процесса.

#### СПИСОК ЛИТЕРАТУРЫ

1. Карпенко Е.А. Анализ функций видеоаналитики интеллектуального видеонаблюдения как составляющей комплексной безопасности. Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2022 с 34-36.
2. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение / пер. с англ. А. А. Слинкина. – 2-е изд., испр. – М.: ДМК Пресс, 2018 – 652 с.: цв. ил.

**Ба М.**

#### **ПОСТРОЕНИЕ КВ ПРИЕМНИКА-СКАНЕРА ДЛЯ ОБНАРУЖЕНИЯ ЛЧМ-СИГНАЛОВ ЗОНДИРОВАНИЯ НА ОСНОВЕ HACKRF ONE**

Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Ростов-на-Дону, Россия

Ключевые слова: Обработки сигналов, ЛЧМ-передатчики, широкополосный программно-определяемый радиоприемник (HackRF One), короткие волны, фреймворк GNU RADIO, ЛЧМ-зондирования, программирование, разработка.

Показана возможность построения КВ приемника-сканера для обнаружения ЛЧМ-передатчиков на основе трансивера HackRF One с использованием среды разработки GNU RADIO. Представлен действующий КВ приемник-сканер, который позволяет не только обнаружить ЛЧМ-передатчики, но и обеспечить запись квадратурных компонент сигналов в полосу до 2МГц в бинарный файл для постреальной обработки и демодуляции отдельных выделенных сигналов. Приведены результаты экспериментальной апробации разработанного программного обеспечения для цифрового приемника HackRF One.

**Ба М.**

#### **DEVELOPMENT OF A SHORTWAVE RECEIVER-SCANNER FOR DETECTING SOUNDING CHIRP BASED ON HACKRF ONE**

Federal State Autonomous Educational Institution of Higher Education "Southern Federal University", Rostov-on-Don, Russia

Keywords: Signal processing, chirp transmitters, wideband software-defined radio receiver (HackRF One), short waves, GNU RADIO framework, chirp sounding, programming, development.

The possibility of developing a HF receiver-scanner for detecting chirp transmitters based on the HackRF One transceiver using the GNU RADIO development environment is shown. An operating HF receiver-scanner is presented, which allows not only to detect chirp transmitters, but also to ensure the recording of quadrature components of signals in a band up to 2 MHz into a binary file for post-real processing and demodulation of individual selected signals. The results of experimental testing of the developed software for the HackRF One digital receiver are presented.

Одной из практически важных задач КВ связи и радиопеленгации является мониторинг ионосферы. Эти задачи являются следующие: определения высот отражения радиоволн КВ диапазона от ионосферы, значений максимально наблюдаемых частот, выше которых возможно просачивание сквозь ионосферы и ниже которых происходит отражение радиоволн от ионосферы (МНЧ), определение по результатам зондирования зависимости концентрации электронов от высоты (высотное распределение концентрации электронов) и зависимости действующей высоты отражения от ионосферы от частоты зондирования (высотно-частотная характеристика) [1, 2].

Для определения выше перечисленных характеристик ионосферы применяются различные методы ионосферного зондирования (вертикальное, наклонное, возвратно-наклонное, трансionoсферное зондирования и внешнее радиозондирование) с помощью современных программно-аппаратных комплексов так называемых ионозондов [2, 3]. Среди излучаемых сигналов ионозондами для зондирования ионосферы, часто используют непрерывный ЛЧМ-сигнал, который излучается передатчиком, отражается от ионосферы и приходят на земную поверхность в область приема, где фиксируется групповая задержка на распространение [3]. ЛЧМ-сигналы также применяются в радиолокации для повышения точности измерений. Однако, к сожалению, режимы работы ЛЧМ-передатчиков неизвестны [4, 5]. Поэтому задача разработки КВ приемника-сканера для обнаружения ЛЧМ-сигналов, а также для определения режимов работы передатчиков: старт с нулевой частоты (chirptime), скорость перестройки частоты, период зондирования, является актуальной. Решение этой задачи позволяет в дальнейшем осуществить настройку приемной части ЛЧМ-зонда и получить ионограммы наклонного зондирования ионосферы от обнаруженных ЛЧМ-передатчиков. В связи с этим целью работы является: разработка на основе широкополосного трансивера HackRF One КВ приёмника-сканера с использованием бесплатного программного обеспечения GNU Radio, который обеспечивал бы решения задач обнаружения ЛЧМ сигналов зондирования ионосферы и определение их параметров.

## РАЗРАБОТКА ПРИЕМНИКА.

Как было выше сказано для реализации КВ приемника используются трансивер HackRf One [6, 7] и специальное программное обеспечение с открытым исходным кодом, которое позволяет выполнять обработку сигналов [8, 9]. На Рис.1 представлена реализация КВ приемник-сканера для обнаружения ЛЧМ-сигналов зондирования.

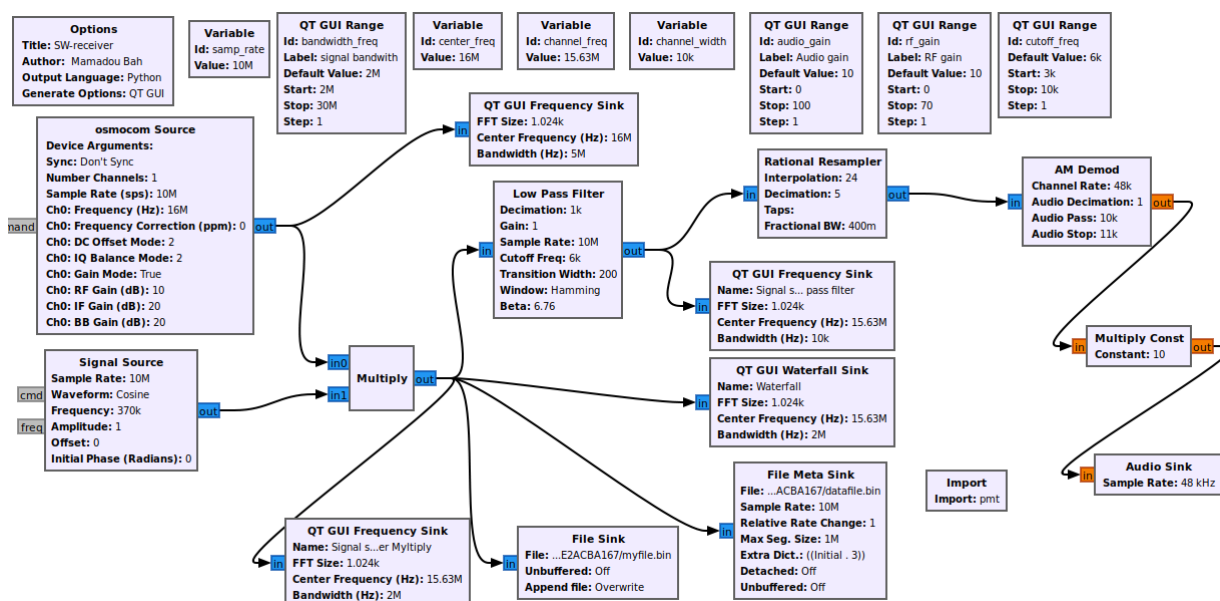


Рисунок 1. Блок-схема реализации КВ приемника-сканера для обнаружения ЛЧМ-сигналов зондирования на основе HackRF One

Блок-схема для обнаружения ЛЧМ-сигналов зондирования начинается с блока приёмника (osmoscom source), который настраивается на центральную частоту, например, равную 16МГц. Этой центральной частотой управляет блок Variable с идентификатором id: center\_freq. В блоке Osmocom Source также настраивается ВЧ-усиление, которое регулирует блок QT GUI Range с идентификатором id: rf\_gain. Частота дискретизации в блоке равна 10МГц, которая задается блоком Variable с идентификатором id: samp\_rate. Затем сигнал подается одновременно на два блока (QT GUI Frequency sink и Multiply).

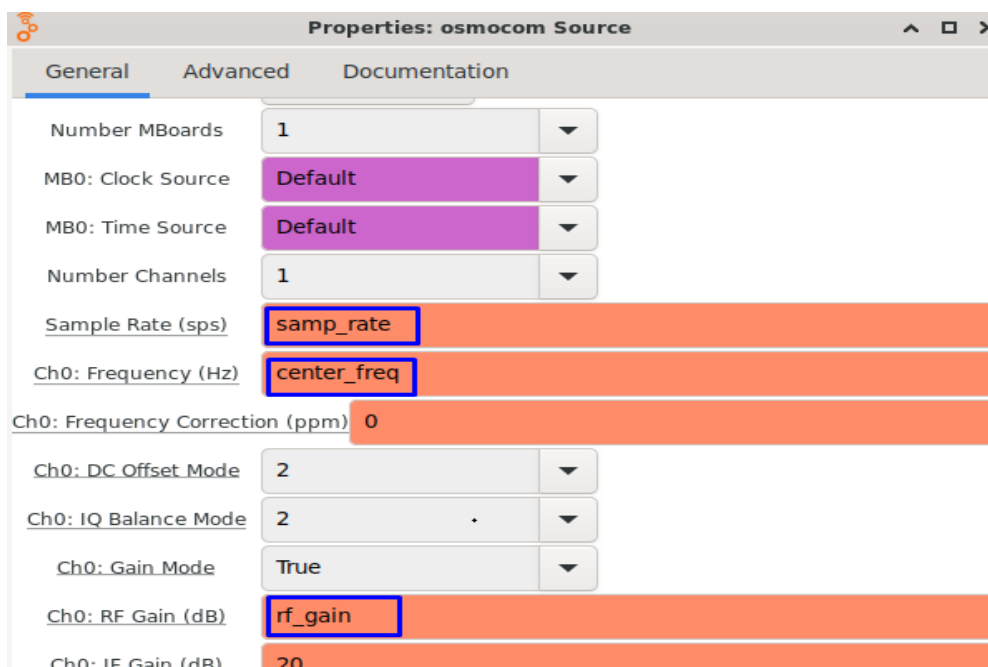


Рисунок 2. Установка параметров Блока Osmocom Source

Блок QT GUI Frequency sink применяет к принятому сигналу преобразование Фурье с длиной выборкой, равной 1024, центральной частотой – 16МГц, и затем рисует обзорный спектр. Из обзорного спектра выбираем частоту, интересующего нас сигнала. В данном примере она равна 15,6МГц.

Блок Multiply умножает принятый сигнал на генерированный синусоидальный сигнал блока Signal source, чтобы сместить интересующую нас частоту в центр спектра. Частота генерированного сигнала равна разнице между центральной частотой обзорного спектра и интересующей нас частотой - 0,4МГц или 370кГц.

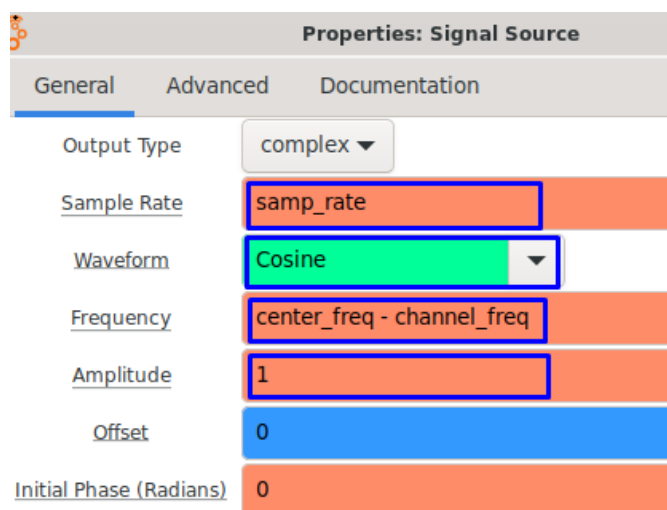


Рисунок 3. Установка параметров блока signal source

Из Блока Multiply умноженный сигнал передается параллельно на пять блоков (QT GUI Frequency sink, File sink, File Meta sink, QT GUI Waterfall sink и Low Pass Filter). Блок QT GUI Frequency применяет к сигналу преобразование Фурье с длиной выборкой 1024, центральной частотой (выбранная нами частота) - 15,6МГц и рисует спектр с шириной – 2МГц. Блок File sink и File Meta sink осуществляют запись квадратурных компонентов принятого сигнала в бинарный файл. Причем Блок File Meta sink не только записывает квадратурные компоненты в бинарный файл, но и заголовки метаданных. Заголовки содержат информацию о типе данных и свойствах данных в следующем сегменте выборки.

Блок QT GUI Waterfall, по сути, это Окно водопада, на котором отображаются сигналы радиочастотного спектра. Т.е. зависимость от времени спектральной плотности мощности в установленной полосе частот. В этом же окне будет отображаться след ЛЧМ-сигнала с шириной спектра до 2МГц.

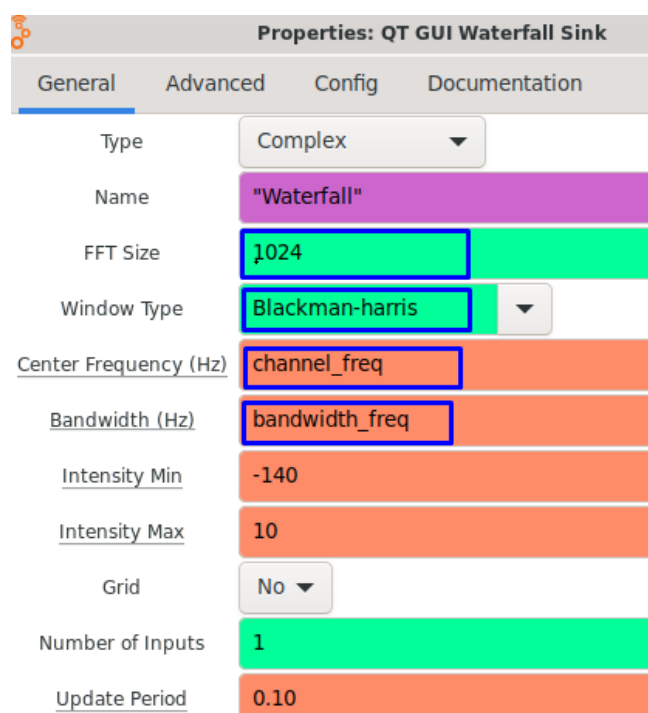


Рисунок 4. Установка параметров блока Водопада

Блок Low Pass Filter это низкочастотный фильтр с следующими параметрами:

- Частота среза – 6кГц,
- Полоса заграждения – 200Гц,
- Для визуального улучшения частотного спектра на разрыве границ окна применяется окно Хеннинга,
- Частота дискретизации – 10МГц, к которой применяется децимация за счёт коэффициентом децимации НЧ- фильтра.
- Коэффициент децимации – 1000 или частота дискретизация делит на ширину канала, где ширина канала равна 10кГц и задается блоком Variable с идентификатором id: channel\_width.



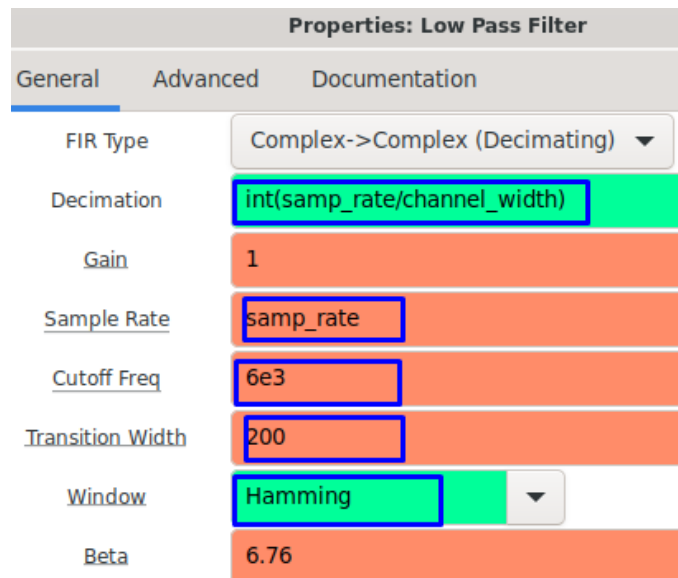


Рисунок 5. Описание параметров низкочастотного фильтра

После фильтра низкочастотный сигнал с частотой дискретизации 10кГц проходит через блок (Rational Resampler), который применяет операции децимации и интерполяции к принятому сигналу. В данном случае коэффициенты интерполяции – 24 и децимации – 5. С блока Rational Resampler сигнал с частотой дискретизацией – 48кГц подается на амплитудный демодулятор (AM demod). Далее сигнал передается на звуковую карту компьютера через блок Multiply const, который контролирует громкость. Значение блока Multiply const задается блоком Qt GUI Range с идентификатором id: audio\_gain.

### РЕЗУЛЬТАТЫ РАБОТЫ КВ ПРИЕМНИКА-СКАНЕРА.

После разработки приемника была выполнена его экспериментальная апробации. Приемником были обнаружены ЛЧМ-сигналы загоризонтных радиолокаторов, размещенных на острове КИПР, трасса наклонного зондирования на трассе Кипр-Ростов-на-Дону. Параметры кипрских передатчиков ЛЧМ сигналов, следующие:

- Мощность -2 мВт
- Период - 5 минут
- Начальная частота -  $f_{на} = 8$  МГц
- Скорость перестройки -  $\frac{df}{dt} = 100$  кГц/с = 0,1 МГц

Для того, чтобы определять время проявления ЛЧМ-сигнала с периодом 5 минут, излученного передатчиком Кипра необходимо сначала найти разницу между частотой настройки разработанного приемника (15,6МГц) и начальной частотой передающего устройства Кипра (8 МГц)  $\Delta f = 15,6 - 8 = 7,6$  МГц. Далее разделить эту разницу на скорость перестройки частоты передатчика, т.е.  $\Delta t = \frac{7,6\text{МГц}}{0,1\text{ МГц/с}} = 76 \text{ с} = 1\text{мин}16\text{с}$ .

Расчеты показывали, что с заданными параметрами ЛЧМ сигнал зондирования передатчика Кипра появляется каждую минуту и 16 секунд с периодом 5 минут. На Рис. 6, 7, 8 представлены спектральные диаграммы и окно радиочастотного водопада до и при проявлении ЛЧМ сигнала зондирования.

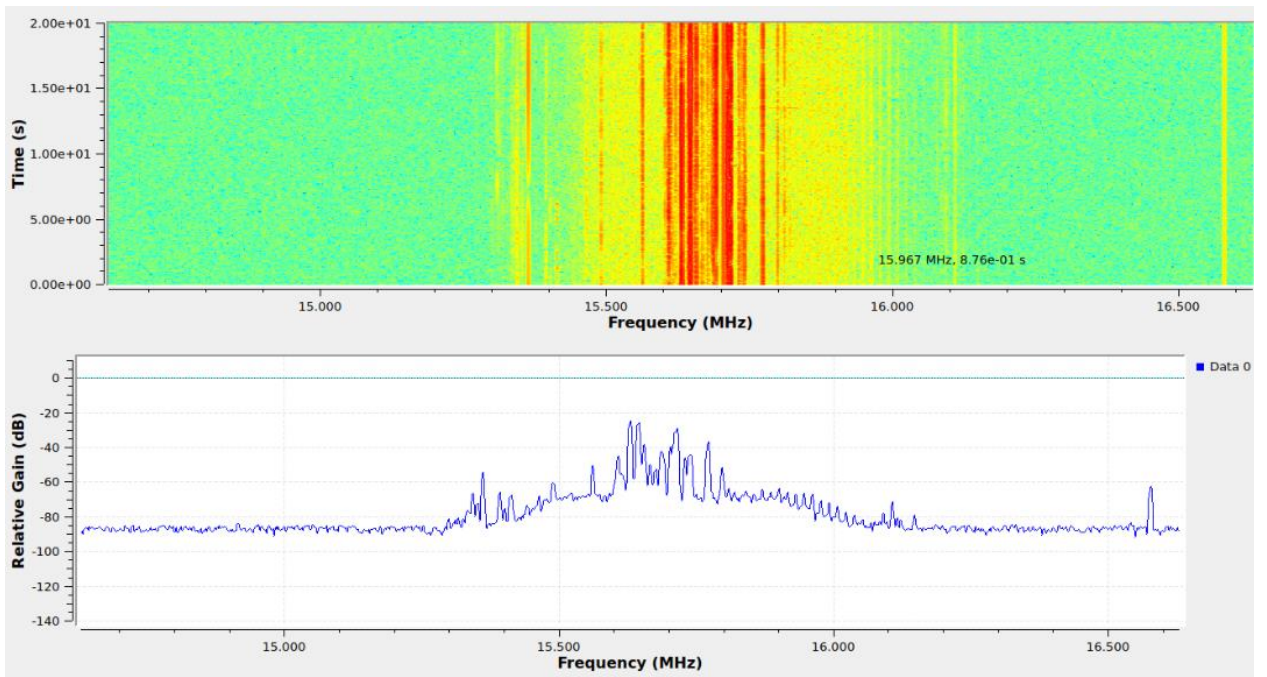


Рисунок 6. Спектральные диаграммы и окно радиочастотного водопада до проявления ЛЧМ сигнала зондирования

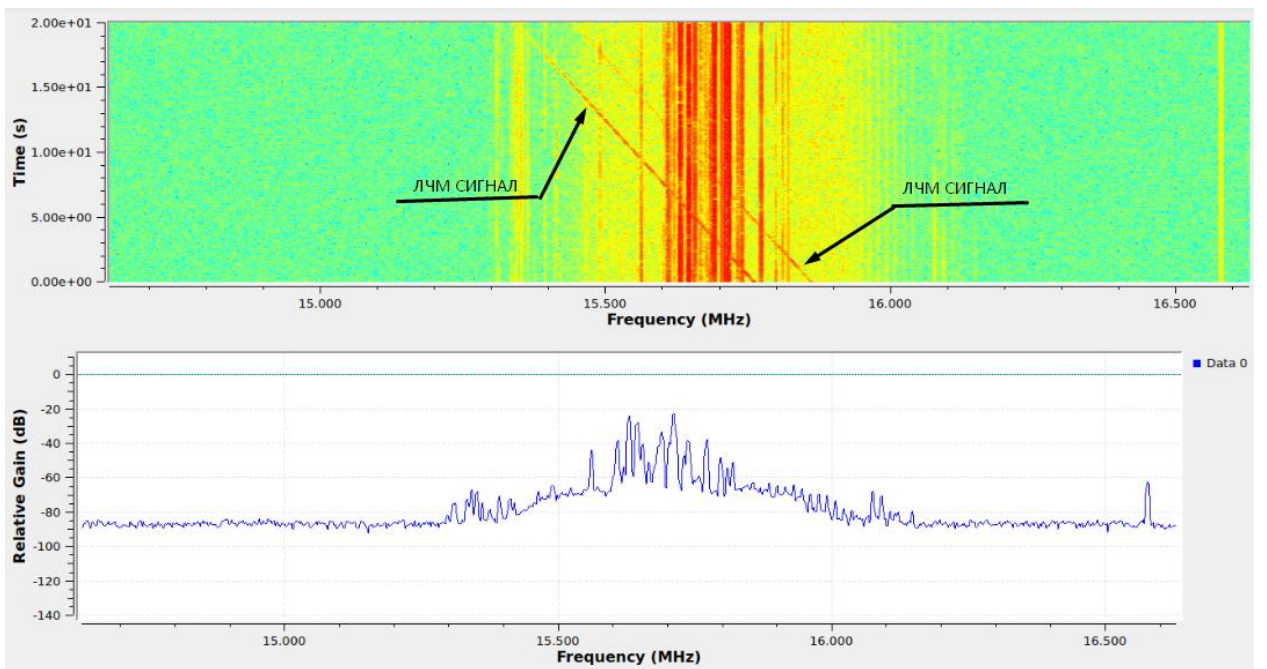


Рисунок 7. Спектральные диаграммы и окно радиочастотного водопада при проявлении ЛЧМ сигнала зондирования с длиной выборкой – 102

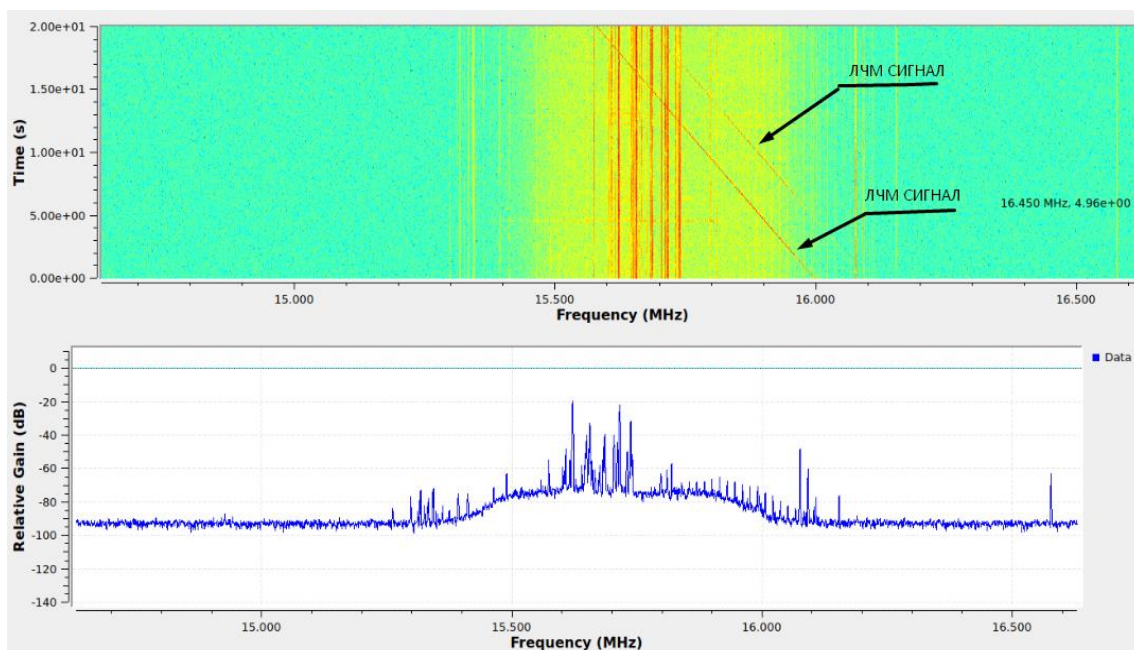


Рисунок 8. Спектральные диаграммы и окно радиочастотного водопада при проявлении ЛЧМ сигнала зондирования с длиной выборкой 4 раза больше, чем предыдущие – 4096

### ЗАКЛЮЧЕНИЕ.

С использованием свободного программного обеспечения GNU Radio на основе HackRF One разработан цифровой приемник-сканер, предназначенный для обнаружения ЛЧМ-сигналов зондирования ионосферы.

Разработанный приемник протестирован экспериментально для решения задач обнаружения ЛЧМ-передатчиков.

Показано, что разработанное программное обеспечение для HackRF One обеспечивает обнаружение ЛЧМ-передатчиков загоризонтной радиолокации, размещенных на острове Кипр.

Цифровой приемник дополнительно обеспечивает функцию записи квадратурных компонент сигналов в бинарный файл в полосе до 2 МГц для постстрельной обработки с целью определения режимов функционирования ЛЧМ-передатчиков.

### СПИСОК ЛИТЕРАТУРЫ

1. М.Г. Дёминов. Ионосфера Земли: закономерности и меха. URL: <https://izmiran.ru/IZMIRAN75/STP/Deminov.pdf>
2. <https://ru.wikipedia.org/wiki/Ионозонд>
3. Сеть ЛЧМ-ионозондов. URL: <http://dep1.iszf.irk.ru/Сеть%20ЛЧМ-ионозондов>
4. GNU Chirp Sounder. URL: [https://www.sgo.fi/~j/gnu\\_chirp\\_sounder/](https://www.sgo.fi/~j/gnu_chirp_sounder/)
5. Chirp reception and interpretation. URL: <http://websdr.ewi.utwente.nl:8901/chirps/article/>.
6. Great Scott Gadgets. HackRF. USER DOCUMENTATION. — [https://hackrf.readthedocs.io/\\_/downloads/en/latest/pdf/](https://hackrf.readthedocs.io/_/downloads/en/latest/pdf/) - Jan 12, 2022.
7. Repository of HackRF One. URL: <https://github.com/greatscottgadgets/hackrf>
8. GNU Radio Manual and C++ API Reference. URL: [https://www.gnuradio.org/doc/doxygen/group\\_\\_base\\_\\_blk.html](https://www.gnuradio.org/doc/doxygen/group__base__blk.html)
9. Alberto A Del Barrio José P Manzano, Víctor M Maroto , Alvaro Villarín , Josué Pagan , Marina Zapater , José Ayala and Román Hermida. - HackRF + GNU Radio: A software-defined radio to teach communication theory. URL: [https://oa.upm.es/64403/1/INVE\\_MEM\\_2019\\_326496.pdf](https://oa.upm.es/64403/1/INVE_MEM_2019_326496.pdf)

**РАДИОЭЛЕКТРОННЫЕ СРЕДСТВА ВОЕННО-ИНЖЕНЕРНОЙ СЛУЖБЫ  
ВЬЕТНАМСКОЙ НАРОДНОЙ АРМИИ И ПЕРСПЕКТИВА ИХ РАЗВИТИЯ**

Ордена Трудового Красного Знамени федеральное государственное Бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», Москва, Россия<sup>1</sup>  
Институт машиноведения им. А.А. Благонравова Российской академии наук, Москва, Россия<sup>2</sup>

Ключевые слова: средства поиска взрывоопасных предметов, металлоискатель, металлообнаружитель, магнитометрический метод, индукционный метод, метод нелинейной радиолокации, радиоэлектронные средства инженерного обеспечения, гуманитарное разминирование, неразорвавшиеся боеприпасы, машинное зрение, информационно-телекоммуникационное оборудование, самодельное взрывное устройство, интеллектуальное управление взрывом.

В статье основное внимание уделено электромагнитным методам и средствам поиска взрывоопасных предметов, используемым военно-инженерной службой Вьетнамской народной армии. Рассмотрены физические основы и принципы действия, преимущества и недостатки поисковых приборов, находящихся на вооружении службы. Предлагается расширить номенклатуру поисковых приборов службы за счет оснащения подразделений нелинейными радиолокационными станциями с повышенной точностью измерения угловых координат. Показано, что неразорвавшиеся боеприпасы и терроризм, осуществляемый с применением радиоэлектроники во взрывных устройствах, вызывают озабоченность политического и военного руководства Социалистической республики Вьетнам, так как препятствуют эффективному природопользованию и загрязняют водные источники.

Pham Duc Huy<sup>1</sup>, Nguyen Van Cuong<sup>1</sup>, A.V. Nikolaev<sup>1,2</sup>

**RADIO-ELECTRONIC MEANS OF THE MILITARY ENGINEERING SERVICE OF  
THE VIETNAMESE PEOPLE'S ARMY AND PROSPECTS FOR THEIR  
DEVELOPMENT**

Moscow Technical University of Communications and Informatics, Moscow, Russia<sup>1</sup>  
Mechanical Engineering Research Institute of the Russian Academy of Sciences,  
Moscow, Russia<sup>2</sup>

Keywords: explosive search means, metal detector, metal detector, magnetometer method, induction method, nonlinear radar method, radio-electronic engineering means, humanitarian demining, unexploded ordnance, machine vision, information and telecommunication equipment, improvised explosive device, intelligent explosion control.

The article focuses on electromagnetic methods and means of searching for explosive objects used by the military engineering service of the Vietnam People's Army. The physical basis and principles of operation, advantages and disadvantages of the search devices in service are considered. It is proposed to expand the nomenclature of search devices of the service by equipping units with nonlinear radar stations with increased accuracy of angular coordinates measurement. It is shown that unexploded ordnance and terrorism carried out with the use of radio-electronics in explosive devices are of concern to the political and military leadership of the Socialist Republic of Vietnam, as they hinder effective environmental management and pollute water sources.

---

### **Актуальность.**

Проблема поиска и обнаружения неразорвавшихся боеприпасов после войны, развязанной американскими агрессорами, при гуманитарном разминировании территорий социалистической республики Вьетнам является серьезной и актуальной, как и для других стран мира. Распространяющийся по всему миру терроризм, осуществляемый с помощью самодельных взрывных устройств (СВУ), наблюдаемая во всем мире урбанизация боевого пространства и использование «умных» боеприпасов с машинным зрением могут стать новой потенциальной угрозой для мирной жизни вьетнамского народа.

Основными предпосылками усугубления проблемы и возникновения угрозы стали: стремительный рост военного потенциала отдельных стран азиатско-тихоокеанского региона, обладающих оборонными технологиями; высокие темпы развития производства микроэлектроники, радиоэлектроники и средств информатизации, увеличение доли специалистов в области радио- и IT технологий.

Все это, а также многое другое указывает на перспективу широкого применения американскими агрессорами и их союзниками азиатско-тихоокеанского региона, включая поддерживаемыми ими террористическими организациями, боеприпасов с машинным зрением и интеллектуальным управлением, в том числе и СВУ.

Дальнейшее развитие радиоэлектронных средств инженерного обеспечения Вьетнамской народной армии может быть ориентировано на использование метода подповерхностной радиолокации, например путем детектирования второй и третьей гармоник сигналов, рассеянных объектами, содержащими в своем составе электронную компонентную базу и контакты с оксидными пленками.

### **Результаты исследований.**

По оценке военно-инженерной службы Вьетнамской народной армии доля неразорвавшихся бомб, мин и взрывчатых веществ (ВВ) на территории Вьетнама составляет 2-5% от количества боеприпасов (эквивалентно примерно 350-800 тыс. тонн), использованных США при бомбометаниях в 1960-1975 гг. При военном применении в отношении Вьетнама «умных» боеприпасов ожидаемо встанет вопрос об использовании Вьетнамской народной армией радиоэлектронных средств поиска, обладающих большой дальностью обнаружения, высоким темпом разведки и точностью измерения координат по азимуту и дальности.

По оценкам вьетнамских ученых, полученным в ходе научно-исследовательской работы «Исследование и картографирование загрязнения бомбами, минами и взрывчатыми веществами страны», количество бомб, мин и ВВ до сих пор разбросано по большинству областей и городов республики (см. рис. 1), в каждом населенном пункте, в сельской и городской местности, в лесах и густых зарослях джунглей, на дне прудов и озер, в море и т.д. [1]. Они представляют до сих пор угрозу, оказывая существенное влияние на развитие экономики, жизнь мирного вьетнамского народа, препятствуют эффективному природопользованию и загрязняют водные источники. В данной работе отмечается, что в течение многих лет периодически возникают техногенные аварии на природоохранных объектах, вызванные взрывом неразорвавшихся боеприпасов, и они продолжаться и дальше, если не будут внедрены дистанционные методы и средства подповерхностной локации для безопасного, точного, ускоренного поиска и уничтожения взрывоопасных предметов (ВОП).

В Социалистической республике Вьетнам задачу по поиску и обнаружению неразорвавшихся боеприпасов, оставшихся после войны, выполняет военно-инженерные службы в целях обеспечения безопасности государства и защиты населения. Кроме того, в настоящее время на службу возложены задачи по поиску и обезвреживанию СВУ, в общественных местах, в т.ч. при проведении массовых мероприятий.



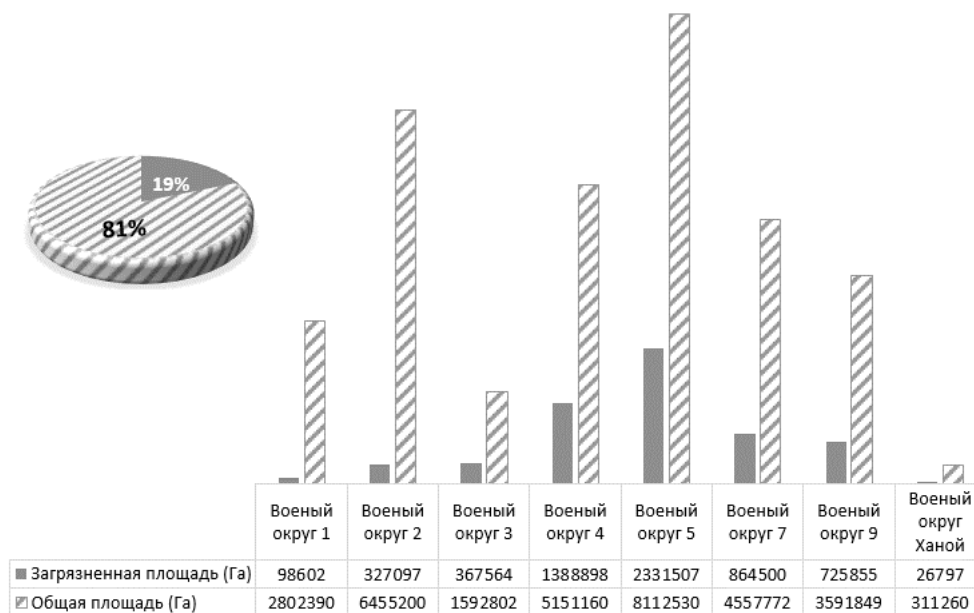


Рисунок 1. Общая доля и соотношения не разминированной площади республики и военных округов [1]

Весь арсенал используемых саперами военно-инженерной службы Вьетнамской народной республики средств поиска ВОП представлен на рисунках 2, 3.



Щуп-зонд сапера



Кинолог с минно-розыскной собакой

Рисунок 2. Поиск ВОП с использованием механического зондирования грунта и обоняния собак-детекторов

Два простых способа для поиска ВОП, используемых в военно-инженерной службе, составляют метод механического зондирования грунта и газоаналитический метод детектирования паров ВВ с помощью собак, физические основы и принципы действия которых представлены ниже.

**Метод механического зондирования грунта** реализуется с использованием щупов-зондов, предназначенный для поиска различных твердых ВОП под грунтом или в кустах, которые не видны саперу. Щупы могут быть длинные или короткие, сделанные из стали. Длинные щуп имеют длины 1,5 - 1,8 м с диаметром 8 мм, а короткие щупы - длина 0,6 - 0,8 м с диаметром 6 мм. В настоящее время щупы стали делать из непроводящих материалов с

---

целью исключения подрыва сапера на mine-ловушке с электрическим контактным замыкателем [2]. Кроме того, имеются и электронные щупы, реализующие антенно-зондовый метод обнаружения ВУ в укрывающих средах. Физическая суть метода заключается в создании условия, при котором объект становится излучателем, при этом он возбуждается током высокой частоты при контакте с токоведущей частью щупа. Метод позволяет определить размер объекта и материал, из которого изготовлен корпус.

При отсутствии угрозы жизни сапер свою работу выполняет стоя, для этого он использует длинный щуп; короткий щуп используется им лежа при непосредственной близости противника. Во время работы щуп держат под углом 20-45 град. к поверхности земли и плавно прокалывают грунт на глубину 10-15 см через каждые 10-20 см во избежание пропуска мин. При постукивании щупом о металлический предмет слышится лязгающий звук, постукивание о деревянный предмет дает глухой звук. Электронный щуп позволяет детектировать радиосигнал и выдавать его в телефонную гарнитуру оператора. Операторы определяют ВВ и ВУ за счет особенностей звукового сопровождения, поэтому металлические объекты не всегда будут ВОП.

К недостаткам метода относятся низкий темп и дальность поиска, невозможность обнаружения ВОП под твердым покрытием, а также субъективность сапера о получаемых акустических данных.

### **Газоаналитические методы обнаружения взрывных устройств.**

ВОП содержит от нескольких десятков граммов до нескольких килограммов ВВ, поэтому ВОП можно обнаружить газоаналитическим методом. Лучшими детекторами ВВ являются служебные собаки. Пороговая чувствительность служебных собак – 10-16 г/см<sup>3</sup>. Поэтому они могут почувствовать запах на расстоянии до 10 м от места закладки ВВ.

Служебная собака является живым существом со своими физиологическими потребностями и ресурсами. Продолжительность работы служебной собаки в течение суток составляет не более 8 часов. Время для отдыха в течение рабочего дня должно составлять 15-20 минут. Время непрерывного эффективного поиска не должно превышать одного часа. Максимальная эффективность работоспособности служебной собаки по обнаружению ВВ достигается при температурах от -15 до +30 градусов по Цельсию. На работоспособность служебной собаки влияют объективные и субъективные факторы. К объективным факторам относятся изменение температуры, скорости ветра (более 10 м/с), дождь, снегопад, наличие большого количества посторонних запахов и т.п. К субъективным – его натренированность, возможность работы в условиях городского шума и при большом скоплении людей [3, 4], а также наличие внезапных аудиовизуальных эффектов (реверберация, резкое изменение интенсивности освещения на обследуемой поверхности, работа систем аудиовизуального оповещения населения и т.п.).

### **Дистанционные методы.**

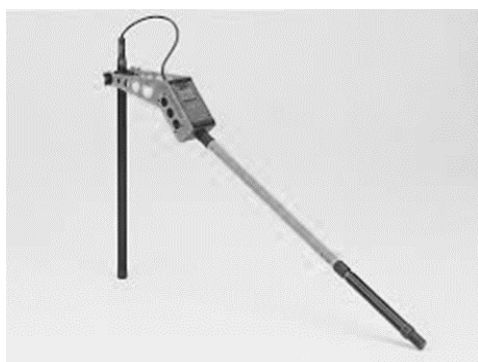
Известно, что в ведущих военных державах для дистанционного обнаружения ВОП широко используются электромагнитные средства поиска, которые позволяют с использованием человеко-машинных интерфейсов получать информацию через сенсорные каналы восприятия (визуальные, аудиальные) об обнаружении прямых и косвенных признаков ВУ, демаскирующих его из-за наличия металлического или пластикового корпуса, электронных датчиков, аномального магнитного и теплового полей, работающего и неработающего радиооборудования и т.п.

Во Вьетнамской народной армии наибольшее распространение получили магнитометрические и индукционные методы обнаружения ВУ, реализованные в радиоэлектронных средствах инженерной разведки, рассмотренных ниже.

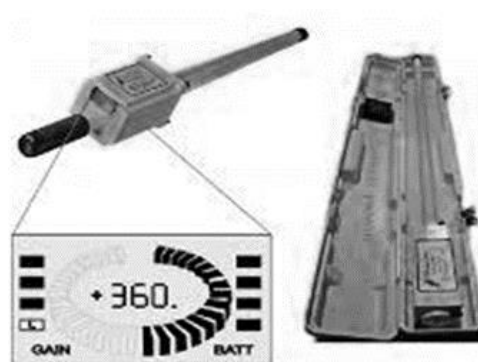
**Магнитометрический метод обнаружения ВОП** основан на электромагнитном явлении, а именно намагничивании ферромагнитных элементов ВУ магнитным полем.

Например, под воздействием магнитного поля Земли ВУ с ферромагнитными элементами создают свое аномальное магнитное поле, искажающее магнитное поле Земли, детектируя указанную аномалию решается задача обнаружения объекта. Для обнаружения ВУ с ферромагнитными элементами используют магнитометрические приборы. Основной частью приборов является измерительный блок, который представляет собой 2 расположенных соосно идентичных феррозондов и находящихся на базовом расстоянии друг от друга. Искажение линий магнитного поля Земли ферромагнитным объектом определяется по изменению положения стрелки на измерительном приборе или экране ЖК - дисплея. При превышении порога обнаружения, наличие объекта обозначается звуковым сигналом, который можно слышать через динамики или наушники сапера.

В настоящее время военно-инженерная служба Вьетнамской народной армии используют для разминирования магнитометрические приборы Vallon EL 1303 – D2, FEREX 4032 - API, GA - 72 CD (см. рис. 3).



Магнитометр (регистратор магнитных аномалий, модель FOERSTER FEREX 4.032, Германия)



Магнитометр (регистратор магнитных аномалий, модель GA - 72 CD, США)



Поиск регистратором магнитных аномалий, модель Vallon EL 1302 D2, США

Рисунок 3. Магнитометрические приборы и оперативно-производственные работы по обнаружению ВУ на местности

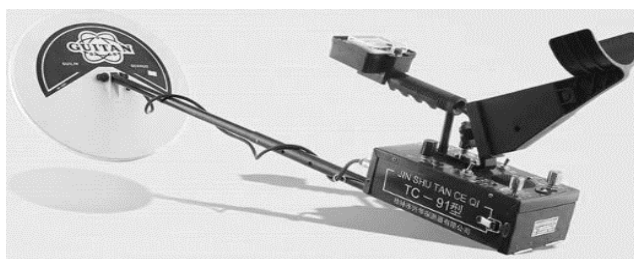
Индукционный метод обнаружения ВОП основан на принципе электромагнитной индукции, возникающей при взаимодействии внешнего электромагнитного поля и электропроводящих элементов, содержащихся в конструкции укрытого слоем грунта объекта. В отличие от магнитометрического, индукционный прибор позволяет обнаружить любой электропроводящий элемент объекта, как ферромагнитный, так и диамагнитный. В таких металлоискателях используются катушки индуктивности. К ним подается переменный ток, который создает переменное первичное магнитное поле с частотой колебаний единицы кГц вокруг излучающей катушки и если металлический объект находится в этом магнитном поле, возникает вихревой ток (ток проводимости)



циркулирующий на тонком поверхностном слое металлической части (скин-слое) объекта. Вихревой ток создает вторичное электромагнитное излучение в окружающем пространстве, которое детектируется измерительным блоком металлоискателя, состоящим из катушки индуктивности и радиоприемного блока. Поэтому вихревые токи являются ключевым параметром метода индукционного обнаружения объектов, поскольку их наличие позволяет обнаружить металлические предметы.

Индукционный прибор получил широкое распространение в Военно-инженерной службе Вьетнамской народной армии. Количество индукционных приборов поиска ВОП, находящихся в армии, примерно в 3 раза больше, чем количество магнитометрических. Такое положение дел в армии связано с тем, что индукционные приборы дешевле и могут обнаружить ВОП из любых металлов.

В настоящее время военно-инженерные службы используют следующие основные индукционные приборы: Guitan TC-91, Minelab F1A4, Vallon VMH3cs (см. рис. 4).



Индукционный прибор (регистратор вихревых токов, модель Guitan TC-91, Китай)



Индукционный прибор (регистратор вихревых токов, модель Vallon VMH3cs, Германия)



Индукционный прибор (регистратор вихревых токов, модель Minelab F1A4, США)

Рисунок 4. Поиск ВОП с использованием принципа электромагнитной индукции

### **Поиск ВОП существующими методами в условиях города.**

Опыт вооруженных конфликтов, специальных военных операций и войн последних десятилетий свидетельствует о широкомасштабной урбанизации боевого пространства, как правило это города со всей своей наземной и подземной инфраструктурой.

Сложная электромагнитная и аудиовизуальная обстановка, широкий масс-спектрометрический состав атмосферного газа в современных городах, а также в их инфраструктурных объектах, сопутствуют применению ВОП в боевом пространстве и существенно усложняют процесс регистрации аномалий в электромагнитных полях и приземном слое атмосферы, что негативно скажется на эффективности применения

---

радиоэлектронных средств инженерной разведки и собак-детекторов, находящихся на вооружении Вьетнамской народной армии.

Как известно, эффективность регистрации аномалий в электромагнитных полях и волнах поисковыми приборами связана:

- с фундаментальными процессами излучения и приема электромагнитных волн и полей в условиях окружающего пространства, зависящих от материальных характеристик окружающей среды (почвы, морской и пресной воды, маскировочного слоя естественного или искусственного происхождения);
- с влиянием размещения и взаимного расположения элементов поискового прибора (датчиков, катушек индуктивности и антенн) относительно ВОП и подстилающей поверхности на эффективность регистрации сигнала;
- с причинно-следственными связями между параметрами сигнала, формой объекта поиска и используемой электронной компонентной базы, а также экранирующих свойств корпуса боеприпаса.

Все эти факторы естественного и искусственного происхождения влияют на эффективность поисковых мероприятий, безопасность и качество разминирования городских территорий находящимися на вооружении Вьетнамской народной армии поисковыми приборами.

### **Перспектива развития радиоэлектронных средств инженерного обеспечения.**

При проведении работ по разминированию необходимо применять современные методы и средства радиоэлектронного обнаружения скрытых ВОП и террористических ВУ, эффективно функционирующие в городских условиях и облегчающие работу сапера по безопасному обнаружению и обезвреживанию ВОП на местности, в том числе в городах и населенных пунктах.

В условиях динамично развивающейся микроэлектронной промышленности в азиатско-тихоокеанском регионе, внедрения векторного анализа сигналов и современных человеко-машинных интерфейсов в разведывательно-поисковую технику, будет обеспечиваться простота восприятия сапером данных об окружающей обстановке и принятие верных решений по обезвреживанию «умных» боеприпасов и СВУ. Важно, что бы на первом этапе развития военно-инженерной службы в комплекте снаряжения сапера должен быть поисковый прибор, позволяющий обнаружить современные ВОП, содержащие в своей конструкции электронные компоненты, на безопасном для него расстоянии.

Одним из перспективных направлений развития радиоэлектронных средств инженерного обеспечения Вьетнамской народной армии является совершенствование методов и средств нелинейной радиолокации, принцип работы которых основан на регистрации вторых и третьих гармоник в спектре рассеянного ВОП зондирующего сигнала. Несмотря на то, что нелинейная радиолокация как новая область науки впервые появилась в начале 1970-х годов, она является новой для исследования вьетнамскими учеными электромагнитных методов обнаружения ВОП.

Принцип нелинейной радиолокации основан на эффекте нелинейного рассеяния электромагнитных волн ВОП, содержащего в своей конструкции р-п переходы (диоды, транзисторы и т.п) или контакты между металлическими предметами с пленкой окислов на контактной поверхности (металл-окисел-металл). Нелинейная радиолокационная станция, реализующая данный принцип работы и радиолинию второго типа с нелинейным объектом отражения, с помощью радиопередающего тракта и узкополосной антенны излучает зондирующий радиосигнал в окружающее пространство. При наличии в окружающем пространстве нелинейного объекта отражения, лишь незначительная часть электромагнитной энергии зондирующего радиосигнала переизлучается объектом в окружающее пространство на второй и третьей гармониках. Радиоприемный тракт нелинейной радиолокационной станции (НРЛС) с широкополосной антенной улавливает

---

радиосигнал на второй и третьей гармониках и сравнивает с установленным порогом обнаружения. При превышении сигнала над порогом обнаружения принимается решение о выявлении ВОП. Факт появления этих гармоник объясняется нелинейной характеристикой полупроводниковых элементов при попадании на них мощных радиоизлучений [6], а также при попадании данного излучения на контактную поверхность с окисной пленкой, генерирующей интермодуляционные помехи в системах связи (эффект «ржавого болта», впервые наблюдаемого на судах ВМС США с мощными радиостанциями) [7].

К основному недостатку НРЛС можно отнести низкую точность измерения угловых координат в направлении на ВОП, укрытый почвой, растительностью или строительным мусором, а также невозможность обеспечить четкое позиционирование объекта, например, на цифровой карте местности.

## СПИСОК ЛИТЕРАТУРЫ

1. Nghiên cứu phát triển tổ hợp thiết bị dò tìm bom, mìn, vật nổ sau chiến tranh ở Việt Nam // Tạp chí khoa học và công nghệ Việt Nam. 2022. №3.
2. Методы и средства обнаружения объектов в укрывающих средах / Дикарев В. И, Заренков В. А, Заренков Д. В, Под ред. Заренкова В. А. Наука и техника, 2004. С. 280. 3. Николай А. П Использование научно-технических средств для обнаружения взрывных устройств, взрывчатых веществ и следов их применения // Вестник Московского университета МВД России. 2019. №4.
3. Рытьков А.А., Зиберова О.С Вопросы применения и использования служебных собак специалистами-кинологами при строительстве и эксплуатации спортивных объектов международного значения в рамках обеспечения антитеррористической безопасности // Проблемы правоохранительной деятельности. 2017. №3.
4. Щербаков Г.Н., Анцелевич М.А., Удинцев Д.Н Оценка предельной глубины обнаружения ферромагнитных объектов искусственного происхождения в толще полупроводящей среды // Специальная техника. 2004. №2.
5. Доматырко Д. Г., Козачок Н. И., Литвиненко В. П Нелинейный радиолокатор и особенности его применения при поиске замаскированных устройств // Вестник ВГТУ. 2010. №1.
6. Луи, П.Л. Пассивные интермодуляционные помехи в системах связи // Журнал IEEE Electronics & Communication Engineering, июнь 1990. Том 2, № 3. С. 109-118.

**С.В. Лазаренко<sup>1</sup>, В.В. Гриценко<sup>1</sup>, И.В. Решетникова<sup>2</sup>**

## **ЭЛЕМЕНТЫ УСТРОЙСТВА ОЦЕНКИ ПАРАМЕТРОВ ТЕЛЕМЕТРИЧЕСКИХ СООБЩЕНИЙ**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,  
Ростов-на-Дону, Россия<sup>1</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: алгоритмы обработки, телеметрические системы, фильтрация, фильтр Калмана.

В статье рассматривается способ повышения точности оценки параметров телеметрических сообщений с использованием вариационных принципов и итерационной

регуляризации. Он позволяет решать эффективно задачи оценки за счет повышения точности получаемых оценок и увеличения скорости их сходимости при реализации последовательного алгоритма оценки параметров телеметрических сообщений.

S.V. Lazarenko<sup>1</sup>, V.V. Gritsenko<sup>1</sup>, I.V. Reshetnikova<sup>2</sup>

## ELEMENTS OF THE DEVICE FOR EVALUATING THE PARAMETERS OF TELEMETRY MESSAGES

«Don State Technical University» Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: processing algorithms, telemetry systems, filtering, Kalman filter.

The article discusses a way to improve the accuracy of estimating the parameters of telemetry messages using variational principles and iterative regularization. It makes it possible to solve estimation problems efficiently by increasing the accuracy of the estimates obtained and increasing the speed of their convergence when implementing a sequential algorithm for estimating the parameters of telemetry messages.

### Введение.

Современные информационно-измерительные (ИИС) системы, нашедшие применение в различных областях [1] очень часто используются по воздействию на их каналы связи (КС) различного рода искажающих помех.

На сегодняшний день широкое распространение получили системы с адаптивным помехоустойчивым кодированием. В таких системах изменяется алгоритм кодирования или его параметры в зависимости от изменения состояния КС [1]. Построение адаптивных систем возможно благодаря передаче на сторону отправителя информации о состоянии КС, для чего организовывается дополнительный канал обратной связи (КОС). В таких случаях, обычно для организации работы применяют полученные статистические данные о текущем состоянии КС. Но таких данных недостаточно для осуществления эффективной адаптации. Данный недостаток особенно сильно влияет на качество адаптации в системах, работающих под действием нестационарных помех. Решение такой проблемы может быть получено на основе предсказания будущего состояния КС, что позволит исключить неточности в оценке, связанных с задержкой передачи информации об актуальном состоянии КС по КОС.

Структурная схема модели системы передачи данных с адаптацией по состоянию КС путем выбора параметров БЧХ-кода представлена на рисунке 1.

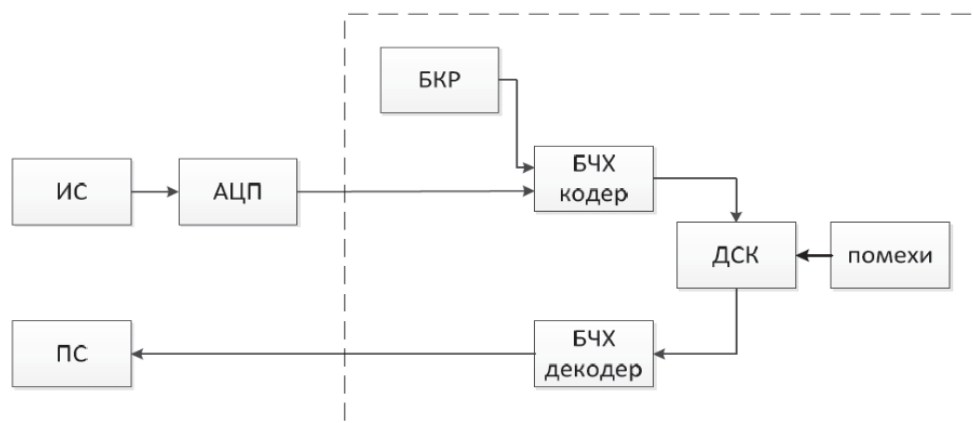


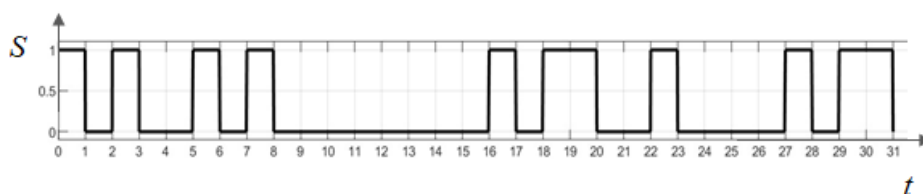
Рисунок 1. Структурная схема модели связи

Сообщение от источника сообщений (ИС) поступает на вход БЧХ кодера, потом, закодированное сообщение передается в дискретный канал связи (ДКС), в качестве модели которого выбран двоичный симметричный канал, в котором присутствуют помехи. Далее сообщение раскодируется декодером БЧХ (ДК) и с помощью блока оценивания качества (БОК) раскодированное сообщение отправляется получателю дискретных сообщений (ПС) и сравнивается с эталонном, после чего подсчитывается число ошибочно принятых бит. Затем, эта информация отправляется на вход блока коррекции параметров (БКР), где принимается решение об изменении параметров кода. При этом, для начала предсказания состояния КС необходимо набрать определенный объем статистики о состоянии.

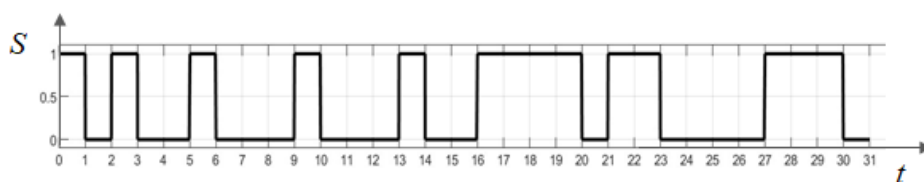
На рисунке 2,а изображен график исходного сообщения, длиной в 8 бит. Допустим, что при раскодировании необходимо исправить в сообщении три ошибки. Для этого надо, выбрать код с определенными параметрами. Для обеспечения требуемой разрядности, надо дополнить исходное сообщение нулями в восьми младших разрядах и подать его на вход кодера с параметрами  $n = 31$  и  $k = 16$ , тогда сообщение на выходе будет иметь вид, представленный на рисунке 2,б. После этого сообщение передается в КС, где на присутствует помеха, в результате чего происходит искажение в следующих семи разрядах: 0, 2, 9, 13, 17, 21, 23 (рисунок 2,в). Далее сообщение раскодируется с исправлением трёх ошибок (рисунок 2,г), что, для выбранных параметров, соответствует восстанавливающей способности выбранного кода.



а)



б)



в)



г)

Рисунок 2. Графики изменения состояния отправляемого сообщения:  
а) исходное сообщение; б) сообщение, которое закодировано БЧХ-кодом;  
в) зашумленное сообщение; г) раскодированное сообщение

### Постановка экстремальной задачи.

Задачи параметрической оценки математических моделей зачастую являются некорректными [3]. Общая запись обратной задачи может быть представлена в форме следующего операторного уравнения

$$A \cdot u = f, \quad u \in U, \quad f \in F, \quad (1)$$

где  $u$  и  $f$  - искомая и наблюдаемая характеристики соответственно, которые понимаются как элементы метрических пространств  $U$  и  $F$ . Оператор  $A:U \rightarrow F$  предполагается известным и имеет область определения  $D(A) \subseteq U$  и область значений  $R(A) \subseteq F$ .

Для решения обратных задач используют методы теории некорректных задач - теории регуляризации. Одним из перспективных направлений теории регуляризации - итерационная регуляризация, в основе которой положен принцип регуляризации А.Н. Тихонова. Смысл указанного метода заключается в построении алгоритмов регуляризации на основе различных итерационных методов, причем параметром регуляризации будет являться номер итерации.

Наиболее удобным методом является метод простой итерации. Его сходимость при точных исходных данных для уравнений с линейным непрерывным оператором, не имеющим ограниченного обратного, была доказана В.М. Фридманом. Он также доказал и сходимость нелинейных градиентных методов типа скорейшего спуска.

Помимо этого, стоит отметить ещё одну проблему, имеющую уже сугубо практический характер - отсутствие встроенной программной системы построения моделей оценки с поддержкой этапов процесса моделирования. Существующие программы очень часто ориентированы или только на какой-то отдельный этап (например, корреляционный анализ данных), или же ориентированы для решения узкого круга задач при ограниченном количестве моделей (чаще всего линейных, внутрилинейных и полиномиальных). Программы, которые позиционируются как универсальные, также не лишены указанных недостатков: их универсальность заключается в том, что для решения каждой отдельной подзадачи предлагаются самые простые варианты, что явно не эффективно для практических целей. В конце концов, многие из аналитических программ ориентированы на моделирование в социально-экономических дисциплинах, в которых стандарты моделирования и правила представления моделей сильно отличаются от принятых в физико-математических и технических областях.

### Общий вид уравнений алгоритма оценки параметров телеметрических сообщений.

Рассмотрим математическую постановку задачи. Отнесение части энергии к работе обобщенных сил  $Q_s(q, \dot{q}, U)$  в режиме декомпозиции позволяет ввести простейшую определенно положительную квадратичную форму, которая трактуется как кинетическая энергия системы

$$T = \frac{1}{2} \sum_{s=1}^n a_{ss} \dot{q}_s^2, \quad s = \overline{1, n}. \quad (2)$$

где  $q_s, \dot{q}_s$  – обобщенные координаты и скорости;

$a_{sk}$  – коэффициенты инерции

В пространстве наблюдений выбран целевой функционал [3], принимающий значение, которое определяет точность измерения

$$J = \frac{1}{2} \int_{t_0}^{t_1} \sum_{s=1}^n N_{ss}^{-1} [\mathbf{y}_s - \hat{\mathbf{q}}_s]^2 dt = \int_{t_0}^{t_1} F(\hat{\mathbf{q}}) dt = D, \quad (3)$$

где  $N_{ss}$  – элементы диагональной весовой матрицы  $N$ , характеризующей интенсивность помех в канале наблюдений;

$D$  – взвешенная априорная дисперсия результатов измерений каналов наблюдения.

Для системы с кинетической энергией (2) в режиме декомпозиции за счет обратных связей модель двигается в соответствии с целью, которая определяется значением функционала (3). Делая допущения, что движение в режиме декомпозиции полностью исключает динамическое взаимовлияние между элементами, имеем соотношение

$$|\dot{\mathbf{q}}_s| = \sqrt{a_{ss}^{-1} \lambda^{-1} N_{ss}^{-1}} |\mathbf{y}_s - \mathbf{q}_s|, s = \overline{1, n}. \quad (4)$$

Общий вид уравнения динамической квазидетерминированной оценки определяется формулой

$$\frac{d}{dt} \left( \frac{\partial T}{\partial \dot{\mathbf{q}}_s} \right) - \frac{\partial T}{\partial \mathbf{q}_s} = \lambda^{-1} \left[ -\lambda \frac{|\dot{\mathbf{q}}_s|}{N_{ss}^{-1} |\mathbf{y}_s - \mathbf{q}_s|} \dot{\mathbf{q}}_s - N_{ss}^{-1} (\mathbf{y}_s - \mathbf{q}_s) \right].$$

С учетом принятой модели кинетической энергии и кинематической связи (4) записываем уравнение оценки в виде

$$\ddot{\hat{\mathbf{q}}}_s(t) = -\sqrt{\lambda_s^{-1}} \dot{\hat{\mathbf{q}}}_s(t) - \lambda_s^{-1} (\mathbf{y}_s(t) - \hat{\mathbf{q}}_s(t)), \quad (5)$$

где  $\lambda_s = a_{ss} \lambda N_{ss}$  – коэффициент адаптации.

### Решение задачи оценки параметров.

Состояние описывается дифференциальным уравнением второго порядка

$$\ddot{x} = f(x, \dot{x}, z^0, z^1) = z^0 \dot{x} + z^1 x. \quad (6)$$

В общем случае уравнение (6) описывает затухающие колебания в некоторой динамической системе, а параметр  $z^0$  – декремент затухания. Пусть параметр  $z^0$  – это постоянная времени. Тогда  $x$  – напряжение [2].

Уравнение наблюдения имеет вид

$$y(t) = x(t). \quad (7)$$

Применение (1) с учетом процесса расширения пространства состояний требует представления уравнения состояния в форме:

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{F}(\mathbf{x}, \mathbf{z}) = \begin{bmatrix} x^1 \\ z^0 x^1 + z^1 x^0 \end{bmatrix}, \\ \dot{\mathbf{z}} &= \boldsymbol{\eta}, \quad \mathbf{z}(t_0) = \mathbf{z}(0), \end{aligned} \quad (8)$$

$$\text{где } \mathbf{x} = \begin{bmatrix} x^0 \\ x^1 \end{bmatrix};$$

$$\boldsymbol{\eta} = \begin{bmatrix} \eta^0 \\ \eta^1 \end{bmatrix};$$

$$\mathbf{z} = \begin{bmatrix} z^0 \\ z^1 \end{bmatrix}.$$

Тогда уравнение наблюдения (7) примет следующую форму

$$\mathbf{y}(t) = \mathbf{x}(t), \quad (9)$$

$$\text{где } \mathbf{y}(t) = \begin{bmatrix} y^0 \\ y^1 \end{bmatrix} = \begin{bmatrix} x^0 \\ 0 \end{bmatrix}.$$

Функционал невязки записывается следующим образом:

$$J_1 = \frac{1}{2} \int_0^T [\mathbf{y} - \hat{\mathbf{x}}]^T [\mathbf{y} - \hat{\mathbf{x}}] dt \rightarrow \min. \quad (10)$$

Уравнения синтезированного алгоритма оценки параметров принимают вид:  
- первая итерация

$$\begin{aligned} \hat{\mathbf{z}}_0 &= \mathbf{P}_0 \mathbf{G}_0^T \gamma_0^0 (\mathbf{y} - \hat{\mathbf{x}}_0), \\ \hat{\mathbf{x}}_0 &= \mathbf{F}(\hat{\mathbf{x}}_0, \mathbf{z}_0) + \mu_0^{-1} \gamma_0^0 (\mathbf{y} - \hat{\mathbf{x}}_0), \\ \dot{\mathbf{P}}_0 &= \mathbf{I} + \mathbf{P}_0 \mathbf{G}_0^T \gamma_0^0 \mathbf{G}_0 \mathbf{P}_0, \\ \dot{\mathbf{G}}_0 &= \frac{\partial \mathbf{F}}{\partial \hat{\mathbf{x}}_0} \mathbf{G}_0 + \frac{\partial \mathbf{F}}{\partial \hat{\mathbf{z}}_0}; \end{aligned} \quad (11)$$

- вторая итерация

$$\begin{aligned} \hat{\mathbf{z}}_1 &= \mathbf{P}_1 \mathbf{G}_1^T \left\{ (1 - \gamma_0^1) (\mathbf{y} - \hat{\mathbf{x}}_0) + (\mathbf{y} - \hat{\mathbf{x}}_1) \right\}, \\ \hat{\mathbf{x}}_1 &= \mathbf{F}(\hat{\mathbf{x}}_1, \mathbf{z}_1) + \mu_1^{-1} \left\{ (1 - \gamma_0^1) (\mathbf{y} - \hat{\mathbf{x}}_0) + (\mathbf{y} - \hat{\mathbf{x}}_1) \right\}, \\ \dot{\mathbf{P}}_1 &= \mathbf{I} - \mathbf{P}_1 \mathbf{G}_1^T (1 - \gamma_0^1) \gamma_0^1 \mathbf{G}_1 \mathbf{P}_1, \\ \dot{\mathbf{G}}_1 &= \frac{\partial \mathbf{F}}{\partial \hat{\mathbf{x}}_1} \mathbf{G}_1 + \frac{\partial \mathbf{F}}{\partial \hat{\mathbf{z}}_1}, \end{aligned} \quad (12)$$

$$\text{где } \hat{\mathbf{x}}_0(0) = [0,3 \quad 0,01]^T, \quad \hat{\mathbf{x}}_1(0) = [0,3 \quad 0,01]^T;$$

$$\hat{\mathbf{z}}_0(0) = \hat{\mathbf{z}}_1(0) = [0 \quad 0]^T;$$

$$\mathbf{G}_0(0) = \mathbf{G}_1(0) = \begin{bmatrix} 0,1 & 0,02 \\ 0,02 & 0,1 \end{bmatrix};$$

$$\mathbf{P}_0(0) = \mathbf{P}_1(0) = \begin{bmatrix} 7 & 0,01 \\ 0,01 & 7 \end{bmatrix};$$

$$\mu_0 = 18, \quad \gamma_0^0 = 1, \quad \mu_1 = 12, \quad \gamma_0^1 = 0,5.$$



---

Получен алгоритм оценки параметров динамической системы с использованием вариационных принципов и итерационной регуляризации (11), (12). Он позволяет решать эффективно задачи оценки за счет повышения точности получаемых оценок и увеличения скорости их сходимости при реализации последовательного алгоритма оценки.

Анализ результатов численного моделирования, полученных в среде MathCAD, показывает, что выигрыш в точности на второй итерации по отношению к первой составляет,  $\delta z^0 = 3,3\%$ ,  $\delta z^1 = 5,1\%$ , соответственно для параметров аналогичных коэффициентам диссипации и жесткости. Это подтверждает эффективность разработанного метода. При этом необходимо отметить, что в соответствии с исследованиями первая итерация уже обеспечивает выигрыш в точности в сравнении с фильтром Калмана.

#### **Заключение.**

В статье представлен Получен алгоритм оценки параметров с использованием вариационных принципов и итерационной регуляризации (11), (12). Он позволяет решать эффективно задачи оценки за счет повышения точности получаемых оценок и увеличения скорости их сходимости при реализации последовательного алгоритма оценки.

В соответствии с исследованиями первая итерация предлагаемого алгоритма оценки уже обеспечивает выигрыш в точности в сравнении с фильтром Калмана

Разработанный модуль оценки содержит четыре взаимосвязанные структуры, что определяются формой уравнений.

#### **СПИСОК ЛИТЕРАТУРЫ**

1. Глинченко, А. С. Цифровая обработка сигналов. Часть 1 : учебное пособие. – Красноярск : издательство КГТУ, 2011. – 1999 с.
2. Костоготов, А. А. Метод последовательных приближений в теории фильтрации / А. А. Костоготов // Автоматика и вычислительная техника. – 2000. – №3. – С. 53-63.
3. Тихонов, В. И. Статистический анализ и синтез радиотехнических устройств и систем : учебное пособие / В. И. Тихонов, В. Н. Харисов. – Москва : Радио и связь, 1991. – 608 с.
4. Андрашитов, Д. С. Регуляризованный алгоритм многопараметрической вариационной идентификации динамических систем / Д. С. Андрашитов, А. А. Костоготов, С. В. Лазаренко // Сервис в России и за рубежом. – 2011. – №. 8. – С. 25-36.
5. Андрашитов, Д. С. Многопараметрическая вариационная идентификация динамических систем на основе объединенного принципа максимума / Д. С. Андрашитов, А. А. Костоготов, С. В. Лазаренко // Информационно-управляющие системы. – 2012. – №4(10). – С. 68-76.

**ОЦЕНКА ЭФФЕКТИВНОСТИ АЛГОРИТМА ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ  
АНАЛОГОВОГО СИГНАЛА НА ФОНЕ ПОМЕХ**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,  
Ростов-на-Дону, Россия<sup>1</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: алгоритмы обработки, телеметрические системы, аналоговый сигнал, телевидение.

В статье рассмотрен алгоритм определения параметров аналогового сигнала на фоне сингулярных помех, являющийся эффективным методом решения поставленной задачи определения характеристик информационного процесса. Анализ результатов моделирования показал, что представленный алгоритм наиболее эффективен при малом количестве отсчетов, малом интервале наблюдения и малых значениях сигнал/шум.

**I.V. Pugachev<sup>1</sup>, S.R. Khumaryants<sup>1</sup>, I.V. Reshetnikova<sup>2</sup>**

**EVALUATION OF THE EFFECTIVENESS OF THE ALGORITHM FOR  
DETERMINING PARAMETERS ANALOG SIGNAL AGAINST THE BACKGROUND  
OF INTERFERENCE**

«Don State Technical University» Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University

of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: processing algorithms, telemetry systems, analog signal, broadcasting.

The article considers an algorithm for determining the parameters of an analog signal against the background of singular interference, which is an effective method for solving the problem of determining the characteristics of the information process. Analysis of the simulation results showed that the presented algorithm is most effective with a small number of samples, a small observation interval and small signal/noise values.

**Введение.**

Аналоговые системы до сих пор активно используются, и разработка методов и алгоритмов обработки аналоговых сигналов является актуальной насущной задачей. Например, в системе ГЛОНАСС каждый штатный навигационный космический аппарат в орбитальной группировке постоянно излучает шумоподобные непрерывные навигационные радиосигналы в двух диапазонах частот ~1600 МГц и ~1250 МГц [1]. Навигационные измерения в двух диапазонах частот позволяют исключить ионосферные погрешности навигационных определений. Шумоподобные навигационные радиосигналы различаются несущими частотами.

**Анализ аналоговых систем связи.**

Принципиальное отличие систем аналоговой и цифровой связи связано со способом оценки их производительности. Сигналы аналоговых систем составляют континуум, так что приемник должен работать с бесконечным числом возможных сигналов. Критерием производительности аналоговых систем связи является критерий достоверности, такой как

---

отношение сигнал/шум, процент искажения или ожидаемая среднеквадратическая ошибка между переданным и принятым сигналами.

Аналоговые транкинговые системы связи включают наземную инфраструктуру (стационарное оборудование) и абонентские станции. Транкинговые системы – радиально-зонавые системы наземной подвижной радиосвязи, осуществляющие автоматическое распределение каналов связи ретрансляторов (базовых станций) между абонентами. Под термином «транкинг» понимается метод доступа абонентов к общему выделенному пучку каналов, при котором свободный канал выделяется абоненту на время сеанса связи [1].

Современные транкинговые системы, как правило, обеспечивают различные типы вызова (групповой, индивидуальный, широковещательный), допускают приоритетные вызовы, имеют доступ к телефонной сети общего пользования, обеспечивают возможность передачи данных и режим прямой связи между абонентскими станциями (без использования канала базовой станции).

### **Введение в задачу.**

В радиосвязи и других системах передачи информации сигнал, предназначенный для передачи сообщений, во время трансляции искажается и маскируется помехами, активными и пассивными, что и создает трудности выделения исходного сигнала.

Выдающимися советскими (позже российскими) и зарубежными учеными была развита мощная теория оптимального радиоприема, базирующаяся на методах математической статистики.

Согласно этой теории, были определены пять основных задач, которые необходимо было решить, для оптимального приема [2]:

1. Обнаружение сигнала – по принятым данным необходимо определить, присутствует сигнал или нет.
2. Различение нескольких сигналов – по принятой реализации электромагнитных колебаний с минимальной ошибкой определить, какой именно сигнал принят.
3. Оценка параметров сигнала – необходимо определить параметры колебания (амплитуда, фаза, частота, время появления и др.) по принятой реализации с минимальной погрешностью.
4. Фильтрация сигналов – по принятой реализации, содержащей случайный процесс, зная характер шума решить оптимальным образом, какая именно реализация случайного процесса присутствует в реализации.
5. Разрешение сигналов – при наличии в реализации двух сигналов необходимо раздельно обнаружить каждый сигнал.

Каждая и указанных задач по-своему интересна, имеет свои особенности и точки соприкосновения с другими. Также, каждая задача может быть связана с какой-либо определенной отраслью радиотехники более, чем с другой. Например, первая задача наиболее характерна для радиолокации, вторая – для радиосвязи, третья – для измерительной техники и радионавигации.

В практике статистической обработки результатов наблюдений преимущественное распространение получили алгоритмы и процедуры обработки информации, обеспечивающие формирование несмещенных (асимптотически несмещенных) оценок неизвестных параметров и процессов. При всех внешних различиях между отдельными оценками их объединяет тот факт, что в основе обширного семейства несмещенных оценок лежат классические методы оценивания – метод максимального правдоподобия и метод наименьших квадратов (МНК).

Для решения различных целевых задач бывает необходимо осуществить оценку набора различных характеристик сигнала на заданном интервале наблюдения. К числу таких характеристик можно отнести значения производных различного порядка, определенных интегралов, спектральных плотностей и др. Причем бывает необходимость оперативно рассмотреть спектр не только во временной области, но и в частотной. На

рисунке 1 показан сложный сигнал во временной и в частотной области. В частотной области показана амплитуда для каждой синусоидальной волны в спектре в зависимости от частоты. Как видно, в данном случае спектр состоит лишь из двух волн. Временная область является предпочтительной для многих измерений, а для некоторых является единственно возможной. К примеру, только во временной области можно измерить длительность фронта и спада импульса, выбросы и биения.

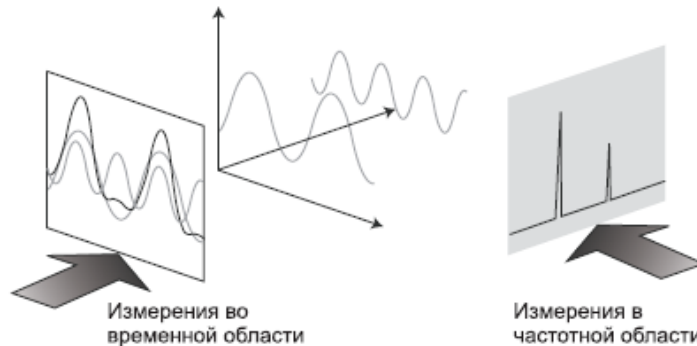


Рисунок 1. Соотношение между временными и частотными областями

### Постановка задачи синтеза алгоритма.

Пусть на отрезке  $[t_0, t_N]$  наблюдается аддитивная смесь  $y(t)$  полезного сигнала  $x(t)$ , СП  $h(t)$  и ФШ  $\xi(t)$  [4]:

$$y_n = x_n + h_n + \xi_n, \quad n = \overline{0, N}, \quad (1)$$

Сигнал  $x(t)$  задается в конечно-аналитическом виде

$$x(t) = A^T q(t) = q^T(t) A, \quad (2)$$

где  $A = [a_m]^T$  – вектор неизвестных коэффициентов;

$q(t) = [q_m(t)]^T$  – вектор линейно-независимых функций на отрезке  $[t_0, t_N]$  (базис сигнала).

Искомый оптимальный вектор функционалов  $Z^*$  обобщенного оценивания требовалось отыскать в виде

$$Z^* \{Y\} = P_Z Y = Z^*, \quad (3)$$

где  $P_Z = [p_{zn}, r = \overline{1, M_Z}, n = \overline{0, N}]$  – матрица неизвестных коэффициентов;

$Z^* = [z_r^*]$  – оценка вектора  $Z$ .

Корреляционная матрица линейной оценки (3) для принятой модели случайного вектора  $\Xi$  находится по правилу

$$K_Z = P_Z K_{\Xi} P_Z^T. \quad (4)$$

Под оптимальной оценкой  $Z = P_Z Y$  будем понимать такую оценку, которая обеспечивает минимизацию следа  $tr(K_Z)$  матрицы  $K_Z$ :

$$\min_{P_Z} tr(K_Z) = \min_{P_Z} \sum_{r=1}^{M_Z} \sigma_{zr}^2, \quad (5)$$

где  $\sigma_{zr}^2$  – диагональные члены матрицы  $K_Z$ ,  
выполнение условия несмещенности значений вектора функционалов:

$$Z \{X\} - Z \{x(t)\} = [0]_{M_Z \times 1} \quad (6)$$

и условия инвариантности к СП:

$$Z \{H\} = [0]_{M_Z \times 1}, \quad (7)$$

где  $[0]_{M_Z \times 1}$  – нулевой вектор столбец размерности  $M_Z$ ;

$$Z \{X\} = \begin{bmatrix} z_r \{X\} \end{bmatrix}^T;$$

$$Z \{H\} = \begin{bmatrix} z_r \{H\} \end{bmatrix}^T.$$

Требовалось с учетом (1)-(7) найти матрицу  $P_Z$ , соответствующую оптимальной оценке  $Z = P_Z Y$ . Ставилась также задача проанализировать влияние неадекватности модели (2) на результаты оценивания [5].

### Решение задачи синтеза алгоритма.

Были введены следующие обозначения:

$$B = [B_0^T, B_1^T, \dots, B_{I\Delta_1}^T, \dots, B_{I1}^T, \dots, B_{I\Delta_1}^T] \quad (8)$$

– расширенный вектор неизвестных коэффициентов СП,

$$\Theta = [\Theta_0, \Theta_{11}, \dots, \Theta_{I\Delta_1}, \dots, \Theta_{I1}, \dots, \Theta_{I\Delta_1}] \quad (9)$$

– расширенная базисная матрица помехи,

где  $\Theta_{ij} = [\theta_{ijm}(t_k)]$  – вспомогательная базисная матрица помехи;

Расширенная базисная матрица помехи  $\Theta$  имеет размерность  $[N + 1] \times M_{h\Sigma}$ , где

$$M_{h\Sigma} = M_{h0} + \sum_{i=1}^I \Delta_i M_{hi}.$$

По аналогии с [6] задача отыскания оптимальной матрицы  $P_Z$  решалась методом множителей Лагранжа, то есть ищались независимые минимумы скалярных функций

$$F(P_{zr}, \gamma_r, \eta_r) = P_{zr}^T K_{\Xi} P_{zr} + \gamma_r^T \Theta^T P_{zr} + \{z_r [q^T(t)] - P_{zr}^T Q\} \eta_r, \quad r = \overline{1, M_Z}, \quad (10)$$

где  $\gamma_r$  и  $\eta_r$  – векторные множители Лагранжа;

$P_{zr}^T = [p_{zrh}]$  –  $r$ -я строка матрицы  $P_Z$ .

При нахождении минимума данной функции путем дифференцирования (10) соответственно по аргументам  $\vec{P}_{zr}$ ,  $\vec{\gamma}_r$  и  $\vec{\eta}_r$  получили необходимые уравнения [6]

$$\begin{cases} \frac{\partial L_r}{\partial \vec{P}_{zr}} = [0]_{(J+1) \times 1}, \\ \frac{\partial L_r}{\partial \vec{\gamma}_r} = [0]_{M_r \times 1}, \\ \frac{\partial L_r}{\partial \vec{\eta}_r} = [0]_{M_r \times 1}, \end{cases} \quad (11)$$

где  $L_r = L(\vec{P}_{zr}, \vec{\gamma}_r, \vec{\eta}_r)$ .

Решение задачи минимизации (11), в которой учитываются условия несмещенности и инвариантности (10), приняло вид

$$P_{zr} = \Psi_{\Theta} \Gamma_Q \left( Q^T \Psi_{\Theta} \Gamma_Q \right)^{-1} z_r \{q(t)\}, \quad (12)$$

где  $\Psi_{\Theta} = E_{(N+1) \times (N+1)} - \Gamma_{\Theta} \Phi_{\Theta}^{-1} \Theta^T$ ;

$E_{(N+1) \times (N+1)}$  – единичная матрица размерности  $(N+1) \times (N+1)$ .

### Проведение эксперимента.

При моделировании для простоты и наглядности в качестве аналогового сигнала использовался степенной многочлен второй степени. На интервале наблюдения 3 с (рисунок 2) сигнал имеет представленный вид.

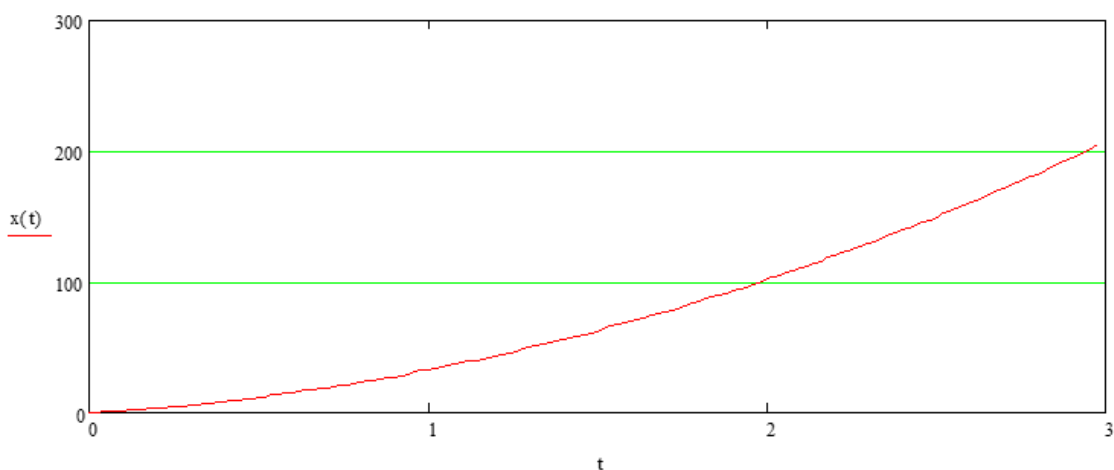


Рисунок 2. Исследуемый аналоговый сигнал

В качестве исходных данных программы выступают:

- интервал наблюдения частота  $T$  (с);
- количество отсчетов  $N$  ;
- базисные функции  $\phi_1(t), \phi_2(t)$  аналогового сигнала  $x(t)$  ;
- коэффициенты  $c_1, c_2$  при базисных функциях  $\phi_1(t), \phi_2(t)$  аналогового сигнала;
- базисные функции  $\phi_1(t), \phi_2(t) \dots \phi_k(t)$  СП;
- варианты среднеквадратического отклонения (СКО)  $\sigma_1 = 1, \sigma_2 = 5, \sigma_3 = 15$  и  $\sigma_4 = 25$ .

При проведении вычислительного эксперимента был введен ряд ограничений для рассмотрения наиболее характерных и интересных свойств исследуемого алгоритма. Сначала было зафиксировано число отсчетов в количестве 100 точек, интервал наблюдения при этом менялся дискретно, шагом 1 с от 3 с до 10 с.

Анализ полученных в результате моделирования данных при указанных условиях показывает следующее:

- при высоких отношениях сигнал/шум ( $\sigma_1$ ) исследуемый алгоритм уступает МНК почти при всех значениях количества точек отсчетов;
- при более низких отношениях сигнал/шум исследуемый алгоритм соизмерим МНК;
- при низких отношениях сигнал/шум и малом числе отсчетов исследуемый алгоритм превосходит МНК;
- при уменьшении количества отсчетов значение коэффициента  $\gamma$  постоянно увеличивается.

Следующим этапом было проведение моделирования при длительности интервала наблюдения 3 с изменением количества точек отсчета в нем от 30 до 100. Результаты моделирования для данных условий представлены на рисунках 3.

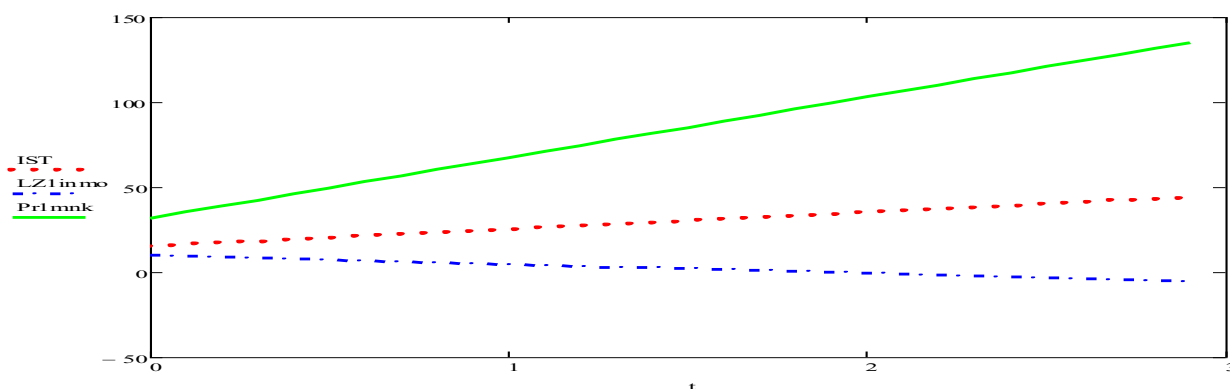


Рисунок 3. Результаты дифференцирования сигнала на интервале 3 с

Таблица 2. Зависимость средней относительной погрешности для различных вариантов СКО в интервале наблюдения 3 с

Количество точек отсчета, шт	Значение средней относительной погрешности для различных вариантов СКО, %				$\gamma$
	$\sigma_1 = 1$	$\sigma_2 = 5$	$\sigma_3 = 15$	$\sigma_4 = 25$	
30	$\delta = 66.25$ $\delta_{MNK} = 75.37$	$\delta = 100.54$ $\delta_{MNK} = 751.69$	$\delta = 50.179$ $\delta_{MNK} = 104.73$	$\delta = 54.07$ $\delta_{MNK} = 125.44$	0.345
40	$\delta = 55.81$ $\delta_{MNK} = 70.68$	$\delta = 126.43$ $\delta_{MNK} = 402.25$	$\delta = 47.94$ $\delta_{MNK} = 93.76$	$\delta = 49.05$ $\delta_{MNK} = 115.78$	0.434
50	$\delta = 40.19$ $\delta_{MNK} = 65.61$	$\delta = 96.52$ $\delta_{MNK} = 167.41$	$\delta = 44.14$ $\delta_{MNK} = 85.67$	$\delta = 46.85$ $\delta_{MNK} = 108.35$	0.429
60	$\delta = 38.57$ $\delta_{MNK} = 52.21$	$\delta = 105.34$ $\delta_{MNK} = 566.18$	$\delta = 39.19$ $\delta_{MNK} = 79.35$	$\delta = 42.01$ $\delta_{MNK} = 104.74$	0.348
70	$\delta = 36.76$ $\delta_{MNK} = 43.22$	$\delta = 86.87$ $\delta_{MNK} = 157.01$	$\delta = 33.61$ $\delta_{MNK} = 74.41$	$\delta = 37.66$ $\delta_{MNK} = 98.23$	0.320
80	$\delta = 34.82$ $\delta_{MNK} = 32.53$	$\delta = 195.52$ $\delta_{MNK} = 171.31$	$\delta = 31.25$ $\delta_{MNK} = 66.65$	$\delta = 35.56$ $\delta_{MNK} = 93.52$	0.340
90	$\delta = 25.37$ $\delta_{MNK} = 24.86$	$\delta = 93.96$ $\delta_{MNK} = 180.16$	$\delta = 29.85$ $\delta_{MNK} = 63.18$	$\delta = 29.37$ $\delta_{MNK} = 85.67$	0.357
100	$\delta = 22.34$ $\delta_{MNK} = 21.42$	$\delta = 87.13$ $\delta_{MNK} = 125.47$	$\delta = 23.85$ $\delta_{MNK} = 55.02$	$\delta = 27.69$ $\delta_{MNK} = 83.12$	0.426

Анализ полученных в результате моделирования данных при указанных условиях показывает следующее:

- при высоких отношениях сигнал/шум ( $\sigma_1$ ) исследуемый алгоритм уступает МНК при количестве отсчетов 80-100;
- при более низких отношениях сигнал/шум исследуемый алгоритм соизмерим МНК и наибольший выигрыш наблюдается при малом количестве отсчетов;
- значение коэффициента  $\gamma$  постоянно колеблется.

### Заключение.

Способность алгоритма достоверно определять характеристики информационного процесса по малому числу отсчетов играет важную роль в реально используемых радиоэлектронных средствах как специального, так и бытового назначения. Рассматриваемый в дипломной работе алгоритм как раз обладает такими качествами.

Современный уровень развития средств анализа частотного спектра позволяет идентифицировать области, «подозрительные» на смену структуры сингулярной помехи, что означает возможность применения алгоритма в действующих системах. Самыми применимыми в РФ на сегодняшний день являются супергетеродинные анализаторы спектра. Но действительно существенной проблемой является тот факт, что отечественное производство средств измерений и анализа значительно отстает от западных конкурентов. Для сокращения отставания РФ в области технологий необходимо развивать как средства производства, так и теоретическую составляющую.

Рассматриваемый в дипломной работе алгоритм определения параметров аналогового сигнала на фоне сингулярных помех является эффективным методом решения поставленной задачи определения характеристик информационного процесса.

Анализ результатов моделирования показал:



- исследуемый алгоритм наиболее эффективен при малом количестве отсчетов, малом интервале наблюдения и малых значениях сигнал/шум;
- при невысоких значениях сигнал/шум, большом интервале наблюдения и большом количестве отсчетов исследуемый алгоритм соизмерим либо уступает МНК;
- при высоких значениях сигнал/шум, малом интервале наблюдения и малом количестве отсчетов исследуемый алгоритм становится неэффективным, как и МНК.

Работа подготовлена в рамках научной темы

«Разработка беспилотных технологий на основе комплексной поэтапной оптимизации с редукцией экстремальных задач и инструментов нейро-нечеткого моделирования (FZNE-2022-0006)».

## СПИСОК ЛИТЕРАТУРЫ

1. Пучков Г.Ю., Шурыгин А.В. Системы транкинговой радиосвязи. М.: ГУ НПО «Специальная техника и связь» МВД России, 2001. 160 с.
2. Костоглотов, А. А. Метод последовательных приближений в теории фильтрации / А. А. Костоглотов // Автоматика и вычислительная техника. – 2000. – №3. – С. 53-63.
3. Костоглотов А.А., Чеботарев А.В. Синтез оптимального алгоритма оценки фазы на основе объединенного принципа максимума // Автоматика и вычислительная техника. 2006. №6. С. 25-33.
4. Костоглотов А.А., Костоглотов А.И., Лазаренко С.В. Объединенный принцип максимума в задаче синтеза оптимального управления нелинейными системами // АВТ. 2007. №5. С. 52 – 61.
5. Булычев Ю.Г., Елисеев А.В. Алгоритм обработки измерений при кусочно-непрерывной помехе // Теория и системы управления. 2007. №2.
6. Булычев Ю.Г., Елисеев А.В. Модифицированный метод наименьших квадратов в обобщенно-инвариантной постановке // Проблемы управления и информатики. 2006. №6.

**И.В. Пугачев<sup>1</sup>, А.К. Вехтер<sup>1</sup>, О.А. Решетникова<sup>2</sup>**

### **СИНТЕЗ СИСТЕМЫ ФАПЧ ИЗ УСЛОВИЯ МАКСИМУМА ФУНКЦИИ ОБОБЩЕННОЙ МОЩНОСТИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,  
Ростов-на-Дону, Россия<sup>1</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: алгоритмы обработки, телеметрические системы, информационно-измерительные системы, цифровой модуль.

В статье показан разработанный алгоритм фазовой автоподстройки частоты в решении задаче оценки фазы позволяющий увеличить точность оценивания в сравнении с получившим распространение фильтром Калмана. Прикладная ценность такого решения продемонстрирована на задаче увеличения достоверности поверки генератора Г4-151.

## SYNTHESIS OF THE PLL SYSTEM FROM THE MAXIMUM CONDITION OF THE GENERALIZED POWER FUNCTION

«Don State Technical University» Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: processing algorithms, telemetry systems, information and measurement systems, digital module.

The article shows the developed algorithm of phase auto-tuning of frequency in solving the problem of phase estimation, which allows to increase the accuracy of estimation in comparison with the widespread Kalman filter. The applied value of such a solution is demonstrated on the task of increasing the reliability of the verification of the G4-151 generator.

### Введение.

Со времени появления (1921 г.) систем фазовой автоподстройки частоты (ФАПЧ) получили широкое распространение в различных устройствах связи [1], в измерительных системах, в узлах синхронизации запоминающих устройств с подвижным носителем информации. Например, ФАПЧ используются для обеспечения стабилизации частоты мощного генератора, основываясь на сигнале маломощного генератора, для создания высокостабильных возбудителей с дискретным множеством частот и устройств, что позволяет плавно и довольно точно изменять частоту высокостабильных генераторов. Также ФАПЧ используется в системах выделения несущей для синхронного и корреляционного приема, в системах телевидения, для фазовой синхронизации лазера, для деления и умножения частоты несущей, для создания фазовых и частотных модуляторов, для стабилизации скорости вращения и синхронизации электродвигателей и т. д. С каждым днем область применения ФАПЧ расширяется.

Реализация устройств ФАПЧ может быть аналоговой и цифровой. В обоих случаях структурная схема будет одинаковой и имеет три основных элемента:

- обратную связь, включающую в себя делитель частоты;
- регулируемый генератор;
- фазовый детектор [2].

Появление недорогих и простых в использовании микросхем устройств ФАПЧ открыло возможности ещё более широкого их применения. Так, например, их предлагается использовать при обработке сигналов вихревого потокоизмерителя. В потокоизмерителях этого типа (поток газа или жидкости) в трубопроводе после препятствия (вихреобразователя) в некотором диапазоне скоростей потока образуются вихри [2], частота которых пропорциональна скорости потока.

Таким образом, можно сделать вывод о том, что потребность в совершенствовании информационно-измерительных систем определяет направление дальнейшего совершенствования системы ФАПЧ. Поэтому оценку ее эффективности целесообразно проводить на примере решения задачи оценивания.

### Постановка задачи синтеза системы фазовой автоподстройки частоты как обратной задачи динамики.

До определенного времени имеющими наибольшее распространение были непрерывные аналоговые системы фазовой синхронизации (ФС), хотя для решения некоторых задач использовались и дискретные (цифровые) системы, к примеру, в системах передачи данных (СПД). Вместе с тем дискретность или непрерывность систем обычно обуславливалась ее назначением. Тем не менее в последние десятилетия за счет повышения

требований к показателям качества радиоаппаратуры и значительных успехов в развитии микроэлектроники дискретные методы обработки сигналов стали обширно использоваться так же и в тех областях, где до недавнего времени употреблялись аналоговые методы обработки. Цифровая система ФС может приниматься как характерный пример такого применения для выделения гармонической несущей из спектра сигнала, который принимается на фоне шума.

Цифровые методы обработки сигналов дали возможность стремительно быстро повысить динамический диапазон работы и стабильность параметров оборудования, а также обеспечить накопление и запоминание сигналов, удобство сопряжения с цифровой ЭВМ и возможности изменения параметров. Цифровые методы, в системах ФАПЧ позволяют реализовать стабильную работу при относительно низком отношении сигнал – шум во входном процессе, значительно уменьшить эквивалентный шумовой процесс при одновременном расширении полосы синхронизма, кроме того разрешить другие задачи, которые невозможно было решить в виду их сложности при использовании аналоговой аппаратуры.

Рассмотрим голономную [3] управляемую динамическую систему, для которой интеграл действия имеет вид

$$R = \int_0^{t_1} (T + A) dt, \quad (1)$$

где  $T = \frac{1}{2} \sum_{s,k=1}^n a_{sk} \dot{q}_s \dot{q}_k$  – кинетическая энергия;

$q = [q_1, \dots, q_n]^T$  – вектор обобщенных координат;

$a_{sk}$  – коэффициенты инерции;

$A = \int_{q(0)}^{q(t)} \sum_{s=1}^n Q_s dq_s$  – работа обобщенных внешних сил;

$Q = [Q_1(q, q, u), \dots, Q_n(q, q, u)]^T$  – непрерывный по совокупности переменных вектор обобщенных сил;

$u = [u_1, \dots, u_m]^T$  – вектор управления;

$q(0), q(t)$  – соответственно начальное и текущее состояние вектора обобщенных координат;

$n = \dim q \geq m = \dim u$ ;

$T$  – знак обозначающий транспонирование.

Потребуем, чтобы при движении системы из начального состояния

$$t=0, q(0) = [q_{10}, \dots, q_{n0}]^T, \quad \dot{q}(0) = [\dot{q}_{10}, \dots, \dot{q}_{n0}]^T \quad (2)$$

в конечном

$$t=t_1, q(t_1) = [q_{11}, \dots, q_{n1}]^T, \quad \dot{q}(t_1) = [\dot{q}_{11}, \dots, \dot{q}_{n1}]^T, \quad (3)$$

под действием управляющего воздействия  $u$  выполнялось соотношение, аналогичное принципу Гамильтона – Остроградского для (1)

$$\delta R = \int_0^{t_1} (\delta T + \delta' A) dt = 0, \quad (4)$$

где  $\delta'$  - бесконечно малая величина, зависящая от вектора вариаций обобщенных координат, но не являющуюся вариацией величины  $A$ .

Такое требование позволяет утверждать, что справедливы уравнения Лагранжа второго рода, которые для голономной системы можно представить в виде [14]

$$\frac{d}{dt} \left( \frac{\partial T}{\partial \dot{q}_s} \right) - \frac{\partial T}{\partial q_s} = Q_s, \quad s = \overline{1, n}. \quad (5)$$

Допустим что задана скалярная непрерывная вместе со всеми своими частными производными на всей области определения, знакопостоянная функция  $F(q, \dot{q})$ . Тогда опишем задачу так: найти вектор-функции  $Q(q, \dot{q})$  и  $q(t)$ , доставляющие минимум функционалу

$$J_1 = \int_0^{t_1} F(q, \dot{q}) dt \rightarrow \min, \quad (6)$$

при условиях (2), (3), (4).

#### Подход к решению поставленной задачи.

Для этого объединим методом неопределенных множителей Лагранжа интеграл целевого функционала (6) и интеграл действия по Гамильтону (4). Таким образом, задача (6) может быть переформулирована в следующем виде [3, 4]:

$$J = \int_0^{t_1} \{F(q, \dot{q}) + \lambda(T + A)\} dt \rightarrow \min, \quad (7)$$

где  $\lambda$  - множитель Лагранжа, и, следовательно, сведена к поиску минимума объединенного функционала (7) лишь с одним множителем Лагранжа.

Введем в рассмотрение функцию  $\Phi(q, \dot{q}, Q, \lambda)$

$$\Phi = \sum_{s=1}^n \Phi_s = \sum_{s=1}^n [\lambda Q_s(q, \dot{q}) + V_s(q, \dot{q})] \dot{q}_s \quad (8)$$

где  $V_s = \frac{\delta' F}{\delta q_s}$  - фиктивная обобщенная сила [8].

Возникает Теорема [8]: если  $\tilde{Q}(t)$  доставляет минимум функционалу (6) при условиях (2),(3),(4), то существует такой постоянный множитель Лагранжа  $\lambda$ , что при любом  $t \in [0, t_1]$  функция  $\Phi$  переменных  $(q, \dot{q}, Q)$  достигает в точке  $(\tilde{Q}(t), \hat{q}(t), \hat{q}(t))$  максимума

$$\Phi(\tilde{Q}(t), \hat{q}(t), \hat{q}(t)) = \max \Phi(Q, q, \dot{q}, \lambda). \quad (9)$$

На интервале  $[\tau + \Delta t, t_1]$  приращения обобщенных координат находится решением дифференциальных уравнений в вариациях, определяемых структурой системы (5) при начальных условиях в момент времени  $t = \tau + \Delta t$ .

Учитывая, что  $\delta q(t) = 0$ ,  $t \in [0, \tau]$ , главную часть приращения расширенного функционала (7) можно записать в виде

$$\begin{aligned} \Delta J = & \int_{\tau}^{\tau+\Delta t} \sum_{s=1}^n \left\{ \lambda [v - \tilde{Q}_s] + [V_s(v) - V_s(\tilde{Q})] \right\} \delta q_s dt + \int_{\tau}^{\tau+\Delta t} \left\{ \lambda (\delta T + \delta'A) + \delta'F \right\} dt + \\ & + \int_{\tau+\Delta t}^{t_1} \left\{ \lambda (\delta T + \delta'A) + \delta'F \right\} dt = \int_{\tau}^{\tau+\Delta t} \sum_{s=1}^n \left\{ \lambda [v - \tilde{Q}_s] + [V_s(v) - V_s(\tilde{Q})] \right\} \delta q_s dt + \\ & + \int_{\tau}^{t_1} \left\{ \lambda (\delta T + \delta'A) + \delta'F \right\} dt. \end{aligned} \quad (10)$$

Поскольку  $\delta q_s(\tau) = \delta q_s(t_1) = 0$ ,  $s = \overline{1, n}$  и с учётом справедливости (5), выражение для приращения функционала, с учётом малости  $\Delta t$ , запишем так

$$\begin{aligned} \Delta J = & \sum_{s=1}^n \left\{ \lambda [v - \tilde{Q}_s] + [V_s(v) - V_s(\tilde{Q})] \right\} \delta q_s \Delta t + \\ & + \int_{\tau}^{t_1} \left[ -\dot{\lambda} \sum_{s=1}^n \frac{\partial T}{\partial \dot{q}_s} \delta q_s \right] dt + \int_{\tau}^{t_1} \sum_{s=1}^n V_s \delta q_s dt. \end{aligned} \quad (11)$$

Пусть  $\tilde{Q}$  доставляет минимум функционалу (6). Определим множитель Лагранжа следующим образом:  $\dot{\lambda} = 0$ .

Тогда с учётом необходимого условия оптимальности  $\delta J \geq 0$ , непрерывности и знакоположительности функции  $F$ , для которой  $\delta'F \geq 0$ , получаем условие для оптимального управления при  $\Delta t \rightarrow 0$

$$\lambda \sum_{s=1}^n [\tilde{Q}_s - v] \dot{q}_s + \sum_{s=1}^n [V_s(\tilde{Q}) - V_s(v)] \dot{q}_s \geq 0. \quad (12)$$

Откуда

$$\sum_{s=1}^n [\lambda \tilde{Q}_s + V_s(\tilde{Q})] \dot{q}_s = \max \sum_{s=1}^n [\lambda Q_s + V_s(Q)] \dot{q}_s = \max \Phi(Q, q, \dot{q}, \lambda) \quad (13)$$

Таким образом, доказана теорема о минимуме целевого функционала в форме объединенного принципа максимума.

Синтез системы фазовой автоподстройки частоты. Применим объединенный принцип максимума для написания алгоритма обработки измерительной информации в задаче определения неустойчивости частоты гармонического сигнала с учетом, что  $\delta F \sim \delta \phi$ .

Пусть динамика фазы описывается выражением [3]

$$\ddot{\phi} = \eta, \quad (14)$$

модель наблюдения для измерительного канала имеет вид

$$y = A \sin(\omega t + (\phi + v)) + n, \quad (15)$$

где  $\omega$  – круговая частота;

$A$  – амплитуда сигнала;

$v$  – шум, определяемый винеровским процессом;

$n$  – белый гауссовский шум.

Критерий, определяющий качество оценки

$$\int_0^T [y - A \cdot \sin(\omega t + \phi)]^2 dt \rightarrow \min. \quad (16)$$

Используем сокращение записи

$$A \cdot \sin(\omega t + \phi) = H(\phi). \quad (17)$$

Тогда согласно теореме об объединенном принципе максимума

$$\eta = \lambda^{-1} \left\{ \mu \hat{\phi} - \frac{\partial H}{\partial \phi} [y - H(\hat{\phi})] \right\}, \quad (18)$$

Для определения выражения для  $\mu$  используем метод интегральных связей [8]

$$\begin{aligned} \frac{\hat{\phi}^2}{2} &= \eta \hat{\phi}, \\ \mu \hat{\phi} + \frac{\partial H}{\partial \phi} [y - H(\hat{\phi})] &= 0. \end{aligned} \quad (19)$$

Тогда для функции  $\eta$  с учетом вычислительной особенности реализации алгоритма имеем

$$\eta = \lambda^{-1} \left\{ - \frac{\hat{\phi} |\hat{\phi}| \left| \frac{\partial H}{\partial \phi} [y - H(\hat{\phi})] \right|}{2 |\eta| |\hat{\phi}| + \varepsilon} + \frac{\partial H}{\partial \phi} [y - H(\hat{\phi})] \right\}, \varepsilon = const. \quad (20)$$

Т.е. система ФАПЧ определяется уравнением

$$\hat{\phi} = \lambda^{-1} \left\{ - \frac{\hat{\phi} |\hat{\phi}| \left| \frac{\partial H}{\partial \phi} [y - H(\hat{\phi})] \right|}{2 |\eta| |\hat{\phi}| + \varepsilon} + \frac{\partial H}{\partial \phi} [y - H(\hat{\phi})] \right\}. \quad (21)$$

### **Заключение.**

Решение задачи синтеза системы ФАПЧ требует нахождения условий минимума целевого функционала, характеризующего погрешность измерений.

Использование концепции обратных задач динамики путем использования метода игольчатого варьирования к инвариантным признакам действительного движения позволяет получить условие минимума целевого функционала, которое имеет название объединенного принципа максимума. На основе теории объединенного принципа максимума синтезирована система ФАПЧ.

Работа подготовлена в рамках научной темы «Разработка беспилотных технологий на основе комплексной поэтапной оптимизации с редукцией экстремальных задач и инструментов нейро-нечеткого моделирования (FZNE-2022-0006)».

### **СПИСОК ЛИТЕРАТУРЫ**

1. Шахдильян В.В., Ляховский А.А. Системы фазовой автоподстройки частоты. М.: «Связь», 1972. 447 с.
2. Костоготов, А. А. Метод последовательных приближений в теории фильтрации / А. А. Костоготов // Автоматика и вычислительная техника. – 2000. – №3. – С. 53-63.
3. Костоготов А.А., Чеботарев А.В. Синтез оптимального алгоритма оценки фазы на основе объединенного принципа максимума // Автоматика и вычислительная техника. 2006. №6. С. 25-33.
4. Костоготов А.А., Костоготов А.И., Лазаренко С.В. Объединенный принцип максимума в задаче синтеза оптимального управления нелинейными системами // АВТ. 2007. №5. С. 52 – 61.
5. Справочник по теории автоматического управления / Под ред. А.А. Красовского. М.: Наука, 1987. 780 с.
6. Лурье А.И. Аналитическая механика. М.: Государственное издательство физико-математической литературы. 1961. 824 с.

**С.В. Лазаренко<sup>1</sup>, Д.А. Лихачев<sup>1</sup>, А.С Пеньков<sup>2</sup>, А.А. Манин<sup>3</sup>**

### **АНАЛИЗ ЭФФЕКТИВНОСТИ ФИЛЬТРА ОБЪЕДИНЕННОГО ПРИНЦИПА МАКСИМУМА ПРИ ОБРАБОТКЕ ИНФОРМАЦИИ О СОСТОЯНИИ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,  
Ростов-на-Дону, Россия<sup>1</sup>

Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный университет путей сообщения»,  
Ростов-на-Дону, Россия<sup>2</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>3</sup>

Ключевые слова: алгоритмы обработки, фильтрация, объединенный принцип максимума.

Один из вариантов адаптации структуры и параметров исследуемого процесса основан на методологии объединенного принципа максимума, что приводит к модели

---

динамической системы, которая удовлетворяет принципу Гамильтона-Остроградского. Структура модели определяется из условия максимума функции обобщенной мощности с точностью до нелинейной синтезирующей функции, определяющей скорость диссипации и, соответственно, степень структурной адаптации синтезированных на ее основе алгоритмов обработки измерительной информации.

**S.V. Lazarenko<sup>1</sup>, D.A. Lihachev<sup>1</sup>, A.S. Penkov<sup>2</sup> A.A. Manin<sup>3</sup>**

**ANALYSIS OF THE EFFECTIVENESS OF THE COMBINED MAXIMUM PRINCIPLE FILTER WHEN PROCESSING INFORMATION ABOUT THE STATE OF AN UNMANNED AERIAL VEHICLE**

«Don State Technical University» Rostov-on-Don, Russia<sup>1</sup>  
«Rostov State Transport University» Rostov-on-Don, Russia<sup>2</sup>  
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia<sup>3</sup>

Keywords: processing algorithms, filtering, combined maximum principle.

One of the options for adapting the structure and parameters of the process under study is based on the methodology of the combined maximum principle, which leads to a model of a dynamic system that satisfies the Hamilton-Ostrogradsky principle. The structure of the model is determined from the condition of the maximum of the generalized power function up to a nonlinear synthesizing function that determines the rate of dissipation and, accordingly, the degree of structural adaptation of measurement information processing algorithms synthesized on its basis.

**Введение.**

В процессе движения беспилотные летательные аппараты (БПЛА) испытывают воздействия ветровых порывов, турбулентностей атмосферы, возмущений, возникающих вследствие нестационарности характеристик и параметров самого аппарата и его исполнительных механизмов. Такого рода воздействия носят сложный характер, обусловленный случайными и регулярными факторами. БПЛА за счет бортовых цифровых вычислительных машин обладают потенциальной возможностью реализовать совершенные алгоритмы оценки ориентации и положения, которые способны обеспечить эффективное функционирование в таких условиях, что определяет необходимость дальнейшего развития теоретических и прикладных разработок в направлении синтеза адаптивных алгоритмов оценки параметров состояния динамических систем. Такие задачи решаются при разработке современных систем оценки, когда возникает необходимость осуществлять текущую идентификацию и адаптацию, обеспечивать инвариантность к заданному множеству возмущений.

Среди современных методов обработки измерительной информации важное место занимают методы оценивания состояния динамических систем с использованием принципов адаптации, которые связаны с изменением структуры, параметров и критериев функционирования.

Структурная адаптация предполагает использования множества моделей с процедурой направленного выбора модели при реализации процесса оценивания. Традиционные одномодельные способы оценки просты в реализации, однако позволяют достичь удовлетворительной точности только в одном режиме движения объекта. Одномодельные адаптивные алгоритмы состоят из двух этапов: принятия решения о наличии регулярного воздействия и оценки параметров с его учетом. Алгоритмы имеют широкий диапазон режимов движения, в которых сохраняется точность оценки, но обладают такими существенными недостатками как необходимость принятия решения о



---

выборе модели до начала фильтрации, а также отсутствие информации о возможной ошибке при принятии решения о выборе модели. [1]

Многомодельные (ММ) алгоритмы функционируют, используя в каждый момент времени несколько моделей движения цели. Результирующая оценка вычисляется на основе использования результатов работы всех элементарных фильтров. Преимущество ММ-алгоритмов выражается в уменьшении запаздывания обнаружения начала воздействия, что приводит к снижению ошибок оценивания состояния на участке нестационарности по сравнению с одномодельными алгоритмами. Недостатком ММ-алгоритмом является экспоненциальный рост возможных комбинаций состояний с течением времени, вследствие чего практическая реализация оптимального ММ-алгоритма часто не представляется возможной.

Адаптивные (самонастраивающиеся) системы – это системы, обеспечивающие компенсацию параметрических, сигнальных, функциональных или структурных неопределенностей динамического объекта за счет адаптации параметров модели в ходе рабочего функционирования системы. Другими словами, адаптивные системы восполняют нехватку априорной информации об объекте управления в ходе рабочего функционирования. В этом смысле они могут также называться самообучающимися системами.

**Способы обработки навигационной информации.** Для описания взаимного положения сопровождающего и связанного с объектом трехгранников могут быть использованы различные кинематические параметры: углы Эйлера – Крылова, направляющие косинусы, параметры Родрига – Гамильтона, параметры Кейли – Клейна и др. С математической точки зрения для описания алгоритмов идеальной работы БИНС все эти параметры приводят к одинаковым результатам. Различные кинематические параметры можно трактовать, как элементы соответствующего линейного пространства, так как все они допускают операции сложения и умножения на число. В каждом линейном пространстве задана операция ортогонального преобразования, позволяющая определить компоненты вектора (элемента пространства) при повороте системы координат. Другими словами, все пространства кинематических параметров изоморфны, т.е. все элементы и операции над ними в одном пространстве имеют взаимно-однозначные аналоги во всех остальных пространствах.

Кинематические уравнения в углах Эйлера — Крылова имеют невысокий порядок (третий) и понятную структуру, но содержат тригонометрические функции от искомым углов и допускают вырождение при угле тангажа, равное 90°. Все это обуславливает их непригодность в БИНС [5]. Уравнения БИНС, записанные с использованием матрицы направляющих косинусов, – линейные, определены для любых углов рыскания, тангажа и крена, однако уравнения Пуассона имеют достаточно высокий – девятый порядок. Кроме того, уравнения Пуассона должны быть дополнены шестью уравнениями связи.

Фильтр Калмана [1, 2] стал признанной основой для построения большинства алгоритмов оценки ориентации. Широкое использование решений Калмана являются доказательством их точности и эффективности, однако они имеют ряд недостатков. Они оказываются сложны в реализации. Координаты, описывающие кинематику в трёх измерениях, как правило, требуют реализации расширенного фильтра Калмана для линеаризации задачи, что требует большой вычислительной нагрузки и определяют чёткие мотивы для поиска альтернативных подходов. Многие подходы к решению этих задач основаны либо на нечёткой обработке или на предпочтении фильтра в пользу акселерометра для определения ориентации на малых угловых скоростях и интегрирование измерений гироскопа при обнаружении высоких угловых скоростей. Такой подход прост, но эффективен только при ограниченных условиях эксплуатации. Э. Бахман предложил альтернативный подход, при котором фильтр достигает оптимального комплексирования данных измерений на всех угловых скоростях. Тем не менее, процесс требует

---

дополнительной аппроксимации методом наименьших квадратов, что увеличивает вычислительную нагрузку. Р. Махони разработал комплементарный фильтр, который, как показывает практика, является эффективным решением. Однако, точность годится только для ИНС без магнитометра.

Основой построения алгоритмов оценки состояния управляемых динамических систем являются их математические модели, которые являются следствием законов движения, представленных в форме дифференциальных уравнений или вариационных принципов. Закон движения устанавливает зависимость состояния объекта от управляющего воздействия. При случайном воздействии для решения задачи оценки параметров траектории движения традиционно используются методы статистического синтеза. Среди решений, полученных на их основе, наиболее распространены алгоритмы калмановской структуры. Характерными недостатками являются относительно высокая вычислительная сложность и слабая зависимость коэффициентов обратной связи от наблюдений в установившемся режиме. В результате получили распространение квазиоптимальные алгоритмы оценивания. При этом ошибка выбора класса модели динамики объекта может приводить к неприемлемо высоким ошибкам оценивания. Это является одной из причин развития методов адаптивной динамической фильтрации.

В случае, когда вектор возмущения полагается квазидетерминированным, задача оценивания ставится как задача синтеза оптимального управления. Один из эффективных подходов к решению такой экстремальной задачи основывается на использовании теоремы о максимуме функции обобщенной мощности, что приводит к получению общей структуры математической модели возмущенной динамической системы с адаптацией к наблюдаемой динамике. Определение параметров полученной модели требует исследования поведения кинетического потенциала на характеристиках в фазовом пространстве. Это позволяет синтезировать семейство новых фильтров оценки навигационных параметров.

### **Результаты математического моделирования обработки навигационной информации с использованием фильтра, синтезированного на основе объединенного принципа максимума.**

С целью анализа качества функционирования синтезированного алгоритма проведено математическое моделирование процесса фильтрации показаний датчиков для определения ориентации применительно к инерциальной навигационной системе, включающей акселерометр и гироскоп.

В процессе моделирования обработка данных проведена тремя способами:

1. Расчет угла крена напрямую из зашумленных данных датчиков ориентации (зеленый цвет на графике);
2. Расчет угла крена при помощи классического фильтра Калмана (синий цвет на графике);
3. Расчет угла крена по предложенному алгоритму (3.13) (красный цвет на графике).

Кроме того, было рассчитана ошибка оценки фильтра Калмана (ФК) в сравнении с предложенным фильтром.

Результаты моделирования представлены на рисунках 1 и 2.

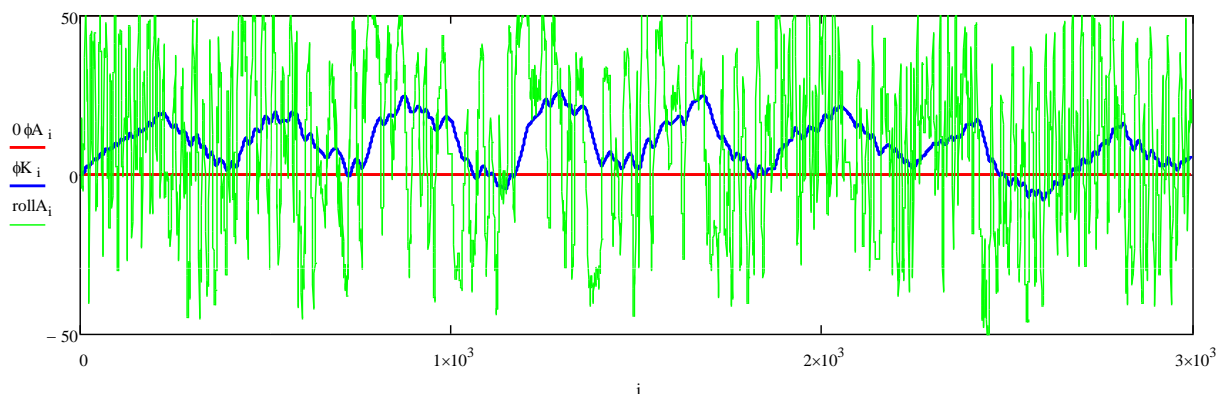


Рисунок 1. Результат работы классического ФК в сравнении с сырыми данными (в градусах)

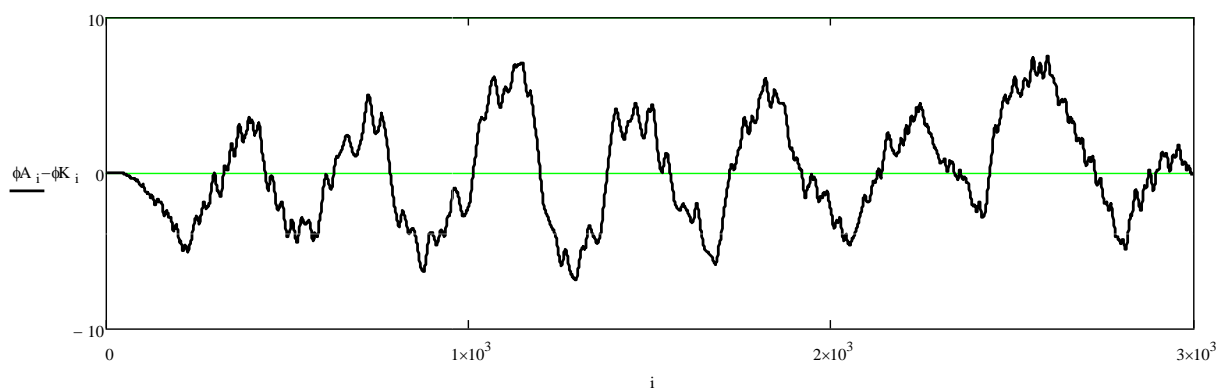


Рисунок 2. Ошибка ФК в сравнении с предложенным алгоритмом

Из графиков видно, что предлагаемый алгоритм позволяет получить более высокую точность определения положения в среднем на 3.3 градуса, а при резких изменениях угла – до 7 градусов, что позволяет сделать вывод о целесообразности использования алгоритма в полетных контроллерах БПЛА.

### Заключение.

Необходимо отметить, что такая высокая ошибка наблюдается в связи с тем, что в рамках данной работы для наглядности произведено моделирование системы, имеющей только микромеханический трехосевой акселерометр, обладающий высоким уровнем зашумленности выходного сигнала. В реальных системах оценки ориентации используется как минимум два датчика (акселерометр и гироскоп), совместная работа которых обеспечивает значительное повышение точности оценки.

Работа подготовлена в рамках научной темы «Разработка беспилотных технологий на основе комплексной поэтапной оптимизации с редукцией экстремальных задач и инструментов нейро-нечеткого моделирования (FZNE-2022-0006)».

### СПИСОК ЛИТЕРАТУРЫ

1. Костоготов А.А., Корнев А.С., Пугачев И.В., Лазаренко С.В. Модифицированный метод инвариантного погружения при синтезе измерительных процедур оценки параметров движения маневрирующей цели / А.А. Костоготов, А.С. Корнев, И.В. Пугачев, С.В. Лазаренко // Измерительная техника. – 2023. – № 2. – С. 47-Тихонов, В. И. Статистический анализ и синтез радиотехнических устройств и систем : учебное пособие / В. И. Тихонов, В. Н. Харисов. – Москва : Радио и связь, 1991. – 608 с.

- 
2. Андрашитов, Д. С. Регуляризованный алгоритм многопараметрической вариационной идентификации динамических систем / Д. С. Андрашитов, А. А. Костоготов, С. В. Лазаренко // Сервис в России и за рубежом. – 2011. – №. 8. – С. 25-36.

**И.В. Пугачев<sup>1</sup>, А.Н. Зубков<sup>1</sup>, В.О. Зехцер<sup>1</sup>, Ю.Д.Безуглов<sup>2</sup>**

### **СТРУКТУРА ЦИФРОВОЙ СИСТЕМЫ ОЦЕНКИ ПАРАМЕТРОВ ТЕЛЕМЕТРИЧЕСКИХ СООБЩЕНИЙ**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,  
Ростов-на-Дону, Россия<sup>1</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: Телеметрическое сообщение, цифровая система, нейронная сеть

В статье рассматривается разработка структуры цифровой системы оценки параметров телеметрических сообщений на основе методов теории интеллектуальных систем. Применение простейшей нейронной сети в совокупности с рекуррентной системой идентификации может повысить точность оценки без дополнительных затрат времени на обучение или оптимизацию структуры сети.

**I.V. Pugachev<sup>1</sup>, A.N. Zubkov<sup>1</sup>, V.O. Zehcer<sup>1</sup>, Yu.D.Bezuglov<sup>2</sup>**

### **THE STRUCTURE OF THE DIGITAL SYSTEM FOR EVALUATING THE PARAMETERS OF TELEMETRY MESSAGES**

«Don State Technical University» Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: Telemetry message, digital system, neural network

The article discusses the development of the structure of a digital system for estimating the parameters of telemetry messages based on the methods of the theory of intelligent systems. The use of a simple neural network in combination with a recurrent identification system can improve the accuracy of the assessment without additional time spent on training or optimizing the network structure.

#### **Введение.**

Номенклатура бытовой радиоэлектронной аппаратуры все время увеличивается. Однако, не смотря на ее разнообразие, основная тенденция ее развития заключается в интегрировании отдельных устройств в сложные информационно – измерительные системы. Большинство наблюдаемых физических процессов изменяются во времени и описываются математическими моделями в форме систем дифференциальных уравнений. Такое представление процессов имеет естественное происхождение и широко используется во многих практических приложениях, Но при построении вектора состояния модели, соответствующей реальной системе, возникает ряд трудностей, связанных с

---

необходимостью определения неизвестных параметров. Процедура их поиска получила название параметрической идентификации.

Традиционные решения задач идентификации с помощью нейронных сетей связаны с поиском их эффективной структуры, что связано со значительными временными затратами. В данной работе рассматривается новый метод синтеза систем идентификации, который обеспечивает повышение эффективности за счет комплексного использования нейросетевых и рекуррентных алгоритмов, полученных с использованием вариационных принципов. Результат синтеза представляет собой параллельно-последовательную процедуру обработки информации и существенно отличается от традиционных нейросетевых алгоритмов и алгоритмов калмановского типа, что определяет степень новизны данной работы. Полученные результаты моделирования позволяют сделать заключение, что совершенствование предложенной процедуры обработки может служить основой построения новых вариантов нейросетевых структур, ориентированных на задачи текущей идентификации параметров динамических систем.

С точки зрения обеспечения единства измерений измерение физической величины (ФВ) – совокупность операций по применению технического средства, хранящей единицу ФВ, обеспечивающих нахождение соотношения (в явном или неявном виде) измеряемой величины с ее единицей и получение значения этой величины [2].

Действительное значение ФВ – значение ФВ, полученное опытным путем, и настолько близкое к истинному, что в условиях поставленной измерительной задачи, может быть использовано вместо него. А истинное значение ФВ идеальным образом характеризует в качественном и количественном отношении данную ФВ. Оно может быть получено только в результате бесконечного процесса измерений с бесконечным совершенствованием методов и средств измерений.

Здесь под ФВ понимается одно из свойств физического объекта (физической системы или процесса), общее в качественном отношении для многих физических объектов, но в количественном отношении индивидуальное для каждого.

Погрешность – отклонение результата измерений от истинного (действительного). Поскольку истинное значение ФВ неизвестно, то на практике пользуются ее действительным значением. Если  $x_0$  - действительное значение,  $\Delta$  - погрешность,  $x_{изм}$  - измеренное значение, то [2]

$$x_{изм} = x_0 + \Delta x_{изм} . \quad (1)$$

Так как измеренное значение и погрешность измерений по сути – СВ, следовательно и  $x_0$  - СВ, то, действительное значение – оценка СВ  $x_{изм}$ , т.е. пользуясь обозначениями МС

$$x_{изм}^* = x_0 . \quad (2)$$

### **Постановка задачи.**

Рассматривается задача текущего определения параметров адаптивных динамических систем из условия минимума функционала невязки наблюдений. Разработанный метод идентификации приводит к получению новых структур обратных связей по переменным состояния и параметрам за счет построения инвариантов. Они позволяют формализовать априорную неопределенность динамики параметров за счет использования дополнительных свойств, проявляющихся на истинной траектории в соответствии со способом варьирования, который вытекает из положенного в основу динамики адаптивной системы и параметров принципа Гамильтона-Остроградского.

Принцип Гамильтона-Остроградского принят в качестве исходного положения динамики системы, для которой интеграл действия имеет вид

$$\dot{G} = \frac{\delta \dot{q}}{\delta \mathbf{z}}, \quad (3)$$

где  $\dot{q}$  – кинетическая энергия динамической системы;  
 $q$  – обобщенная координата.

Варьирование (3) приводит к уравнению Лагранжа второго рода, которое может быть разрешено относительно старшей производной

$$\begin{aligned} \ddot{q} &= f(q, \dot{q}, \mathbf{z}, t), \\ q(t_0) &= q^0, \quad \dot{q}(t_0) = \dot{q}^0, \end{aligned} \quad (4)$$

где  $\mathbf{z}$  – вектор неизвестных параметров;  
 $f$  – функция, непрерывная вместе со своими частными производными.

При этом предполагается, что рассматриваемая динамическая система записана относительно главных обобщенных координат  $\mathbf{x}$ , для которых гессиан системы  $L_{\dot{\mathbf{x}}\dot{\mathbf{x}}}$  представляет собой единичную матрицу.

Действительно, поскольку кинетическая энергия по определению является положительно определенной квадратичной формой произвольных обобщенных скоростей  $\dot{q}_s$ , ее всегда можно привести к сумме квадратов главных обобщенных скоростей  $\dot{x}_s$  с помощью некоторого невырожденного линейного преобразования.

Уравнение наблюдения имеет вид:

$$y = H(q, t) + \zeta(t), \quad (5)$$

где  $y$  – наблюдение;  
 $H(q, t)$  – непрерывная вместе с частными производными функция;  
 $\zeta(t)$  – белый гауссовский шум с известными локальными характеристиками.

### Нейросетевая идентификация динамических систем.

Поскольку подлежащий идентификации объект описывается решением дифференциального уравнения (4), то для формирования нейросети можно принять  $\mathbf{x}$  в качестве вектора состояния  $\mathbf{x} \in R^n$ ,  $\mathbf{z}$  – вектор неизвестных постоянных параметров  $\mathbf{z} \in R^m$ ,  $\mathbf{u}$  – вектор входных воздействий  $\mathbf{u} \in R^p$ ,  $\mathbf{y}$  – выходной вектор (5)  $\mathbf{y} \in R^l$ . Общее описание системы (4), (5), функционирующей в дискретном времени, может быть представлено в виде

$$\begin{aligned} \mathbf{x}_{i+1} &= \varphi[\mathbf{x}_i, \mathbf{u}_i, \mathbf{z}_i], \\ \mathbf{y}_i &= \psi[\mathbf{x}_i], \\ i &= \overline{1, n}, \end{aligned} \quad (6)$$

где  $\mathbf{x}_i, \mathbf{z}_i, \mathbf{u}_i, \mathbf{y}_i$  обозначают векторы мгновенных значений соответствующих переменных;

$\varphi$  и  $\psi$  – векторные стохастические нелинейные функции  $\varphi \in R^n, \psi \in R^l$ , полученные на основе процедуры конечно-разностной аппроксимации.

---

Задача идентификации объекта сводится к построению и обучению нейросетевой параметрической модели, чтобы отклики объекта  $y_i$  и модели  $\hat{y}_i$  на одно и то же возбуждение  $u_i$  совпадали в пределах допустимой невязки в соответствии с критерием (6) [1]

$$\|\hat{y} - y\| \leq \varepsilon. \quad (7)$$

Предлагается метод синтеза системы идентификации на базе комплексного использования нейронной сети и рекуррентного алгоритма для обработки данных наблюдения с целью определения приближенного значения и получения результирующей оценки параметра динамической системы. Для определения эффективности предложенного подхода рассмотрим следующий пример.

### **Структура цифровой системы оценки параметров.**

Рассмотрим задачу идентификации неизвестного параметра  $z$  в динамической системе второго порядка, которая описывает телеметрическое сообщение и записана в безразмерных величинах

$$\begin{aligned} \ddot{x} + z\dot{x} + 2x &= 0, \\ x(0) &= 1.5, \dot{x}(0) = 0. \end{aligned} \quad (8)$$

Идентификации параметра  $z$  производится по результатам наблюдения

$$y(t) = x(t) + n(t), \quad (9)$$

где  $n(t)$  – вектор белого гауссовского шума с известными локальными характеристиками.

Для решения поставленной задачи построим нейронную сеть для предварительной оценки параметра и рекуррентный алгоритм оценки для уточнения полученных оценок.

Структура нейронной сети приведена на рисунке 1, она построена в среде *Matlab*, состоит из двух слоёв. В первом слое 10 нейронов с функцией активации гиперболический тангенс, 10 входами и 1 выходом. Во втором слое 1 нейрон с линейной функцией активации, 10 входами и 1 выходом. На вход сети подаются обучающие наборы значений  $y(t)$  с погрешностью исходных данных  $\sigma = 0,05$ , на выходе имеем оценку  $z$ .

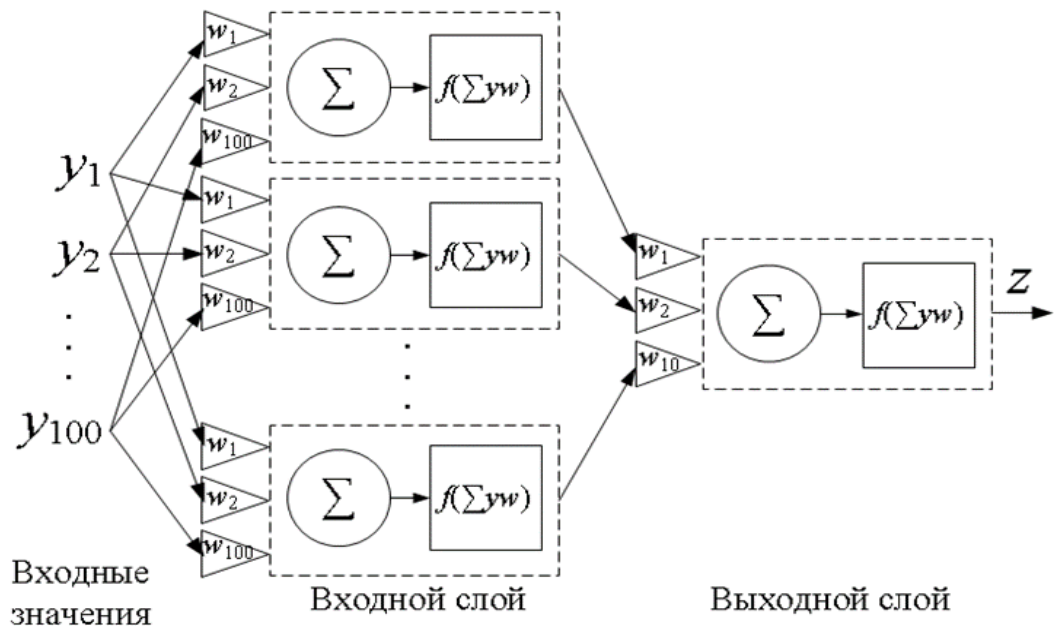


Рисунок 1. Структура искусственной нейронной сети

Рассмотрим применение рекуррентной процедуры идентификации с использованием полученных нейросетевым методом оценок в виде начального приближения параметра  $\hat{z}(0)$ .

Уравнения идентификации имеют вид

$$\begin{aligned} \dot{\hat{x}} &= -\hat{z}\hat{x} - 2\hat{x} - \mu^{-1}(\hat{x} - y), \quad \ddot{G} = -\hat{z}\dot{G} - 2G - \hat{x}, \\ \dot{\hat{z}} &= PG(\hat{x} - y), \quad \dot{P} = \alpha^{-1} - P^2G^2, \\ \hat{x}(0) &= 1,5, \quad \dot{\hat{x}}(0) = 0, \quad G(0) = \dot{G}(0) = 0,5, \quad P(0) = 0,5. \end{aligned} \quad (10)$$

Алгоритм (10) в конечно-разностном виде:

$$\begin{aligned} x_i &= 2x_{i-1} - x_{i-2} - z_{i-1}\Delta t(x_{i-1} - x_{i-2}) - 2\Delta t^2 x_{i-1} - \Delta t^2 \mu^{-1}(x_{i-1} - y_{i-1}), \\ g_i &= 2g_{i-1} - g_{i-2} - z_{i-1}\Delta t(g_{i-1} - g_{i-2}) - 2\Delta t^2 g_{i-1} - \Delta t^2(x_{i-1} - x_{i-2}), \\ p_i &= \Delta t(\alpha^{-1} - p_{i-1}^2 g_{i-1}^2) + p_{i-1}, \\ z_i &= \Delta t p_{i-1} g_{i-1}(x_{i-1} - y_{i-1}) + z_{i-1}, \\ x_{i-1} &= x_{i-2} = 1,5, \quad g_{i-1} = 0,55, \quad g_{i-2} = 0,5, \\ p_{i-1} &= 0,5, \quad z_{i-1} = \hat{z}(0), \quad \Delta t = 0,25. \end{aligned} \quad (11)$$

Результаты оценки параметра с использованием алгоритма (11) имеют следующие значения:  $\hat{z}_{u1} = 0,407$  при  $\mu = 0,23$  и  $\alpha = 4,6$ ,  $\hat{z}_{u2} = 0,603$  при  $\mu = 0,075$  и  $\alpha = 20$ ,  $\hat{z}_{u3} = 0,805$  при  $\mu = 0,06$  и  $\alpha = 5$ ,  $\hat{z}_{u4} = 1,027$  при  $\mu = 0,1$  и  $\alpha = 5$  соответственно. Временные диаграммы процесса идентификации представлены на рисунках 2-5. Среднее значение ошибки идентификации составляет 1,35%.



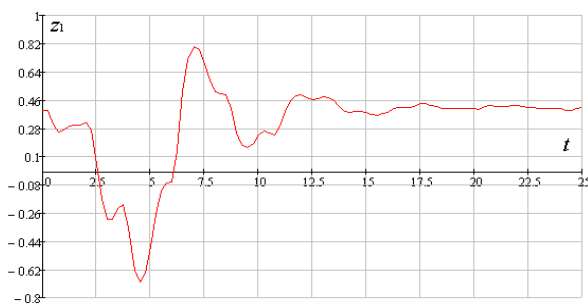


Рисунок 2 - Оценка параметра  $z_1$



Рисунок 3 - Оценка параметра  $z_2$



Рисунок 4 - Оценка параметра  $z_3$

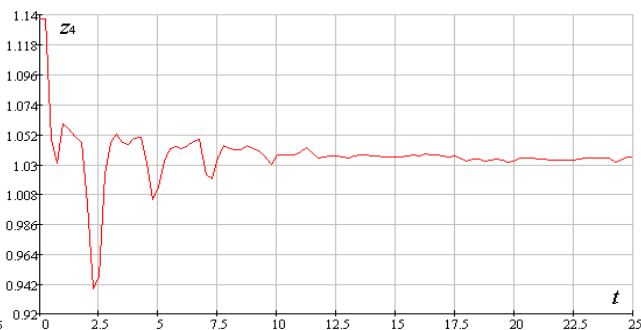


Рисунок 5 - Оценка параметра  $z_4$

В работе проведено исследование зависимости точности оценок от уровня шумов в исходных данных. Анализ точности оценок, полученных с использованием комплексной идентификации, позволяет сделать вывод о высокой эффективности применения рекуррентных процедур идентификации в совокупности с простейшими нейронными сетями.

### Заключение.

Предложена структура цифровой системы оценки параметров телеметрических сообщений на основе использования нейронной сети. Произведена оценка ее эффективности на основе математического моделирования. Результаты математического моделирования простейшей нейронной сети и оценок рекуррентной идентификации, позволяют сделать вывод, что комплексная система идентификации позволяет практически на порядок повысить точность идентификации без использования традиционных процедур. Таким образом, используя простейшую нейронную сеть в совокупности с рекуррентной системой идентификации, можно повысить точность оценки параметров динамической системы без дополнительных затрат времени на обучение или оптимизацию структуры сети, что исключительно актуально для систем реального времени.

Работа подготовлена в рамках научной темы «Разработка беспилотных технологий на основе комплексной поэтапной оптимизации с редукцией экстремальных задач и инструментов нейро-нечеткого моделирования (FZNE-2022-0006)».

### СПИСОК ЛИТЕРАТУРЫ

1. Ананьевский, И.М. Синтез непрерывного управления механической системой с неизвестной матрицей инерции / И.М. Ананьевский // Изв. РАН. Теория и системы управления – 2006. – № 3. – С. 24 – 35.
2. Универсальный метод синтеза оптимальных управлений нелинейными Лагранжевыми динамическими системами / Д.С. Андрашитов, А.А. Костоготов, А.И. Костоготов, С.В. Лазаренко // Инженерный вестник Дона. – 2014. – № 1 (28). – 200 с.

3. Структурный синтез Лагранжевых систем автоматического управления с использованием первых интегралов движения / Д.С. Андрашитов, А.А. Костоготов, А.А. Кузнецов, С.В. Лазаренко // Информационно-измерительные и управляющие системы. – 2015. – № 12. – С. 12 – 18.
4. Афанасьев, В.Н. Динамические системы управления с неполной информацией : алгоритмическое конструирование / В.Н. Афанасьев. - Москва : КомКнига, 2007. – 204 с.
5. Ашурбейли, И.Р. Основные направления развития средств воздушно-космической обороны Российской Федерации / И.Р. Ашурбейли, А.И. Лаговьер // Успехи современной радиоэлектроники. – 2009. – № 12. – С.46 – 54.
6. Бар-Шалом, Я. Траекторная обработка. Принципы, способы и алгоритмы. Ч. 2 / Я. Бар-Шалом. – Москва : МГТУ им. Н. Э. Баумана, 2011. – 244 с.

**С.В. Лазаренко<sup>1</sup>, В.М. Евтюхов<sup>1</sup>, И.А. Енгибарян<sup>2</sup>**

### **СИНТЕЗ ИНТЕЛЛЕКТУАЛЬНОГО ФИЛЬТРА СОПРОВОЖДЕНИЯ С НЕЧЕТКОЙ СТРАТЕГИЕЙ НАСТРОЙКИ ПАРАМЕТРОВ В ЗАДАЧАХ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,  
Ростов-на-Дону, Россия<sup>1</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: алгоритмы обработки, интеллектуальность, фильтрация, фильтр Калмана.

В исследовании развивается подход к синтезу нечетких фильтров сопровождения на основе построения динамических моделей движения из условия максимума функции обобщенной мощности. Это, как показано в работе, позволяет получить нелинейную матрицу перехода состояний. Она за счет выбора параметра адаптации с достаточной на практике степенью точности может быть представлена как матрица перехода состояний, получаемая с применением математической модели движения объекта с постоянной скоростью. Тогда применение базы правил конъюнктивного типа для описания движения маневрирующего летательного аппарата приводит к нечеткому фильтру сопровождения. На основе математического моделирования установлено его превосходство по показателю точности над интеллектуальным альфа-бета фильтром, построенным с использованием математической модели движения объекта с постоянной скоростью, и фильтром Калмана, синтезированным на основе математической модели ускорения Зингера.

**S.V. Lazarenko<sup>1</sup>, V.M. Evtyukho<sup>1</sup>, I.A. Engibaryan<sup>2</sup>**

### **SYNTHESIS OF AN INTELLIGENT SUPPORT FILTER WITH A FUZZY STRATEGY FOR SETTING PARAMETERS IN AIR TRAFFIC CONTROL AUTOMATION TASKS**

«Don State Technical University» Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

---

Keywords: processing algorithms, telemetry systems, filtering, Kalman filter.

The study develops an approach to the synthesis of fuzzy tracking filters based on the construction of dynamic motion models from the condition of the maximum of the generalized power function. This, as shown in the work, allows us to obtain a nonlinear state transition matrix. Due to the choice of the adaptation parameter, with a sufficient degree of accuracy in practice, it can be represented as a state transition matrix obtained using a mathematical model of the movement of an object at a constant speed. Then the use of a conjunctive type rule base to describe the movement of a maneuvering aircraft leads to a fuzzy tracking filter. Based on mathematical modeling, its superiority in terms of accuracy over the intelligent alpha-beta filter, built using a mathematical model of object motion with a constant speed, and the Kalman filter, synthesized based on a mathematical model of Singer acceleration, has been established.

### **Введение.**

Теория Винера-Колмогорова оптимальной фильтрации послужила стимулом преодоления проблем, создаваемых уравнением Винера-Хопфа. Для порождаемых линейными дифференциальными уравнениями стационарных процессов были получены уравнения оценки без использования уравнения Винера-Хопфа, которые отличаются, прежде всего, разностным уравнением ковариации ошибки фильтрации. Несмотря на то, что эти методы развивались независимо, все они тесно связаны с поиском экстремума квадратичных форм [1 – 8]. При этом подобный синтез фильтров сопровождения летательных аппаратов осложняется отсутствием априорных сведений о параметрах маневров воздушных целей. Это послужило развитию методов решения экстремальных задач в совокупности с разработкой процедур восстановления недостающей информации, что получило обобщенное название адаптивной фильтрации.

В рамках такого подхода рассматривается не отдельный объект, а некоторое множество объектов, каждому из которых ставится в соответствие абстрактный параметр. Кроме того предполагается, что динамика каждого объекта задается множеством изменяющихся настраиваемых параметров (настроек). Их совокупность называют стратегией настройки параметров, которая должна обеспечить задаваемую функционалом цель функционирования объекта. В теории статистического синтеза настройки чаще всего связываются с параметрами формирующего фильтра. Для их идентификации не редко расширяется пространство состояний и решается задача оценки. Однако на практике, например, в задаче цифровой обработки результатов радиолокационных измерений параметров движения маневрирующих летательных аппаратов, нет возможности накопить необходимую статистику. Выход из такой ситуации может базироваться на нечеткой логике.

Среди интеллектуальных фильтров сопровождения широко распространены различные варианты альфа-бета фильтров [9, 10]. Положенные в основу подобных решений математические модели, как правило, традиционные и не подлежат адаптации. Это приводит к относительно простым вычислительным процедурам и не позволяет приблизиться к потенциальной точности оценивания. Одно из конструктивных направлений выхода из описанной ситуации может заключаться в применении динамических моделей движения при синтезе интеллектуальных фильтров сопровождения.

В исследовании развивается подход к построению динамических моделей движения, основанный на использовании условия максимума функции обобщенной мощности. Это, как показано в работе, позволяет получить нелинейную матрицу перехода состояний. Она за счет выбора параметра адаптации с достаточной на практике степенью точности вырождается в матрицу перехода состояний, получаемую с применением математической модели движения объекта с постоянной скоростью. Это позволяет предложить процедуру подстройки алгоритма оценки к маневрам летательного аппарата, базирующуюся на экспертном выборе параметра адаптации. Входные данные синтезируемого нечеткого фильтра – ускорение летательного аппарата и величина порога принятия решения о начале

---

маневра цели, что позволяет отнести наблюдаемое движение к одному из пяти вариантов: прямолинейное равномерное движение, прямолинейное равноускоренное движение, поворот с приблизительно постоянной скоростью, поворот с ускорением и маневр. Процесс принятия решения о значении выходного сигнала происходит в соответствии с базой правил конъюнктивного типа по Мамдани. Для дефазификации выбран центроидный метод [11].

Целью исследования является синтез интеллектуального фильтра сопровождения из условия максимума функции обобщенной мощности и оценка его эффективности путем математического моделирования цифровой обработки результатов радиолокационных измерений на основе экспертных знаний о режимах движения летательных аппаратов.

#### **Постановка экстремальной задачи.**

Задачи параметрической оценки математических моделей очень часто являются некорректно поставленными [3]. Общая запись обратной задачи может быть представлена в форме операторного уравнения

$$A \cdot u = f, u \in U, f \in F, \quad (1)$$

где  $u$  и  $f$  - соответственно искомая и наблюдаемая характеристики, которые трактуются как элементы метрических пространств  $U$  и  $F$ . Оператор  $A:U \rightarrow F$  предполагается заданным, имеет область определения  $D(A) \subseteq U$  и область значений  $R(A) \subseteq F$ .

Для решения обратных задач применяют методы теории некорректных задач - теории регуляризации. Одно из перспективных направлений развития теории регуляризации - итерационная регуляризация, в основе которого лежит принцип регуляризации А.Н. Тихонова. Суть указанного направления заключается в построении регуляризирующих алгоритмов на основе различных итерационных методов, причем параметром регуляризации является номер итерации.

Наиболее удобным для исследований является метод простой итерации. Его сходимость при точных исходных данных для уравнений с линейным непрерывным оператором, не имеющим ограниченного обратного, была доказана В.М. Фридманом, который также доказал и сходимость нелинейных градиентных методов типа скорейшего спуска.

Кроме того, следует также обозначить ещё одну проблему, носящую уже сугубо практический характер - отсутствие интегрированной программной системы построения моделей оценки с поддержкой всех этапов процесса моделирования. Существующие программные пакеты, как правило, ориентированы или только на какой-то отдельный этап (например, корреляционный анализ данных), или же предназначены для решения узкого круга задач на весьма ограниченном множестве моделей (чаще всего линейных, внутрилинейных и полиномиальных). Пакеты, которые на рынке программного обеспечения позиционируются как универсальные, также несвободны от указанных недостатков: их универсальность приводит к тому, что для решения каждой отдельной подзадачи предлагаются только самые простые варианты, что явно недостаточно для практических целей. Наконец, многие из аналитических программных пакетов ориентированы на моделирование в социально-экономических дисциплинах, в которых стандарты моделирования и правила представления моделей сильно отличаются от принятых в физико-математических и технических областях.

---

**Общий вид уравнений алгоритма оценки параметров телеметрических сообщений.**

Рассмотрим математическую постановку задачи. Формальное отнесение части энергии к работе обобщенных сил  $Q_s(q, \dot{q}, U)$  при движении в режиме декомпозиции позволяет ввести простейшую определенно положительную квадратичную форму скоростей, которая трактуется как кинетическая энергия системы

$$T = \frac{1}{2} \sum_{s=1}^n a_{ss} \dot{q}_s^2, \quad s = \overline{1, n}. \quad (2)$$

где  $q_s, \dot{q}_s$  – обобщенные координаты и скорости;  
 $a_{sk}$  – коэффициенты инерции

В пространстве наблюдений выбран целевой функционал [3], принимающий некоторое заданное значение, которое определяет точность измерения фазовых координат исследуемой системы

$$J = \frac{1}{2} \int_{t_0}^{t_1} \sum_{s=1}^n N_{ss}^{-1} [\mathbf{y}_s - \hat{\mathbf{q}}_s]^2 dt = \int_{t_0}^{t_1} F(\hat{q}) dt = D, \quad (3)$$

где  $N_{ss}$  – элементы диагональной весовой матрицы  $N$ , характеризующей интенсивность помех в канале наблюдений;

$D$  – взвешенная априорная дисперсия результатов измерений каналов наблюдения.

Для наблюдаемой системы с кинетической энергией (2) в режиме декомпозиции за счет обратных связей модель двигается в соответствии с целью, которая определяется значением функционала (3). В силу допущения о том, что движение в режиме декомпозиции полностью устраняет динамическое взаимовлияние между элементами, имеем соотношение

$$|\dot{\mathbf{q}}_s| = \sqrt{a_{ss}^{-1} \lambda^{-1} N_{ss}^{-1}} |\mathbf{y}_s - \mathbf{q}_s|, \quad s = \overline{1, n}. \quad (4)$$

Общий вид уравнения динамической квазидетерминированной оценки определяется следующей формулой

$$\frac{d}{dt} \left( \frac{\partial T}{\partial \dot{\mathbf{q}}_s} \right) - \frac{\partial T}{\partial \mathbf{q}_s} = \lambda^{-1} \left[ -\lambda \frac{|\dot{\mathbf{q}}_s|}{N_{ss}^{-1} |\mathbf{y}_s - \mathbf{q}_s|} \dot{\mathbf{q}}_s - N_{ss}^{-1} (\mathbf{y}_s - \mathbf{q}_s) \right].$$

С учетом принятой модели кинетической энергии и кинематической связи (4) получим уравнения оценки в виде

$$\ddot{\mathbf{q}}_s(t) = -\sqrt{\lambda_s^{-1}} \dot{\mathbf{q}}_s(t) - \lambda_s^{-1} (\mathbf{y}_s(t) - \hat{\mathbf{q}}_s(t)), \quad (5)$$

где  $\lambda_s = a_{ss} \lambda N_{ss}$  – коэффициент адаптации.

**Решение задачи оценки параметров.**

Состояние описывается дифференциальным уравнением второго порядка

$$\ddot{x} = f(x, \dot{x}, z^0, z^1) = z^0 \dot{x} + z^1 x. \quad (6)$$

В общем случае уравнение (6) описывает затухающие колебания в некоторой динамической системе, а параметр  $z_0$  - декремент затухания. Пусть параметр  $z_0$  - это постоянная времени. Тогда  $x$  - напряжение [2].

Уравнение наблюдения имеет вид

$$y(t) = x(t). \quad (7)$$

Применение (1) с учетом процесса расширения пространства состояний требует представления уравнения состояния в форме:

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{F}(\mathbf{x}, \mathbf{z}) = \begin{bmatrix} x^1 \\ z^0 x^1 + z^1 x^0 \end{bmatrix}, \\ \dot{\mathbf{z}} &= \boldsymbol{\eta}, \quad \mathbf{z}(t_0) = \mathbf{z}(0), \end{aligned} \quad (8)$$

где

$$\mathbf{x} = \begin{bmatrix} x^0 \\ x^1 \end{bmatrix};$$

$$\boldsymbol{\eta} = \begin{bmatrix} \eta^0 \\ \eta^1 \end{bmatrix};$$

$$\mathbf{z} = \begin{bmatrix} z^0 \\ z^1 \end{bmatrix}.$$

Тогда уравнение наблюдения (7) примет следующую форму

$$\mathbf{y}(t) = \mathbf{x}(t), \quad (9)$$

где

$$\mathbf{y}(t) = \begin{bmatrix} y^0 \\ y^1 \end{bmatrix} = \begin{bmatrix} x^0 \\ 0 \end{bmatrix}.$$

Функционал невязки записывается следующим образом:

$$J_1 = \frac{1}{2} \int_0^T [\mathbf{y} - \hat{\mathbf{x}}]^T [\mathbf{y} - \hat{\mathbf{x}}] dt \rightarrow \min. \quad (10)$$

Уравнения синтезированного алгоритма оценки параметров принимают вид:

- первая итерация

$$\begin{aligned} \hat{\mathbf{z}}_0 &= \mathbf{P}_0 \mathbf{G}_0^T \gamma_0^0 (\mathbf{y} - \hat{\mathbf{x}}_0), \\ \hat{\mathbf{x}}_0 &= \mathbf{F}(\hat{\mathbf{x}}_0, \mathbf{z}_0) + \mu_0^{-1} \gamma_0^0 (\mathbf{y} - \hat{\mathbf{x}}_0), \\ \dot{\mathbf{P}}_0 &= \mathbf{I} + \mathbf{P}_0 \mathbf{G}_0^T \gamma_0^0 \mathbf{G}_0 \mathbf{P}_0, \\ \dot{\mathbf{G}}_0 &= \frac{\partial \mathbf{F}}{\partial \hat{\mathbf{x}}_0} \mathbf{G}_0 + \frac{\partial \mathbf{F}}{\partial \hat{\mathbf{z}}_0}; \end{aligned} \quad (11)$$

- вторая итерация

$$\begin{aligned}
\hat{\mathbf{z}}_1 &= \mathbf{P}_1 \mathbf{G}_1^T \left\{ (1 - \gamma_0^1) (\mathbf{y} - \hat{\mathbf{x}}_0) + (\mathbf{y} - \hat{\mathbf{x}}_1) \right\}, \\
\hat{\mathbf{x}}_1 &= \mathbf{F}(\hat{\mathbf{x}}_1, \mathbf{z}_1) + \mu_1^{-1} \left\{ (1 - \gamma_0^1) (\mathbf{y} - \hat{\mathbf{x}}_0) + (\mathbf{y} - \hat{\mathbf{x}}_1) \right\}, \\
\dot{\mathbf{P}}_1 &= \mathbf{I} - \mathbf{P}_1 \mathbf{G}_1^T (1 - \gamma_0^1) \gamma_0^1 \mathbf{G}_1 \mathbf{P}_1, \\
\dot{\mathbf{G}}_1 &= \frac{\partial \mathbf{F}}{\partial \hat{\mathbf{x}}_1} \mathbf{G}_1 + \frac{\partial \mathbf{F}}{\partial \hat{\mathbf{z}}_1},
\end{aligned} \tag{12}$$

где  $\hat{\mathbf{x}}_0(0) = [0,3 \quad 0,01]^T$ ,  $\hat{\mathbf{x}}_1(0) = [0,3 \quad 0,01]^T$ ;

$$\hat{\mathbf{z}}_0(0) = \hat{\mathbf{z}}_1(0) = [0 \quad 0]^T;$$

$$\mathbf{G}_0(0) = \mathbf{G}_1(0) = \begin{bmatrix} 0,1 & 0,02 \\ 0,02 & 0,1 \end{bmatrix};$$

$$\mathbf{P}_0(0) = \mathbf{P}_1(0) = \begin{bmatrix} 7 & 0,01 \\ 0,01 & 7 \end{bmatrix};$$

$$\mu_0 = 18, \quad \gamma_0^0 = 1, \quad \mu_1 = 12, \quad \gamma_0^1 = 0,5.$$

Получен алгоритм оценки параметров динамической системы с использованием вариационных принципов и итерационной регуляризации (11), (12). Он позволяет решать эффективно задачи оценки за счет повышения точности получаемых оценок и увеличения скорости их сходимости при реализации последовательного алгоритма оценки.

Анализ результатов численного моделирования, полученных в среде *MathCAD*, показывает, что выигрыш в точности на второй итерации по отношению к первой составляет,  $\delta z^0 = 3,3\%$ ,  $\delta z^1 = 5,1\%$ , соответственно для параметров аналогичных коэффициентам диссипации и жесткости. Это подтверждает эффективность разработанного метода. При этом необходимо отметить, что в соответствии с исследованиями первая итерация уже обеспечивает выигрыш в точности в сравнении с фильтром Калмана.

### **Заключение.**

В статье представлен Получен алгоритм оценки параметров с использованием вариационных принципов и итерационной регуляризации (11), (12). Он позволяет решать эффективно задачи оценки за счет повышения точности получаемых оценок и увеличения скорости их сходимости при реализации последовательного алгоритма оценки.

В соответствии с исследованиями первая итерация предлагаемого алгоритма оценки уже обеспечивает выигрыш в точности в сравнении с фильтром Калмана

Разработанный модуль оценки содержит четыре взаимосвязанные структуры, что определяются формой уравнений.

Работа подготовлена в рамках научной темы «Разработка беспилотных технологий на основе комплексной поэтапной оптимизации с редукцией экстремальных задач и инструментов нейро-нечеткого моделирования (FZNE-2022-0006)».

### **СПИСОК ЛИТЕРАТУРЫ**

1. Глинченко, А. С. Цифровая обработка сигналов. Часть 1 : учебное пособие. – Красноярск : издательство КГТУ, 2011. – 1999 с.
2. Костоготов, А. А. Метод последовательных приближений в теории фильтрации / А. А. Костоготов // Автоматика и вычислительная техника. – 2000. – №3. – С. 53-63.

3. Тихонов, В. И. Статистический анализ и синтез радиотехнических устройств и систем : учебное пособие / В. И. Тихонов, В. Н. Харисов. – Москва : Радио и связь, 1991. – 608 с.
4. Андрашитов, Д. С. Регуляризованный алгоритм многопараметрической вариационной идентификации динамических систем / Д. С. Андрашитов, А. А. Костоготов, С. В. Лазаренко // Сервис в России и за рубежом. – 2011. – №. 8. – С. 25-36.
5. Андрашитов, Д. С. Многопараметрическая вариационная идентификация динамических систем на основе объединенного принципа максимума / Д. С. Андрашитов, А. А. Костоготов, С. В. Лазаренко // Информационно-управляющие системы. – 2012. – №4(10). – С. 68-76.

**И.В. Пугачев<sup>1</sup>, Е.О. Камер<sup>1</sup>, В.И. Юхнов<sup>2</sup>**

### **АДАПТИВНЫЕ МНОГОРЕЖИМНЫЕ РЕГУЛЯТОРЫ АВТОМАТИЗИРОВАННЫХ РАДИОТЕХНИЧЕСКИХ СИСТЕМ**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,  
Ростов-на-Дону, Россия<sup>1</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: ПИД регулятор, управление антенной, обратная задача динамики, обратная связь.

В статье рассматривается радиоэлектронная аппаратура как информационно – измерительная система. При этом высокие требования, предъявляемые к ней, определяют выделение в ее структуре информационно – управляющей системы. Существующие информационно – управляющие системы бытовой радиоэлектроники, как правило, на квазиоптимальных алгоритмах функционирования. Повышение их эффективности может базироваться на объединенном принципе максимума.

**I.V. Pugachev<sup>1</sup>, E.O. Kamer<sup>1</sup>, V.I. Yukhnov<sup>2</sup>**

### **ADAPTIVE MULTI-MODE REGULATORS OF AUTOMATED RADIO ENGINEERING SYSTEMS**

«Don State Technical University» Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: PID controller, antenna control, inverse dynamics problem, feedback..

The article considers radio–electronic equipment as an information and measuring system. At the same time, the high requirements imposed on it determine the allocation of an information management system in its structure. The existing information and control systems of household radio electronics, as a rule, are based on quasi–optimal algorithms of functioning. Increasing their efficiency can be based on the combined principle of maximum.



---

### **Введение.**

Бытовая радиоэлектронная аппаратура часто в своем составе имеет информационно – управляющую систему (ИУС). Классический пример – системы фазовой автоподстройки частоты [1].

Такие системы в качестве исполнительных устройств используют преобразователи, превращающие входной сигнал (электрический, оптический и др.) в выходной сигнал. Современные информационно – управляющие системы базируются на использовании цифрового компьютера. Последние два десятилетия были ознаменованы резким повышением надежности и удешевлением компьютеров. В связи с этим они все шире стали применяться в качестве регуляторов (корректирующих устройств). В такой системе по определенной программе обрабатывает представленную в цифровой форме ошибку и выдает на выходе сигнал также в цифровой форме. Программа может быть написана так, что качество системы в целом будет равно или очень близко к заданному. При этом основой таких программ традиционно являются различные модификации пропорционально – интегрально – дифференциальных (ПИД) алгоритмов. Это не позволяет добиться потенциальной эффективности функционирования бытовой радиоэлектронной аппаратуры. Кроме того, область работы таких решений ограничена, что приводит к необходимости синтеза совокупности алгоритмов для каждого из режимов функционирования.

### **Применение цифровых систем управления.**

За последние тридцать лет общее число цифровых систем управления, используемых в промышленности, значительно выросло, и сейчас их насчитывается около 100 миллионов, хотя имеется большой разброс по размеру и производительности компьютеров, входящих в состав этих систем. Цифровое управление имеет ряд преимуществ, куда относятся: повышенная точность измерений; использование цифровых сигналов (кодов), датчиков и преобразователей и микропроцессоров; меньшая чувствительность к шумам и помехам; возможность легко изменять алгоритм управления в программном обеспечении. Повышенная точность (чувствительность) измерений объясняется тем, что цифровые датчики и устройства работают с маломощными сигналами. Наличие цифровых сигналов дает возможность использовать широкий спектр цифровых устройств и линий коммуникации. Цифровые датчики и преобразователи способны эффективно измерять, передавать сигналы и связывать между собой различные устройства. Кроме того, многие системы объективно являются цифровыми, потому что они работают с импульсными сигналами. Примерами таких систем могут служить радиолокационные системы слежения и системы управления спутниками.

### **Традиционные алгоритмы функционирования.**

В технике используют довольно много различных законов регулирования, которые тесно связаны с конструкцией управляющего устройства, и одним из распространенных видов классификации регуляторов непрерывного действия является классификация по законам управления.

Статические, или пропорциональные, регуляторы (сокращенно П-регуляторы) представляют собой устройства, в которых величина регулирующего воздействия  $\mu$  пропорциональна входной величине  $\sigma$ . Пропорциональные регуляторы не могут поддерживать постоянное значение регулируемой величины, так как перемещение регулирующего органа в таких системах однозначно связано с изменением входной величины, следовательно, всякому новому его положению, необходимому при изменениях нагрузки, отвечает некоторое новое значение регулируемого параметра. Это неизбежное отклонение называют остаточной неравномерностью регулирования или статической ошибкой. Величина остаточной неравномерности тем меньше, чем больше коэффициент передачи регулятора по прямому тракту. Достоинство пропорциональных регуляторов в их

---

относительной простоте и способности устойчиво регулировать многие технологические процессы.

В астатических, или интегральных, регуляторах (сокращенно И-регуляторах) величина регулирующего воздействия пропорциональна интегралу отклонения входной величины:

$$\mu = \varepsilon_p \int \sigma dt, \quad (1)$$

где  $\varepsilon_p$  - коэффициент, характеризующий величину перемещения регулирующего органа при отклонении регулируемого параметра на единицу измерения.

Изодромные, или пропорционально-интегральные, регуляторы (сокращенно ПИ-регуляторы) объединяют в себе положительные свойства пропорциональных и интегральных регуляторов. Как следует из сказанного выше, наличие отрицательной обратной связи благотворно влияет на переходный процесс регулирования, но приводит к остаточному отклонению. В пропорционально-интегральных регуляторах применяется особая обратная связь - упругая, действие которой постепенно исчезает после осуществления пропорционального воздействия. Благодаря этому возникают дополнительные перемещения регулирующего органа, ликвидирующие статическую ошибку.

Дифференциальное уравнение ПИ-регулятора имеет, соответственно, два члена, характеризующие действие пропорциональной и интегральной частей:

$$\mu = k_p \left( \sigma + \frac{1}{T_{II}} \int \sigma dt \right). \quad (2)$$

Постоянная времени  $T_{II}$ , называемая временем изодрома, определяет долю участия астатической составляющей в законе регулирования.

При постоянном значении  $\sigma$  (однократное ступенчатое отклонение регулируемого параметра) выражение (2) принимает вид:

$$\mu = k_p \sigma \left( 1 + \frac{1}{T_{II}} \int dt \right). \quad (3)$$

Заметное улучшение переходного процесса при статическом регулировании можно получить, введя в систему пропорционального регулятора сигнал по производной регулируемого параметра. Такие устройства называются пропорционально-дифференциальными регуляторами (ПД-регуляторами). Уравнение ПД-регулятора:

$$\mu = k_p (\sigma + T_{IP} \sigma'). \quad (4)$$

Изодромные регуляторы с воздействием по производной отклонения параметра регулирования называются пропорционально-интегрально-дифференциальными регуляторами (ПИД-регуляторами).

Дифференциальное уравнение ПИД-регулятора имеет вид:

$$\mu = k_p \sigma \left( 1 + \frac{1}{T_{II}} \int dt + T_{IP} \sigma' \right). \quad (5)$$

---

Коэффициент  $T_{\text{ПР}}$ , называемый временем предварения, характеризует степень участия дифференциальной составляющей в регулирующем воздействии.

Наиболее часто используется ПИД-регулятор, поскольку он сочетает в себе достоинства всех трех типовых регуляторов. Однако даже ПИД-регуляторы, на практике, не являются оптимальными и поэтому не позволяют достичь управляемой системе потенциальных характеристик. Основа постановки экстремальных задач – математическая модель динамики материальной системы.

Использование идей принципа максимума Л.С. Понтрягина и принципа Гамильтона-Остроградского для построения расширенного функционала позволяет получить необходимые и достаточные условия минимума в форме объединенного принципа максимума (ОПМ) и построить управление отличающиеся высокой эффективностью [2].

### Постановка задачи.

Рассматривается задача стабилизации палубной параболической антенны в заданном положении. Принято, что стабилизация и позиционирование антенны осуществляется с использованием электрического привода (рисунок 1).

Электропривод (ЭП) участвует в определении такого важного технического параметра РЛС, как азимут цели, скорость обзора, точность определения координат цели. От его безотказной и качественной работы зависит эффективность работы всей РЛС.

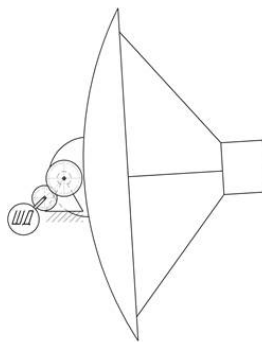


Рисунок 1. Оценки дальности и действительная дальность

В связи с этим ЭП вращения антенны должен обеспечивать [3]:

- вращение и наведения антенны с высокой точностью и быстродействием;
- работу при больших динамических перегрузках, вызванных большой величиной инерционных масс (размах антенн достигает 40 м), а также действием ветра, который может вызвать ее механические повреждения, в связи с чем требуется обеспечить плавность переходных процессов;
- вращение с различными по величине скоростями для различной скорости ветра, сканирование в секторе, установка на азимут, наведение на цель и ее сопровождение;
- высокие энергетические показатели, т.к. РЛС является автономным объектом с источником энергии ограниченной мощности;
- высокие массогабаритные показатели в связи с необходимостью создания малогабаритных и мобильных РЛС;
- повышенную надежность ввиду работы РЛС в тяжелых климатических условиях, в том числе в составе сухопутных и морских комплексов спецтехники.

На практике используются различные электрические двигатели. В работе рассматривается электрический двигатель постоянного тока. При их исследовании часто пренебрегают малыми постоянными времени электрических процессов двигателя в

сравнении с постоянной времени механической части привода. Математическая модель представлена уравнением [4]

$$\ddot{q} = u = kU, \quad (6)$$

где  $q$  имеет размерность угла вращения привода;

$u = kU$  – момент, развиваемый двигателем;

$k$  – коэффициент пропорциональности;

$U$  – управляющее воздействие на исполнительный механизм.

Уравнение (1) является следствием принципа Гамильтона – Остроградского в соответствии с которым интеграл действия по Гамильтону [3] на истинном пути достигает минимума. В математическом плане задача стабилизации палубной параболической антенны в заданном положении требует решения задачи синтеза оптимального управления из условия минимума целевого функционала [5]:

$$J = \frac{1}{2} \int_{t_0}^{t_1} (q - q_{уст})^2 dt \rightarrow \min, \quad (7)$$

где  $(q - q_{уст})$  – разница между текущим  $q$  и установленным (заданным)  $q_{уст}$  значениями.

Учет ограничений требует использования метода множителей Лагранжа, что позволяет сконструировать расширенный целевой функционал следующего вида:

$$J_1 = J + \lambda_1 R \rightarrow \min. \quad (8)$$

Необходимо отметить, что технические средства, которыми до последнего времени располагала электротехника, не позволяли получить экономически оправданное решение этой задачи с использованием ЭП переменного тока. Лишь с освоением серийного производства мощных полупроводниковых приборов – тиристоров в последнем десятилетии появилась практическая возможность решения указанной задачи – создания электропривода переменного тока, обладающего не только широким диапазоном регулирования частоты вращения ротора, но и нужными моментными характеристиками, не уступающими характеристикам ЭП постоянного тока.

#### **Условие максимума функции обобщенной мощности.**

Решение поставленной задачи в общем виде получают на основе использования следующей теоремы: для того чтобы обобщенная сила  $\mathbf{Q}(\mathbf{q}, \dot{\mathbf{q}}, \mathbf{u}, t) \in \bar{G}_Q$  и соответствующая ей траектория  $(\mathbf{q}, \dot{\mathbf{q}}) \in R^{2n}$  доставляли минимум расширенному функционалу (6), необходимо выполнить условия максимума для обобщенной мощности [6]:

$$\Phi(q, \dot{q}, u, \lambda) = \max_{\mathbf{Q} \in \bar{G}_Q} \sum_{s=1}^n [\lambda u + (q - q_{уст})] \dot{q}_s, \quad (9)$$

при этом  $\lambda = const > 0$ , а на концах траектории  $t = t_0$ ,  $t = t_k$  выполняются условия трансверсальности для функции Гамильтона-Остроградского  $H(\mathbf{q}, \mathbf{p}, t)$  и обобщенного кинетического потенциала  $L(\mathbf{q}, \dot{\mathbf{q}}, t)$ .

$$H = \lambda(T + A) + \sum_{s=1}^n (q - q_{ycm})^2 = 0; \quad (10)$$

$$L = \lambda(T - A) + \sum_{s=1}^n (q - q_{ycm})^2 = 0. \quad (11)$$

Из теоремы следует, что

$$u = \lambda^{-1} [\mu(q, \dot{q})\dot{q} + (q - q_{ycm})], \quad (12)$$

где  $\mu(q, \dot{q})$  синтезирующая функция.

Для построения функции  $\mu_s$  используются следующие положения:

- уравнение

$$\mu(q, \dot{q})\dot{q} + (q - q_{ycm}) = 0 \quad (13)$$

описывает линию переключения управления. Эта линия проходит через терминальную точку фазового пространства и на ней управление меняет знак:

$$\bar{u}(t') = \begin{cases} \bar{u}(\tau - 0), & t' < \tau, \\ 0, & t' = \tau, \\ \bar{u}(\tau + 0), & t' > \tau, \end{cases} \quad (14)$$

- функция  $\mu$  - знакопостоянная, что вытекает из способа максимизации функции  $\Phi$ , а именно

$$\max_{Q \in G_Q} \Phi = [\lambda u + (q - q_{ycm})]\dot{q}, \quad (15)$$

откуда необходимым условием максимума является не совпадение знаков множителей и их пропорциональность

$$\begin{aligned} \text{sign}[\lambda u + (q - q_{ycm})] &= -\text{sign}\dot{q}, \\ [\lambda u + (q - q_{ycm})] &= \mu\dot{q}, \end{aligned} \quad (16)$$

что и определяет необходимость знакопостоянства функции  $\mu$ ;

- условия совместности на линии переключения:

1 для траекторий, приходящих на линию переключения любой интеграл движения и уравнение линии переключения в точке стыка определяются одними и теми же значениями фазовых координат;

2 на линии переключения выполняются условия трансверсальности, что возможно, так как всякая часть траектории является оптимальной траекторией:

$$[\lambda(A - T) + F] = 0. \quad (17)$$

Таким образом, эти условия позволяют определять функцию  $\mu$  через интегралы движения, или через кинематические характеристики фазовой траектории точки.

Для построения синтезирующей функции предложены методы интегральных связей, фазовых траекторий и пространства, аналитического построения формы линии переключения. Проведенный анализ литературы показал, что в данном рассматриваемом случае, когда необходимо учитывать свойства динамической системы целесообразно использовать метод выбранных траекторий [1]. Тогда

$$\mu = -\lambda \frac{|\dot{q}|a}{|q|b}, \quad (18)$$

где  $a, b$  - константы.

### Синтез уравнений обратных связей.

Возможны следующие варианты построения комбинированного управления.

Первый вариант. Управление выбирается из класса ограниченных измеримых функций. Уравнение, определяющее линию переключения управления

$$\lambda u + \frac{\partial F}{\partial q} = 0. \quad (19)$$

На этой линии Гамильтониан постоянен

$$H_0 = \lambda(T + A) + F = \text{const}, \quad (20)$$

откуда закон комбинированного управления по отклонению и возмущению имеет вид

$$Q = \lambda^{-1} \left[ -\lambda \frac{|\dot{q}|a}{|q|b} - (q - q_{\text{уст}}) \right]. \quad (21)$$

Второй вариант. Управление выбирается из класса ограниченных функций

$$Q = \lambda^{-1} \text{sign} \left[ -\lambda \frac{|\dot{q}|a}{|q|b} - (q - q_{\text{уст}}) \right]. \quad (22)$$

Результаты математического моделирования приведены на рисунке 2.

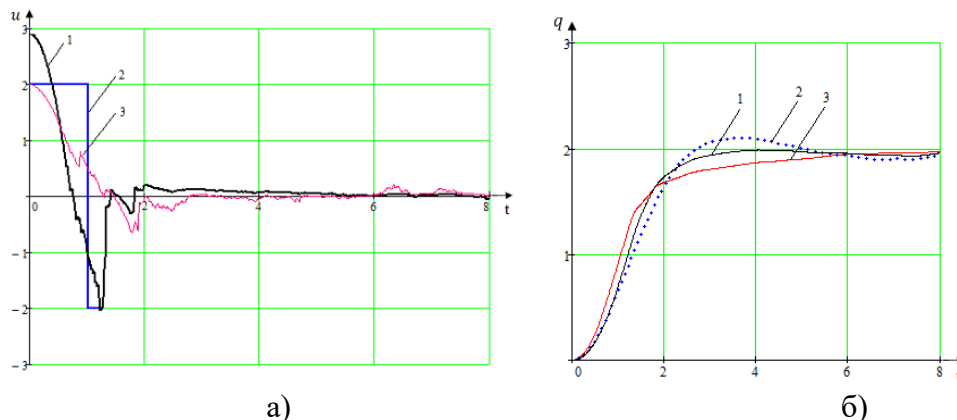


Рисунок 2. а) Управляющие воздействия ИУС б) Переходной процесс

---

На рисунке 2 цифрами обозначено: 1 – управление (21); 2 – управление (22); 3 – комбинированное управление.

### **Заключение.**

Наибольшей эффективностью отличается комбинированное управление. Однако его использование связано с большими вычислительными затратами. Типовые решения предусматривают возможность реализации релейных управлений.

Работа подготовлена в рамках научной темы «Разработка беспилотных технологий на основе комплексной поэтапной оптимизации с редукцией экстремальных задач и инструментов нейро-нечеткого моделирования (FZNE-2022-0006)».

### **СПИСОК ЛИТЕРАТУРЫ**

1. Студер Ф., Фарина А. Цифровая обработка радиолокационной информации. М.: Радио и связь. 1993. 319 с.
2. Тихонов В.И., Харисов В.Н. Статистический анализ и синтез радиотехнических устройств и систем. Уч. пос. для высших уч. заведений. М.: Радио и связь, 1991. 238 с.
3. Лурье А.И. Аналитическая механика М.: Государственное издательство физико-математической литературы, 1961. 824 с.
4. Андрашитов Д.С., Костоготов А.А., Лазаренко С.В. Многопараметрическая вариационная идентификация динамических систем на основе объединенного принципа максимума // Информационно – управляющие системы. 2012. №4 (10). С. 68 – 76.
5. Костоготов А.А., Костоготов А.И., Лазаренко С.В. Объединенный принцип максимума в задачах оценки параметров движения маневрирующего летательного аппарата // Радиотехника и электроника. 2009. №4 (54). С. 450 – 457

**Э.З. Кожяев, П.Э. Ухов**

### **ДИСТАНЦИОННОЕ ЗОНДИРОВАНИЕ ЗЕМЛИ. АНАЛИЗ СПОСОБОВ ПОЛУЧЕНИЯ ИНФОРМАЦИОННЫХ МАТЕРИАЛОВ**

Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Ростов-на-Дону, Россия.

Ключевые слова: дистанционное зондирование, радиоволны, космическая съемка, окна прозрачности, спектральный диапазон.

В статье рассмотрены способы получения информационных материалов при помощи спутников дистанционного зондирования.

**E.Z. Kozhaev, P.E. Ukhov**

### **REMOTE SENSING OF THE EARTH. ANALYSIS OF WAYS TO OBTAIN INFORMATION MATERIALS**

Federal State Autonomous Educational Institution of Higher Education "Southern Federal University", Rostov-on-Don, Russia.

---

Keywords: remote sensing, radio waves, satellite imagery, transparency windows, spectral range.

The article discusses the methods of obtaining information materials using remote sensing satellites.

### **Введение.**

Дистанционное зондирование Земли (ДЗЗ) – это метод наблюдения поверхности Земли с помощью космических и авиационных средств, оснащенных различной съемочной аппаратурой. Этот метод позволяет изучать природные ресурсы Земли и решать задачи метеорологии.

Дистанционное зондирование можно разделить на активное и пассивное. В активном дистанционном зондировании сигнал сначала излучается космическим аппаратом, а затем регистрируется отраженный или рассеянный сигнал. В пассивном дистанционном зондировании регистрируются только сигналы других источников, например, отраженный солнечный свет.

Пассивные сенсоры дистанционного зондирования регистрируют сигналы, излучаемые или отраженные объектами или окружающей территорией. Отраженный солнечный свет является наиболее часто используемым источником излучения, регистрируемым пассивными сенсорами. Примеры пассивного дистанционного зондирования включают цифровую и пленочную фотографию, инфракрасные приборы, приборы с зарядовой связью и радиометры.

Активные приборы дистанционного зондирования излучают сигналы для сканирования объектов и пространства, а затем сенсоры регистрируют отраженное или рассеянное излучение, что позволяет определить расположение, скорость и направление движения объекта. Примерами активных сенсоров дистанционного зондирования являются радар и лидар, которые измеряют задержку между излучением и регистрацией возвращенного сигнала.

Космические аппараты, используемые для изучения природных ресурсов, часто оснащены оптической или радиолокационной аппаратурой. Радиолокационная аппаратура имеет преимущество, так как позволяет наблюдать поверхность Земли в любое время суток и независимо от состояния атмосферы.

Дистанционное зондирование позволяет получать данные о различных объектах и явлениях без прямого физического контакта с ними. Современные технологии воздушного или космического зондирования местности используют распространяемые сигналы, такие как электромагнитная радиация, для обнаружения, классификации и анализа объектов земной поверхности, атмосферы и океана.

Применение дистанционного зондирования включает мониторинг вырубки лесов, состояния ледников в Арктике и Антарктике, а также измерение глубины океана с помощью лота. Этот метод позволяет получать данные о опасных, труднодоступных и быстро движущихся объектах, а также проводить наблюдения на больших территориях. Вместо дорогостоящих и медленных методов сбора информации с поверхности Земли, дистанционное зондирование обеспечивает невмешательство человека в природные процессы на наблюдаемых территориях или объектах.

Орбитальные космические аппараты собирают и передают данные в различных диапазонах электромагнитного спектра. В сочетании с воздушными и наземными измерениями и анализом эти данные обеспечивают необходимую информацию для мониторинга природных явлений как в краткосрочной, так и в долгосрочной перспективе.

Целью данной работы является анализ способов получения информационных материалов с поверхности Земли с использованием спутников дистанционного зондирования. Для достижения этой цели необходимо проанализировать существующие методы получения материалов дистанционного зондирования и выявить их особенности.



## Методы получения информации дистанционного зондирования.

Дистанционное зондирование осуществляется с использованием различных окон прозрачности атмосферы, Окна прозрачности атмосферы – это участки электромагнитного спектра, в которых атмосфера наиболее прозрачна для прохождения энергии. (Рисунок 1), дистанционное зондирование широко применяется: – световом (видимом, ближнем и среднем инфракрасном), тепловом инфракрасном и радиодиапазоне.

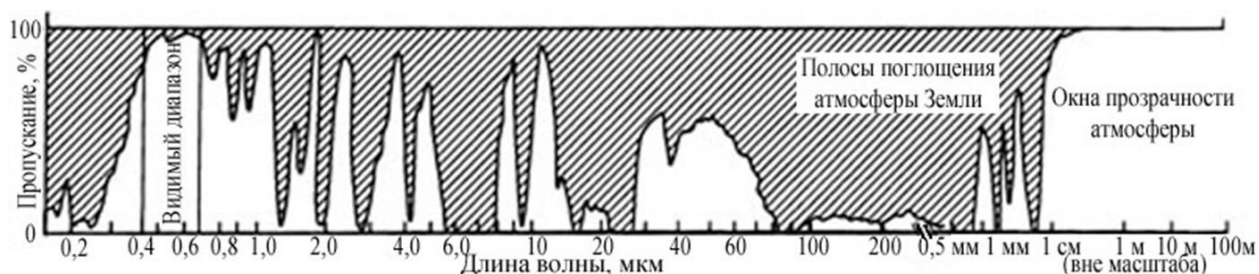


Рисунок 1. Окна прозрачности атмосферы

В зависимости от диапазона, используются различные технологии и методы обработки для формирования изображений. (Рисунок 2).

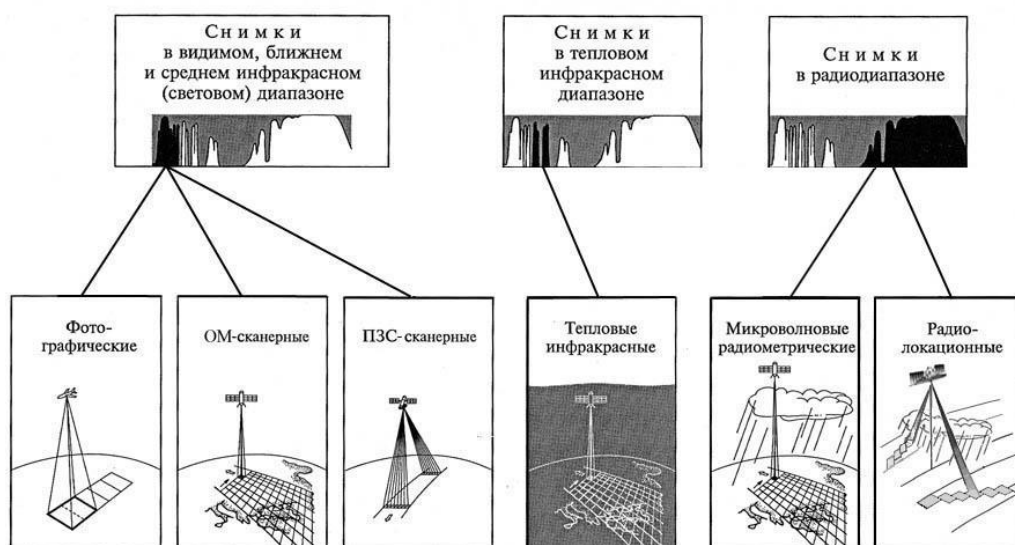


Рисунок 2. Классификация космических снимков по спектральным диапазонам и технологиям получения изображения

Фотографии в световом диапазоне дистанционного зондирования земли относятся к изображениям, полученным с помощью спутников, самолетов или дронов, которые используют электромагнитное излучение в видимом световом диапазоне. Дистанционное зондирование земли (ДЗЗ) является методом сбора информации о поверхности Земли без прямого контакта с ней.

В процессе ДЗЗ, сенсоры на борту спутников или других аппаратов регистрируют отраженное от поверхности Земли световое излучение. Это излучение затем преобразуется в цифровое изображение, которое может быть использовано для анализа и извлечения информации о различных объектах на земной поверхности. Фотографии, полученные в световом диапазоне ДЗЗ, могут быть использованы в различных областях, таких как картография, геология, сельское хозяйство, экология и многое другое.

Эти фотографии предоставляют ценную информацию о сезонных изменениях растительности, состоянии почвы, использовании земли, изменениях климата и других

---

параметрах, которые могут быть использованы для принятия решений и мониторинга нашей планеты.

Снимки в тепловом инфракрасном диапазоне, получаемые при зондировании Земли, предоставляют информацию о тепловых характеристиках поверхности и атмосферы. В этом диапазоне используется инфракрасное излучение, которое объекты испускают в зависимости от их температуры.

Съемка в радиодиапазоне при зондировании земли может быть выполнена с использованием радиолокационных методов. Радиолокационные снимки получаются путем регистрации отраженного радиоизлучения, которое посылается с носителя. Этот метод позволяет получить информацию о различных аспектах поверхности Земли, таких как рельеф, типы почвы, наличие водных объектов и другие характеристики. Радиолокационные снимки могут быть особенно полезны в условиях ограниченной видимости, таких как облачность или ночное время, когда оптические методы съемки могут быть затруднены. Эти снимки могут быть использованы для различных приложений, включая обнаружение изменений на земной поверхности, картографирование и мониторинг окружающей среды.

### **Радиолокационная съемка.**

Радиолокационная съемка дистанционного зондирования или радарное зондирование – это метод получения информации о поверхности Земли, используя радиоволны. В радарной съемке, радиосигналы излучаются на поверхность Земли, а затем отражаются и регистрируются радарным приемником. Анализ этих отраженных сигналов позволяет получить информацию о различных характеристиках поверхности, таких как рельеф, тип почвы, влажность, растительность, а также обнаружить объекты на поверхности.

Качество радиолокационного снимка зависит от длины волны радиосигнала и размера апертуры антенны. Чем меньше длина волны и больше размер апертуры, тем выше разрешение и, следовательно, лучшее качество снимка. Качество снимка также зависит от точности геометрической регистрации, то есть от соответствия между местоположением объектов на снимке и их реальными координатами на земле. Неточности в геометрической регистрации могут привести к искажениям и неточностям в изображении.

Также на качество снимков сильно влияет выбор частоты радиосигнала. Частота прямо пропорционально влияет на проникновение сигнала через различные типы поверхностей. Низкие частоты имеют лучшую проникающую способность, но могут иметь более низкое разрешение, в то время как высокие частоты обладают лучшим разрешением, но меньшей способностью проникновения.

Так низкие частоты ниже 1 ГГц способны проникать в воду и почву на глубину от нескольких сотен метров до нескольких километров, но с низким разрешением. Высокие (10-100 ГГц) и средние частоты (1-10 ГГц) имеют низкую проникающую способность, но имеют достаточно высокое разрешение.

Важной характеристикой радиолокационной съемки является угол обзора радара. Он определяет ширину и площадь поверхности, которую он может охватить за один раз. Чем больше угол обзора, тем больше информации можно получить на снимке. Однако, при большом угле обзора может снижаться разрешение и детализация снимка.

Дополнительно к сказанному существует еще один метод получения информации который использует радиосигналы называемый радиолокационной интерферометрией.

Радиолокационная интерферометрия – это метод, который используется для получения информации о удаленных объектах или поверхностях, путем анализа интерференции радиоволн. Он основан на принципе интерференции, когда две или более волны сливаются вместе и создают интерференционные полосы, которые могут быть использованы для извлечения полезной информации. Радиолокационная интерферометрия используют зачастую микроволновый диапазон от (1 до 300 ГГц), для измерения фазовых

---

изменений возвращенного отраженного сигнала. Путем анализа разности фаз между различными приемниками или повторными излучателями, можно получить информацию о форме, движении и других характеристиках объекта или поверхности.

### **Тепловые съемки.**

Тепловая съемка дистанционного зондирования (термальное зондирование) – это метод получения информации путем анализа распределения тепловой энергии на поверхности Земли с помощью специальных инфракрасных камер, установленных на борту искусственных спутников. Данным методом возможно измерение температуры объектов и расчёт тепловых потоков в различных районах планеты. Тепловая съемка имеет широкий спектр применения, она используется для мониторинга климата и окружающей среды, исследования поверхности океана, анализа распределения теплового излучения в городах, обнаружения пожаров, изучения вулканической активности и других геологических явлений.

Информация, полученная с помощью тепловой съемки дистанционного зондирования, может быть использована для прогнозирования погоды, определения изменений климата, контроля за состоянием сельскохозяйственных угодий, обнаружения утечек нефти и газа, а также для многих других приложений.

Аппаратура, используемая для тепловой съемки – это тепловизоры для дистанционного зондирования которые состоят из оптической системы, детектора инфракрасного излучения, электроники обработки сигналов и дисплея для визуализации изображений. Оптическая система фокусирует инфракрасное излучение на детектор, который преобразует его в электрический сигнал. Затем электроника обрабатывает этот сигнал и создает тепловое изображение, которое отображается на дисплее.

### **Космическая съемка.**

Космическая съемка (КС) – это процесс фотографирования земной поверхности с использованием специальных космических фотоаппаратов, которые находятся на спутниках или космических аппаратах. Эта технология позволяет получать изображения Земли со значительной высоты, что дает обзорную перспективу и охватывает большие территории.

В КС используются различные типы оборудования, включая фотоаппараты, мультиспектральные сканеры и радары. Видимый спектр электромагнитного излучения и инфракрасный диапазон являются наиболее распространенными для фотографирования.

Масштабы съемки определяются высотой полета снимающего аппарата и фокусным расстоянием объектива. Чем выше полет и меньше фокусное расстояние, тем более широкую территорию можно охватить на снимке.

Современная фотоаппаратура, используемая в КС, обладает высоким разрешением, что позволяет получать изображения с большой детализацией и мелкими деталями. Космические фотоаппараты создают плановые и перспективные изображения земной поверхности с различными углами наклона оптической оси.

Для космической съемки применяются различные фотографические системы, например, КАТЭ-140, МКФ-6, ФМС и ДР. Они имеют спектральные каналы, работающие в разных областях спектра, и могут фотографировать в различных спектральных диапазонах. Это позволяет получить информацию о разных свойствах объектов на Земле, таких как растительность, водные ресурсы, почва и т. д.

Высокое разрешение снимков космической съемки позволяет увеличивать изображения без значительной потери информации. Зональные снимки, полученные в различных спектральных каналах, могут быть увеличены до определенного масштаба и использованы для геологической интерпретации и анализа.

### **Сканерная съемка.**

Сканерная съемка – это метод фотографирования земной поверхности с использованием оптико-механических сканеров, установленных на космических аппаратах, таких как спутники. Сканеры формируют изображения путем последовательного сканирования местности и регистрации светового сигнала.

Процесс сканерной съемки включает использование сканирующего элемента, такого как качающееся или вращающееся зеркало, которое перемещается поперек движения космического аппарата. Этот элемент направляет лучистый поток света через объектив на точечный датчик, который преобразует световой сигнал в электрический. Электрический сигнал передается на приемные станции по каналам связи.

Изображение местности получается в виде непрерывной ленты, состоящей из полос-сканов, где каждый скан представляет собой отдельный элемент изображения, известный как пиксель. Сканерные системы обеспечивают возможность получения изображений в различных спектральных диапазонах, но особенно эффективными являются видимый и инфракрасный диапазоны.

Сканерное изображение представляет собой упорядоченный набор яркостных данных, которые передаются по радиоканалам на Землю и могут быть записаны на магнитную ленту в цифровом формате. Эти данные могут быть преобразованы в кадровую форму для удобства анализа и интерпретации.

В геологии и других науках широко используются материалы сканерной съемки, полученные с помощью спутников серии "Метеор". На этих спутниках установлены различные типы сканирующих устройств, такие как МСУ-М (малое разрешение), МСУ-С (среднее разрешение), МСУ-СК (коническая развертка) и МСУ-Э (электронная развертка).

Сканерная съемка позволяет получать высококачественные и детализированные изображения земной поверхности, которые используются для мониторинга изменений климата, изучения геологических структур, анализа растительности, оценки использования земель и многих других приложений в научных, географических и окружающих нас областях.

Таким образом, в работе были рассмотрены особенности дистанционного зондирования Земли и технологии, с помощью которых оно осуществляется. Дистанционное зондирование Земли является мощным инструментом для изучения поверхности Земли и решения различных научных и практических задач. Оно позволяет получать информацию о природных ресурсах, метеорологических явлениях и состоянии окружающей среды. Различные способы получения материалов дистанционного зондирования обеспечивают широкий спектр данных, необходимых для мониторинга и анализа нашей планеты.

### **СПИСОК ЛИТЕРАТУРЫ**

1. Михайлов С.И. Применение данных дистанционного зондирования Земли для решения задач в области сельскохозяйственного производства // Земля из космоса. 2011. – Выпуск 9. – С. 17-23.
2. Белый Р.В., Харланов А.С., Харламов М.М. и др. Инновационное развитие и космос: военные аспекты стратегии и экономики. // Монография – Москва: РУСАЙНС, 2020 г. – 88 с.
3. Роскосмос [Электрон. ресурс] - Режим доступа: URL:<https://www.roscosmos.ru/24707/>, (дата обращения: 02.10.2023).
4. Российские космические системы [Электрон. ресурс] - Режим доступа: URL:<http://russianspacesystems.ru/bussines/dzz/>, (дата обращения: 28.09.2023).
5. Terrestrial Heat Flux Measuring and Geothermal Zoning for Regional and Petroleum Geology on the Base of Satellite IR-Thermal Survey / V. I. Gorny, S. G. Kritzuk, I. Sh.

---

Latypov, A. A. Tronin // Proc. of the Eleventh Thematic and Conference Geologic Remote Sensing, Vol. 1 1996, Las Vegas Nevada, USA.

6. Обиралов А.И., Лимонов А.Н., Гаврилова Л.А. Фотограмметрия и дистанционное зондирование. – М.: Колосс, 2006. – 334 с.

---

**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ  
И СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**

**INFORMATION TECHNOLOGIES  
AND ARTIFICIAL INTELLIGENCE SYSTEMS**

**Т.Д. Фатхулин, М.С. Кожанов**

**ПРОБЛЕМЫ ХРАНЕНИЯ И УПРАВЛЕНИЯ РЕЗУЛЬТАТАМИ СТАТИЧЕСКОГО  
АНАЛИЗА В ЖИЗНЕННОМ ЦИКЛЕ РАЗРАБОТКИ БЕЗОПАСНОГО ПО И ПУТИ  
ИХ РЕШЕНИЯ**

Ордена Трудового Красного Знамени федеральное государственное Бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», Москва, Россия

Ключевые слова: статический анализ, SAST, уязвимости, безопасность, хранение, надежность, жизненный цикл, разработка, управление, данные, искусственный интеллект.

В статье рассматриваются проблемы, возникающие при хранении и управлении результатами статического анализа в жизненном цикле разработки безопасного ПО. Оценивается важность рассматриваемого процесса, выявляются связанные с ним проблемы и риски, а также предлагаются методы и технологии для их решения. Приводятся возможности применения искусственного интеллекта и машинного обучения в данном контексте.

**T.D. Fatkhulin, M.S. Kozhanov**

**PROBLEMS OF STORING AND MANAGING THE RESULTS OF STATIC ANALYSIS  
IN THE LIFE CYCLE OF SECURE SOFTWARE DEVELOPMENT AND WAYS TO  
SOLVE THEM**

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: static analysis, SAST, vulnerabilities, security, storage, reliability, life cycle, development, management, data, artificial intelligence.

The article discusses the problems that arise when storing and managing the results of static analysis in the security software development life cycle. The importance of the process under consideration is assessed, problems and risks associated with it are identified, and methods and technologies for solving them are proposed. The possibilities of using artificial intelligence and machine learning in this context are presented.

**Введение.**

Статический анализ SAST (Static Application Security Testing) является важным инструментом в области разработки программного обеспечения (ПО), особенно в контексте обеспечения безопасности. Он представляет собой процесс анализа исходного кода или бинарных файлов без их фактического выполнения. Важной особенностью SAST является его способность обнаруживать потенциальные ошибки, уязвимости и недочеты в коде на ранних этапах разработки, когда они более легко и дешево исправляются [1].

---

Целью работы является исследование проблем хранения и управления результатами SAST в жизненном цикле разработки безопасного ПО, а также поиск путей их решения. Для достижения поставленной цели необходимо решить целый ряд представленных ниже взаимосвязанных задач:

- изучить аспекты SAST;
- оценить важность хранения и управления результатами SAST в процессе разработки ПО;
- выявить проблемы, связанные с хранением результатов SAST;
- проанализировать опасности и риски, связанные с недостаточным управлением данными SAST;
- оценить методы решения проблем, связанных с хранением результатов SAST;
- исследовать примеры использования технологий и инструментов для автоматизации управления результатами SAST;
- представить практические примеры использования рассматриваемых систем.

Настоящая работа базируется на таких методах исследования, как теоретический анализ, систематизация и обобщение, а также сравнительный анализ.

### **Аспекты SAST.**

При SAST в контексте безопасности ПО обеспечения выделяют следующие важные аспекты.

- *Обнаружение уязвимостей и ошибок на ранних этапах.* SAST позволяет выявлять потенциально опасные конструкции и паттерны в коде до его компиляции или выполнения. Это позволяет разработчикам исправить уязвимости на более ранних стадиях разработки, что существенно снижает затраты на их устранение и риск их эксплуатации в будущем.
- *Поиск ошибок безопасности.* Множество уязвимостей, таких как инъекции SQL, переполнение буфера, утечки информации и другие, могут быть обнаружены с помощью SAST. Это способствует созданию более надежного и безопасного ПО, которое менее подвержено атакам.
- *Соблюдение стандартов и правил безопасности.* SAST также позволяет контролировать соблюдение стандартов кодирования и правил безопасности в проекте. Разработчики могут настраивать анализаторы кода так, чтобы они проверяли код на соответствие установленным стандартам и рекомендациям.
- *Улучшение процесса обучения и квалификации разработчиков.* SAST способен выявлять уязвимости, которые могут быть связаны с недостаточным пониманием безопасности со стороны разработчиков. Это может помочь обучать команду разработчиков и повышать их уровень компетенций в области безопасности.
- *Интеграция в жизненный цикл разработки.* SAST может быть интегрирован в процесс непрерывной интеграции и доставки (CI/CD), что позволяет автоматически проводить анализ при каждом коммите кода и предупреждать разработчиков о проблемах немедленно.

Все указанные аспекты сделали SAST неотъемлемой частью разработки безопасного ПО. Он помогает выявлять и устранять проблемы безопасности на ранних этапах, что значительно повышает качество и надежность конечного продукта.

### **Значение хранения и управления результатами SAST в процессе разработки.**

Важным фактором успешного использования SAST в разработке безопасного ПО является хранение и управление результатами анализа. Неправильное или недостаточное управление этими результатами может привести к ряду серьезных проблем.

- *Потеря данных.* Результаты SAST содержат важную информацию о потенциальных уязвимостях и ошибках в коде. Неправильное управление

---

результатами может привести к их потере, что увеличит риск упущенных уязвимостей.

- *Неудачное сопровождение.* Поскольку код часто изменяется, результаты SAST должны регулярно обновляться и перепроверяться после внесения изменений, чтобы избежать упущенных уязвимостей.
- *Потеря контекста.* Контекст и история результатов SAST важны для понимания, какие уязвимости были найдены и исправлены. Надежное управление результатами помогает отслеживать историю анализов и изменений в коде.
- *Большие объемы данных.* Большие проекты могут генерировать огромные объемы данных результатов SAST. Эффективные инструменты и системы управления помогают хранить, передавать и анализировать эти данные.
- *Безопасность данных.* Результаты SAST могут содержать чувствительную информацию о уязвимостях. Необходимо обеспечить безопасное хранение этих данных, чтобы избежать утечек или эксплуатации уязвимостей.
- *Отсутствие надежности.* Ненадежное управление результатами SAST может привести к их игнорированию разработчиками, что уменьшит эффективность процесса анализа.

Проблемы, описанные выше, подчеркивают важность использования специализированных инструментов и систем для правильного управления результатами SAST в процессе разработки, обеспечивая высокий уровень безопасности и качества ПО.

### **Проблемы хранения результатов SAST**

Проблемы, связанные с хранением и управлением данными, создаваемыми статическим анализом программного кода (SAST), могут включать:

- *Объем данных в больших проектах.* Большие проекты могут порождать огромное количество отчетов об ошибках и уязвимостях после SAST-анализа. Например, web-приложение может создать сотни или даже тысячи отчетов о потенциальных угрозах безопасности.
- *Разнообразие данных.* Результаты SAST могут включать в себя разнообразные типы данных, такие как списки уязвимостей, предупреждения о потенциальных проблемах, информацию о кодовых метриках и структуры данных. Все эти данные требуют удобной организации и хранения.
- *История результатов.* Для обеспечения надежности, результаты анализа должны сохраняться с их историческим контекстом. Это позволяет отслеживать изменения в результате анализа со временем.
- *Возможность повторного анализа.* Важно иметь возможность повторно проанализировать код при необходимости. Это может потребовать хранения больших объемов промежуточных данных и метаданных для воспроизводимости результатов.
- *Интеграция с CI/CD (continuous integration / continuous delivery).* Результаты SAST должны быть доступными для автоматической проверки при каждом обновлении кода в средах непрерывной интеграции и доставки (CI/CD). Это требует быстрого доступа к данным и интеграции с системами CI/CD.
- *Динамическое обновление.* Разработка может быть динамичной, и код может изменяться часто. Поэтому система хранения и управления данными должна поддерживать обновление результатов анализа по мере необходимости и отслеживать соответствующие изменения.

Эти проблемы подчеркивают необходимость специализированных инструментов и систем для эффективного управления и хранения данными, создаваемыми SAST, в целях обеспечения безопасности и эффективности разработки программного обеспечения.



Существует несколько методов и инструментов для хранения и управления результатами SAST.

- *Базы данных.* Системы управления базами данных (СУБД), такие как PostgreSQL и MySQL, могут использоваться для структурированного хранения результатов анализа. Однако для малых команд или проектов установка, настройка и управление такими СУБД может быть сложной и затратной задачей. Кроме того, при работе с большими объемами данных могут возникнуть ограничения производительности, что может затруднить быстрый доступ к информации. На рисунке 1 представлены наиболее популярные СУБД для хранения и управления результатами SAST [4].

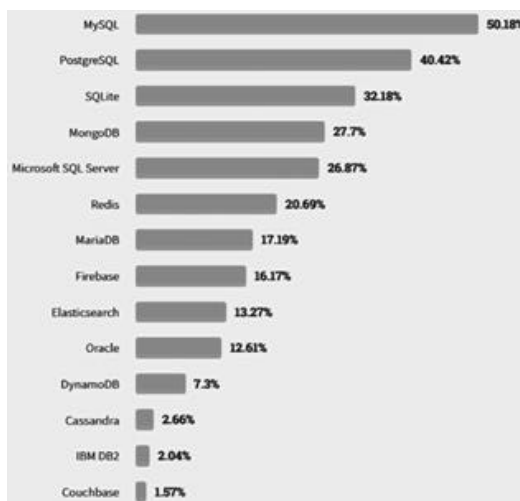


Рисунок 1. Наиболее популярные СУБД для решения поставленных задач

- *Инструменты управления ошибками.* Инструменты управления ошибками, такие как ClickUp, JIRA и Redmine, иногда используются для хранения результатов анализа в форме задач или баг-репортов. Однако такие инструменты могут оказаться ограниченными в функциональности для эффективного управления данными SAST. Они часто не обладают специализированными функциями, необходимыми для обработки результатов анализа, такими как фильтрация или интеграция с инструментами анализа. На рисунке 2 изображены одни из самых востребованных инструментов управления ошибками по версии ресурса «clickup.com» [5].

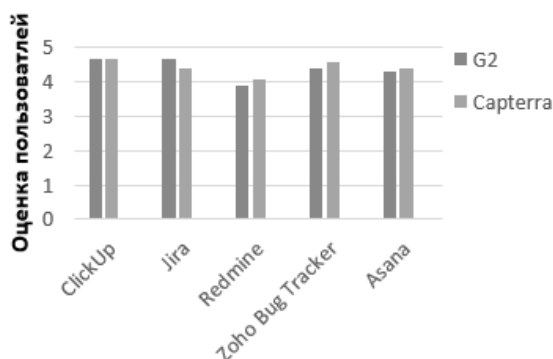


Рисунок 2. Рейтинг инструментов управления ошибками [5]

- *Системы управления версиями.* Системы управления версиями, такие как Git или SVN, могут использоваться для хранения и отслеживания результатов анализа вместе с кодом. Однако они не специализированы для управления

данными SAST и часто не предоставляют удобных инструментов для организации и анализа таких данных.

- *Специализированные системы управления результатами SAST.* Существуют специализированные инструменты и системы для управления результатами SAST, такие как SonarQube, Fortify, Coverity и Checkmarx. Однако некоторые из них могут быть дорогостоящими в плане лицензий и обслуживания, что может вызвать затруднения для небольших компаний или проектов с ограниченным бюджетом. Также настройка и интеграция таких систем могут потребовать значительных временных и финансовых затрат. Тройка лучших альтернатив инструменту Fortify по версии ресурса «G2 Community» [6]: Первое место занимает SonarQube, за ним следует Coverity, а тройку лидеров завершает G2 Deals.

### **Опасности и риски, связанные с недостаточным управлением данными SAST.**

Недостаточное управление данными SAST может серьезно угрожать безопасности, качеству и конфиденциальности данных, а также замедлить процесс разработки. Конкретные опасности и риски представлены в таблице 2.

Таблица 2. Рассматриваемые опасности и риски при управлении данными SAST

<b>Опасности и риски</b>	<b>Пример</b>	<b>Последствия</b>
<i>Утеря данных</i>	Отсутствие сохранения результатов анализа может привести к их необратимой потере при системных сбоях или случайных удалениях файлов.	Хранение результатов анализа в незащищенном виде может угрожать конфиденциальности данных, особенно при анализе чувствительного или личного кода.
<i>Недостаточная конфиденциальность данных</i>	Результаты анализа хранятся в незащищенном виде, могут возникнуть угрозы конфиденциальности данных.	Несанкционированный доступ к результатам анализа может позволить злоумышленникам получить информацию о уязвимостях в системе и злоупотреблять ею в атаках или краже данных.
<i>Потеря истории результатов</i>	Результаты анализа не управляются с сохранением истории, команда разработки может потерять контекст о предыдущих результатах анализа.	Это может затруднить процесс принятия решений разработчиками и ухудшить их способность отслеживать изменения в уязвимостях и качестве кода.
<i>Неудачное сопровождение результатов</i>	Результаты анализа не обновляются регулярно после изменений в коде.	В таком случае, разработчики могут продолжать видеть устаревшие результаты, что может привести к неверным решениям и недоразумениям относительно текущего состояния безопасности и качества кода.

Все эти опасности и риски подчеркивают важность правильного управления данными SAST. Недостаточное внимание к этому аспекту может оказаться дорогостоящим и опасным для безопасности и надежности ПО.

### **Пути решения проблем хранения результатов SAST**

Система управления результатами SAST играет критическую роль в обеспечении безопасности и качества ПО. Для эффективной работы данная система должна удовлетворять ряду важных требований представленных в таблице 3.

Таблица 3. Требования к системе управления результатами SAST

Наименование требования	Описание требования	Обоснование требования
<i>Хранение и сохранность данных</i>	Система должна обеспечивать надежное и долгосрочное хранение результатов анализа.	Важно для того, чтобы иметь доступ к результатам анализа в будущем, а также для соблюдения требований нормативных актов и стандартов безопасности.
<i>История и версионность</i>	Система должна поддерживать хранение истории результатов анализа для каждой версии кода.	Исторический контекст позволяет отслеживать изменения в безопасности и качестве кода со временем и принимать обоснованные решения.
<i>Интеграция с инструментами разработки</i>	Система должна интегрироваться с инструментами разработки, такими как IDE, системы управления версиями и CI/CD-среды.	Интеграция облегчает автоматизацию анализа и включение его в рабочий процесс разработки.
<i>Масштабируемость</i>	Система должна масштабироваться для обработки больших объемов данных, сгенерированных SAST.	Проекты могут быть крупными, и система должна способствовать эффективной работе с большими объемами результатов анализа.
<i>Поддержка разных языков и платформ</i>	Система должна поддерживать анализ кода на разных языках программирования и платформах.	Разработка может включать в себя множество технологий, и система должна быть гибкой и адаптированной к разнообразным окружениям.
<i>Отслеживание статусов и сроков</i>	Система должна предоставлять средства для отслеживания статусов результатов анализа и установления приоритетов для устранения уязвимостей.	Это позволяет команде разработки фокусироваться на наиболее критических угрозах и управлять ресурсами более эффективно.
<i>Безопасность и конфиденциальность</i>	Система должна обеспечивать высокий уровень безопасности данных и контроль доступа к результатам анализа.	Защита данных об уязвимостях и ошибках в коде является критически важной для предотвращения их злоупотребления.
<i>Генерация отчетов и визуализация</i>	Система должна позволять генерировать отчеты о результатах анализа и визуализировать данные для легкости интерпретации.	Отчеты могут помочь разработчикам и руководству лучше понять текущее состояние безопасности и качества кода.
<i>Гибкость и возможность настройки</i>	Система должна быть гибкой и настраиваемой под потребности конкретного проекта.	Разные проекты могут требовать разных методов анализа и настройки.
<i>Аудит и журналирование</i>	Система должна поддерживать аудит и журналирование действий, связанных с результатами анализа.	Это важно для отслеживания, кто и когда имел доступ к данным анализа, и для обеспечения ответственности.

Удовлетворение этих требований позволяет системе управления результатами SAST эффективно поддерживать безопасность, качество и надежность ПО на всех этапах разработки.

Для эффективного хранения и управления данными SAST, система должна быть спроектирована с учетом оптимальной архитектуры. Вот несколько конкретных архитектурных подходов, которые могут быть использованы:

- *Централизованное хранилище данных.* Создание центрального хранилища данных, где все результаты анализа сохраняются и управляются в единой БД, обеспечивает единое место для хранения и доступа к результатам анализа, упрощает управление данными и обеспечивает централизованный контроль доступа. Однако данное решение может потребовать больших ресурсов для масштабирования и обеспечения высокой доступности.

- *Система управления контейнерами.* Использование контейнеризации, такой как Docker для упаковки и изоляции системы управления результатами анализа, облегчает развертывание и масштабирование системы, а также обеспечивает изоляцию данных. Однако для успешной реализации данного подхода требуется наличие знаний и опыта в области контейнеризации. На рисунке 3 представлена архитектура Docker [7].

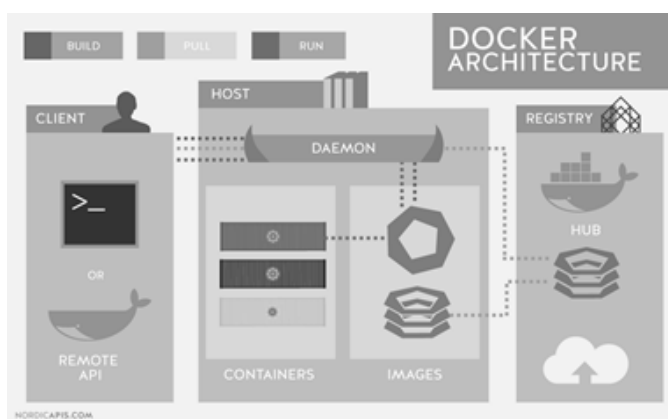


Рисунок 3. Архитектура Docker [7]

- *Микросервисная архитектура.* Разработка системы управления результатами как набора микросервисов, где каждый отвечает за определенные функции (например, хранение данных, аутентификацию, генерацию отчетов), предоставляет ряд преимуществ. Это подход упрощает масштабирование и обслуживание системы, а также позволяет разрабатывать и внедрять новые функции независимо друг от друга. Однако для успешной реализации такой архитектуры требуется более сложное управление сетью и инфраструктурой. Сравнение микросервисной и монолитной архитектуры показано на рисунке 4 [8].



Рисунок 4. Сравнение микросервисной и монолитной архитектуры

С учетом вышеприведенных фактов, выявлено, что выбор архитектурного подхода должен зависеть от конкретных требований проекта, его масштаба и бюджета.

Эффективное хранение и управление данными SAST играют важную роль в обеспечении безопасности и качества ПО, поэтому правильный выбор архитектуры является ключевым аспектом.

### Примеры использования технологий и инструментов для автоматизации управления результатами SAST

Автоматизация управления результатами SAST существенно упрощает процесс сбора, хранения и анализа данных, а также позволяет быстро реагировать на обнаруженные уязвимости и ошибки. Рассмотрим несколько технологий и инструментов, которые могут помочь в автоматизации этого процесса. Выбор этих технологий, представленных в таблице 4 обоснован их способностью улучшить эффективность и точность процесса.

Таблица 4. Перечень рассматриваемых технологий и инструментов для автоматизации управления результатами SAST

Наименование	Описание	Инструменты	Преимущества
<i>CI/CD интеграция</i>	Интеграция SAST в CI/CD позволяет автоматически запускать анализ после каждого коммита кода.	Jenkins Travis CI CircleCI GitLab CI/CD	Автоматический анализ заранее обнаруживает проблемы и ускоряет разработку.
<i>Скрипты автоматизации</i>	Написание скриптов для автоматического сбора, обработки и сохранения результатов SAST.	Python Bash PowerShell	Пользовательские скрипты могут быть интегрированы в процессы CI/CD
<i>Инструменты управления результатами</i>	Использование специализированных инструментов для управления и анализа результатами SAST.	SonarQube Fortify Coverity Checkmarx	Готовые решения для хранения, анализа и фильтрации результатов
<i>Автоматическая генерация отчетов</i>	Настройка системы для автоматической генерации отчетов о результатах SAST.	Отчеты можно создать с помощью управления или кастомных скриптов.	Автоматические отчеты облегчают мониторинг и делегирование задач по устранению уязвимостей.
<i>Интеграция с системами управления задачами</i>	Интеграция результатов SAST с системами управления задачами	JIRA Trello Asana	Позволяет автоматически создавать задачи для устранения обнаруженных проблем и отслеживать их статус.

Приведенные инструменты и технологии позволяют автоматизировать различные аспекты управления результатами SAST, снижая ручной труд и ускоряя процесс разработки безопасного ПО.

### Практические примеры

Компании и проекты, успешно внедрившие системы управления результатами SAST, часто используют разнообразные инструменты и решения для обеспечения безопасности и качества своего ПО. В таблице 5 приведены конкретные примеры компаний и решений [9].

Таблица 5. Примеры компаний и используемых ими решений для управления результатами SAST

<b>1. Институт Системного Программирования Российской Академии Наук и Svsace</b>	
<b>Решение</b>	<b>Преимущества</b>
Svsace - основной статический анализатор компании Samsung, обнаруживающий более 50 классов критических ошибок в исходном коде на языках C, C++, C#, Java, Kotlin и Go [1, 3].	Инновационный продукт объединяет качества иностранных аналогов, используя открытые компиляторы для поддержки новых стандартов языков программирования, результат многолетних исследований.
<b>2. ПАО Ростелеком и Solar appScreener</b>	
<b>Решение</b>	<b>Преимущества</b>
ПАО Ростелеком использует Solar appScreener для всестороннего контроля безопасности приложений с удобным унифицированным интерфейсом, интеграцией различных анализаторов кода и подробными отчетами о результатах проверок [14].	Одно решение для уменьшения рисков информационной безопасности, предотвращения инцидентов связанных с уязвимостями, анализа кода, контроля над разработчиками и проверки наследуемого ПО.
<b>3. Microsoft и Azure DevOps</b>	
<b>Решение</b>	<b>Преимущества</b>
Microsoft использует Azure DevOps для управления результатами SAST и обеспечения безопасности кода. В рамках Azure DevOps интегрированы инструменты SAST, такие как SonarQube, Checkmarx, и другие.	Microsoft использует инструмент, который мониторит качество и безопасность кода в реальном времени, автоматически создает задачи для устранения ошибок и уязвимостей, а также интегрирует анализ в CI/CD процессы.
<b>4. Google и инструменты Linters</b>	
<b>Решение</b>	<b>Преимущества</b>
Google использует инструменты SAST, собственные линтеры для различных языков программирования.	Это помогает Google поддерживать высокие стандарты кодирования и улучшать безопасность и производительность.

Рассмотренные примеры демонстрируют успешное внедрение систем управления результатами SAST в крупных технологических компаниях и организациях, что способствует улучшению безопасности и качества их ПО.

### **Заключение.**

SAST на ранних этапах разработки снижает риски безопасности, но управление результатами сталкивается с проблемами объема данных и эффективности инструментов. Автоматизация с помощью ИИ и МО улучшает обнаружение угроз. Примеры, такие как Microsoft с Azure DevOps, подтверждают практичность этих решений. Дальнейшие исследования должны сосредоточиться на усовершенствовании алгоритмов, интеграции машинного обучения и обработке больших данных. Важно также снижение ложных срабатываний, интеграция в DevSecOps и создание инструментов для новых языков и многопоточных систем. Гибкие политики безопасности дополнят защиту данных, сделав разработку безопасного ПО более эффективной и надежной.

### **СПИСОК ЛИТЕРАТУРЫ**

1. *Иванников В. П., Белеванцев А. А., Бородин А. Е., Игнатьев В. Н., Журихин Д. М., Аветисян А. И., Леонов М. И.* Статический анализатор Svsace для поиска дефектов в исходном коде программ. – Труды ИСП РАН, 26(1):231—250, 2014.
2. Education at ISPRAS [Электронный ресурс]: // Статический анализ исходного кода – Режим доступа: <https://education.at.ispras.ru/static-analysis>, свободный. – Загл. с экрана. (дата обращения 13.09.2023)
3. *Belevantsev A., Izbyshchev, A., Zhurikhin, D.*, Monitoring program builds for Svsace static analyzer, Syst. Admin., 2017, nos. 7-8, pp. 135-139.

- 
4. Insights Stackoverflow [Электронный ресурс]: // Technology databases – Режим доступа: <https://insights.stackoverflow.com/survey/2021#technology-databases-all-respondents4>, свободный. – Загл. с экрана. (дата обращения 14.09.2023)
  5. Clickup [Электронный ресурс]: // 20 Best Bug Tracking Software, Tools, & Solutions in 2023 – Режим доступа: <https://clickup.com/blog/bug-tracking-software/>, свободный. – Загл. с экрана. (дата обращения 14.09.2023)
  6. G2 [Электронный ресурс]: // Top 10 Fortify Static Code Analyzer Alternatives & Competitors – Режим доступа: <https://www.g2.com/products/fortify-static-code-analyzer/competitors/alternatives>, свободный. – Загл. с экрана. (дата обращения 15.09.2023)
  7. Cosmicportal [Электронный ресурс]: // Как использовать Docker – Режим доступа: <https://cosmicportal.ru/bolshoj-vypusk-pro-docker%E2%80%8B-kak-ispolzovat-doker-docker/>, свободный. – Загл. с экрана. (дата обращения 17.09.2023)
  8. IT-world [Электронный ресурс]: // Переход от монолита к микросервисам – Режим доступа: <https://www.it-world.ru/tech/practice/173784.html>, свободный. – Загл. с экрана. (дата обращения 17.09.2023)
  9. ИСП РАН [Электронный ресурс]: // Статический анализатор Svace – Режим доступа: <https://www.ispras.ru/technologies/svace/>, свободный. – Загл. с экрана. (дата обращения 17.09.2023)
  10. Комплексный подход к анализу ПО [Электронный ресурс]: // Solar appScreener для информационной безопасности – Режим доступа: [https://rt-solar.ru/products/solar\\_appscreener/](https://rt-solar.ru/products/solar_appscreener/), свободный. – Загл. с экрана. (дата обращения 17.09.2023)

**Т.Д. Фатхулин, Н.Ю. Климов, С.А. Гежин**

### **АНАЛИЗ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ, ПОЗВОЛЯЮЩИХ ГЕНЕРИРОВАТЬ ТЕКСТ**

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», Москва, Россия

Ключевые слова: нейронные сети, генерация текста, искусственный интеллект, глубокое обучение, рекуррентные нейронные сети, сверточные нейронные сети, обработка естественного языка.

В представленной статье приведен обзор современных нейросетевых методов и технологий, используемых для генерации текста. В ней рассматриваются ключевые аспекты и достижения в области генерации текста с использованием искусственных нейронных сетей, включая генерацию текста на естественном языке и текстовых данных в различных контекстах. Статья также подробно исследует применение нейросетей в создании автоматизированных текстовых систем и их потенциальные применения в будущем. В заключении сделаны выводы по проведенному анализу.

## ANALYSIS OF NEURAL NETWORK TECHNIQUES FOR TEXT GENERATION

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: neural networks, text generation, artificial intelligence, deep learning, recurrent neural networks, convolutional neural networks, natural language processing.

This article provides an overview of modern neural network methods and technologies used for text generation. It reviews key aspects and advances in the field of text generation using artificial neural networks, including the generation of natural language text and text data in various contexts. The article also explores in detail the use of neural networks in creating automated text systems and their potential applications in the future. At the end, conclusions are drawn from the carried out analysis.

### **Введение.**

В последние годы технологии, использующие нейронные сети (НС), стали неотъемлемой частью современной обработки естественного языка и автоматической генерации текста. Рассматриваемая предметная область исследований и приложений продолжает стремительно развиваться, предоставляя уникальные возможности для создания текстовых данных, обогащения контента и автоматизации процессов написания текстов.

Актуальность данной работы обусловлена несомненным ростом интереса к применению нейросетевых технологий для генерации текста в различных сферах. Они позволяют автоматизировать создание контента, улучшать процессы анализа текстовых данных, создавать персонализированный контент, и обогащать множество областей, таких как маркетинг, медицина, образование и другие. Важность исследований в этой области состоит в том, что они способствуют усовершенствованию современных методов обработки текста, что имеет широкую применимость в цифровом мире.

Цель данного доклада состоит в исследовании и анализе современных нейросетевых технологий, используемых для генерации текста, для понимания их актуальных применений и потенциальных перспектив.

Для достижения поставленной цели следует решить ряд задач:

- определить назначение генерации текста нейронными сетями;
- проанализировать методы машинного обучения, применяемые в области обработки текста и его генерации до появления нейросетей;
- выявить особенности применения рекуррентных и трансформерных нейронных сетей для генерации текста;
- рассмотреть области применения и практические аспекты генерации текста;
- сделать выводы по проведенному анализу.

Для решения поставленных задач были использованы теоретические методы исследования, такие как анализ, систематизация и обобщение.

### **Общая характеристика задачи генерации текста.**

Задача генерации текста — это одна из ключевых задач в области обработки естественного языка (Natural Language Processing, NLP) и машинного обучения (МО, Machine Learning – ML) [1]. Она заключается в создании компьютерной системы или модели, способной автоматически создавать текстовую информацию, подобную той, которую может создать человек. Вот общие характеристики этой задачи. Главной целью задачи генерации текста является создание качественного и понятного текста, который может быть прочитан и понят человеком. Этот текст может представлять собой непрерывный поток слов, предложений или даже целых документов [1, 2].



---

Задача генерации текста остается активной областью исследований, и с развитием глубокого обучения и нейросетей появляются все более продвинутые методы для достижения более качественных результатов в этой области.

### **Основные методы МО, применяемые для генерации текста.**

Методы машинного обучения, применяемые в области обработки текста и генерации до появления нейросетей, представляют собой важный исторический обзор развития этой области. До появления нейронных сетей, исследователи и инженеры внимательно разрабатывали и применяли различные традиционные методы машинного обучения для анализа и создания текстовых данных. Вот некоторые из них [3].

- *Метод байесовской классификации.* Один из первых методов, применяемых в обработке текста, основывается на теореме Байеса. Этот метод использовал вероятностные модели для классификации текстовых данных, например, для фильтрации спама в электронной почте.
- *Метод статистического анализа.* В этом методе текстовые данные анализируются с использованием статистических методов, таких как TF-IDF (Term Frequency-Inverse Document Frequency), который определяет важность слов в тексте, или статистические методы для кластеризации текстовых документов.
- *Методы машинного обучения на основе деревьев решений.* Методы, такие как деревья решений и случайные леса, применялись для классификации текстовых данных и анализа сентимента, а также для построения систем рекомендации на основе текстовых данных.
- *Скрытые марковские модели.* Эти модели были широко применяемы для анализа последовательностей текстовых данных, таких как распознавание речи и машинный перевод.
- *Методы кластеризации и снижения размерности.* К этим методам относятся такие, как метод главных компонент (PCA) и кластерный анализ. Они использовались для организации и визуализации больших объемов текстовых данных.

Эти методы машинного обучения показали себя весьма эффективными в своей области, но они имели ограничения, связанные с обработкой больших объемов данных и сложностью моделирования высокоуровневых текстовых паттернов. Появление нейросетей, особенно рекуррентных и сверточных нейронных сетей, внесло революцию в область обработки текста, позволяя моделировать сложные текстовые зависимости и достигать выдающихся результатов в задачах генерации и анализа текста.

### **Рекуррентные нейронные сети (RNN) в генерации текста.**

Рекуррентность - основное отличие RNN от других типов нейронных сетей, таких как сверточные сети (CNN), заключается в наличии рекуррентного (циклического) соединения. Это означает, что выход RNN на текущем временном шаге также становится входом на следующем временном шаге. Это создает обратную связь в сети, которая позволяет ей сохранять информацию о предыдущих шагах.

В RNN данные разбиваются на последовательные временные шаги или *timestamp*. На каждом временном шаге RNN принимает входные данные и скрытое состояние (прошлой скрытое состояние или начальное состояние) и выдает выходной результат и новое скрытое состояние. Скрытое состояние служит для передачи информации от одного временного шага к следующему.

RNN имеют весовые матрицы, которые обучаются в процессе обучения сети. Эти матрицы используются для преобразования входных данных и скрытых состояний в выходные данные и новые скрытые состояния.

---

Благодаря рекуррентному соединению RNN способны учитывать контекст и зависимости в последовательных данных. Это делает их подходящими для задач, таких как обработка естественного языка (NLP), где порядок слов имеет значение, и временные ряды, где значения зависят от предыдущих моментов времени.

У RNN есть некоторые недостатки и проблемы, такие как затухание и взрывание градиента. Затухание градиента может привести к тому, что долгосрочные зависимости становятся трудноразличимыми, а взрывание градиента может привести к неустойчивости обучения. Эти проблемы частично решаются с использованием различных архитектурных модификаций, таких как LSTM (Long Short-Term Memory) и GRU (Gated Recurrent Unit).

RNN широко используются в задачах, где важен контекст и порядок данных, включая машинный перевод, генерацию текста, анализ временных рядов, обработку речи, предсказание временных рядов и многое другое.

Важно отметить, что несмотря на свои преимущества, традиционные RNN имеют ограничения, связанные с обработкой долгосрочных зависимостей. Эти ограничения привели к разработке более сложных архитектур, таких как LSTM и GRU, которые помогают справиться с проблемой затухания градиента и улучшить способность моделей обрабатывать долгосрочные зависимости в данных.

### **Трансформеры и архитектура Attention.**

Архитектура Attention является ключевым компонентом в современных генеративных моделях, таких как трансформеры. Она позволяет модели фокусироваться на определенных частях входных данных в зависимости от их важности, что делает ее мощным инструментом для обработки последовательных данных, таких как тексты и временные ряды. Вот некоторые основные концепции и элементы архитектуры Attention в контексте трансформеров.

- *Словесное внимание (Self-Attention)*. Самое важное внимание в трансформерах - это механизм само-внимания, который позволяет модели определять важность различных частей входных данных внутри самих себя. Для текстов это означает, что модель может выявлять зависимости между словами в предложении, учитывая их контекст.
- *Входные эмбединги*. Перед тем как применить механизм внимания, текст (или другие последовательные данные) представляются в виде эмбедингов. Эмбединги - это числовые векторы, представляющие каждое слово или элемент последовательности.
- *Оценки важности (Attention Scores)*. Для каждой пары элементов входных данных вычисляются оценки важности с использованием функции сходства (как правило, скалярное произведение или многослойная нейронная сеть). Эти оценки определяют, насколько важен каждый элемент для других элементов в последовательности.
- *Весовые коэффициенты (Attention Weights)*. Оценки важности нормализуются (чтобы они суммировались до 1), чтобы получить весовые коэффициенты, которые отражают, какую часть входных данных следует учитывать в конкретный момент времени.
- *Взвешенная сумма (Weighted Sum)*. Используя весовые коэффициенты, вычисляется взвешенная сумма входных данных, что и представляет собой результат внимания. Эта взвешенная сумма позволяет модели обрабатывать контекст и фокусироваться на наиболее важных элементах.
- *Многозаголовочное внимание (Multi-Head Attention)*. В трансформерах применяется многозаголовочное внимание, что позволяет модели фокусироваться на разных аспектах входных данных. Каждая составляющая («Head») вычисляет свои собственные оценки важности и весовые

---

коэффициенты, а затем их объединяют для получения окончательного результата.

- *Подслои само-внимания (Self-Attention Sublayers)*. Архитектура трансформера включает в себя несколько подслоев само-внимания, которые позволяют модели многократно обрабатывать входные данные, уточняя свой контекст с каждым проходом.

Архитектура Attention в трансформерах играет ключевую роль в обработке текста, переводе, генерации текста и других задачах, где последовательность данных имеет значение. Эта архитектура позволяет моделям улавливать долгосрочные зависимости и контекст, что делает ее мощным инструментом для работы с текстом и последовательными данными.

Трансформеры представляют собой современную архитектуру для обработки последовательных данных, которая имеет ряд преимуществ перед рекуррентными нейронными сетями (RNN). Вот некоторые из основных преимуществ трансформеров:

1. **Параллельная обработка.** Трансформеры способны обрабатывать входные данные параллельно, в отличие от RNN, которые обрабатывают данные последовательно по времени. Это делает трансформеры гораздо более эффективными с точки зрения вычислительных ресурсов, поскольку их можно обучать и применять на графических процессорах (GPU) или тензорных процессорах (TPU) в больших пакетах данных.
2. **Долгосрочные зависимости.** Трансформеры способны обрабатывать долгосрочные зависимости в данных благодаря механизму само-внимания (Attention), который позволяет модели фокусироваться на разных частях входных данных в зависимости от их важности. Также не имеют проблем с исчезающим градиентом, которые часто встречаются в RNN.
3. **Гибкость архитектуры.** Трансформеры могут быть адаптированы для различных задач, включая обработку текста, машинный перевод, генерацию текста, обработку аудиосигналов и многое другое. Они достигли выдающихся результатов во многих областях и позволяют легко внедрять дополнительные компоненты и адаптировать архитектуру.
4. **Внимание к контексту.** Трансформеры обладают хорошей способностью обрабатывать контекст и учитывать долгосрочные зависимости между элементами последовательности. Это позволяет им лучше понимать и генерировать текст, а также решать задачи, связанные с последовательностями данных.
5. **Многозаголовочное внимание.** Трансформеры используют многозаголовочное внимание, что позволяет моделям фокусироваться на разных аспектах входных данных и улавливать разные типы зависимостей, что делает их мощными для различных задач.
6. **Снижение зависимости от длины последовательности.** Трансформеры обычно более устойчивы к вариации длины последовательности, чем RNN, и могут работать с последовательностями разной длины без необходимости использования паддингов.
7. **Простота реализации.** Трансформеры имеют более простую структуру и меньше параметров по сравнению с RNN, что может снижать риск переобучения.

Эти преимущества сделали трансформеры популярными и ведущими архитектурами в машинном обучении и глубоком обучении. Однако, в зависимости от задачи и доступных данных, RNN могут оставаться полезными и эффективными, особенно при работе с последовательными данными, где важна временная зависимость.

---

### **АРХИТЕКТУРЫ BERT и GPT.**

BERT (BIDIRECTIONAL ENCODER REPRESENTATIONS FROM TRANSFORMERS) и GPT (GENERATIVE PRE-TRAINED TRANSFORMER) - две из наиболее важных и влиятельных архитектур в области обработки естественного языка (NLP). Обе архитектуры основаны на трансформере, но имеют разные цели и структуры. В таблице 1 представлено сравнение BERT и GPT [4].

Обе архитектуры, BERT и GPT, имеют огромное влияние на область NLP и являются основой для множества приложений и исследований в этой области. Кроме того, существуют различные вариации и модели, основанные на этих архитектурах, что делает их ещё более мощными и универсальными.

### **Применение и практические аспекты генерации текста.**

Генерация текста имеет широкий спектр практических применений, включая автоматическое реферирование, создание контента для web-сайтов и социальных медиа, генерацию диалоговых систем (чат-ботов), автоматический перевод, генерацию литературных произведений и многое другое.

Генерация текста имеет множество практических применений и может быть полезной в различных областях. Вот несколько примеров использования и практических аспектов генерации текста [5-7]:

- генерация контента для сайтов и блогов: автоматическая генерация статей, новостных заголовков и контента для интернет-ресурсов может быть полезной для увеличения объема контента и привлечения аудитории;
- создание продуктовых описаний: генерация текстовых описаний для товаров и услуг может улучшить эффективность электронной коммерции, а также помочь в управлении большим объемом товаров;
- генерация рекламных текстов и объявлений: автоматическая генерация рекламных текстов, баннеров и объявлений может помочь в маркетинге и рекламе продуктов и услуг.
- автоматическое дополнение текста: системы автодополнения текста используют генерацию текста для предложения пользователю завершений предложений, слов и фраз во время набора текста, что повышает удобство использования приложений и web-сайтов.
- системы виртуальных ассистентов и чат-боты: генерация текста используется для создания ответов и диалоговых систем, таких как Siri, Google Assistant, Яндекс.Алиса и других чат-ботов для обработки запросов, и взаимодействия с пользователями.
- генерация музыки и лирики: музыкальные композиторы и текстовые писатели могут использовать генерацию текста для создания музыкальных текстов и лирики, а также для создания новых мелодий.
- генерация кода программ: генерация текста может использоваться для создания кода программ, автоматической генерации скриптов и облегчения разработки программного обеспечения.
- машинный перевод: модели генерации текста могут применяться в системах машинного перевода для создания текста на целевом языке на основе входного текста на исходном языке.

Таблица 1. Сравнение нейронных сетей BERT и GPT

	<b>BERT (Bidirectional Encoder Representations from Transformers)</b>	<b>GPT (Generative Pre-trained Transformer)</b>
<i>Описание</i>	Модель для предварительного обучения, ориентированная на двустороннее понимание контекста в тексте. Основная идея BERT заключается в том, чтобы обучить модель на большом объеме текстовых данных и предсказать недостающие слова в контексте предложения (masked language modeling) и в то же время обучить модель на предсказание следующего предложения в тексте. Это позволяет модели понимать более глубокие семантические зависимости в тексте.	Модель для генерации текста и обработки последовательных данных. Основная идея GPT заключается в том, чтобы обучить модель на большом объеме текстовых данных и использовать ее для автоматической генерации текста, учитывая контекст предложения.
<i>Архитектура</i>	Состоит из многозаголовочного механизма внимания, который позволяет модели улавливать контекст и зависимости между словами в обоих направлениях (слева направо и справа налево). Он имеет два варианта размера: BERT-Base и BERT-Large.	Использует архитектуру трансформера, но ориентирован на генерацию текста. Его механизм внимания ограничен однонаправленным контекстом (слева направо), что делает его хорошо подходящим для задач генерации текста. Существуют несколько версий GPT, таких как GPT-2 и GPT-3, с различными размерами и количеством параметров. GPT-3, например, является одним из самых больших искусственных нейронных сетей, когда-либо созданных.
<i>Применение</i>	Быстро стала основой для множества задач NLP, таких как классификация текста, извлечение именованных сущностей, вопросно-ответные системы, машинный перевод и многое другое. Существуют различные вариации BERT, такие как DistilBERT, RoBERTa, и др., которые представляют собой улучшенные и оптимизированные версии оригинальной модели.	Используется в задачах генерации текста, автоматической дополнительной записи, генерации кода программы, создания искусств и других задач, связанных с текстовой генерацией. GPT-3 также продемонстрировал способность к выполнению разнообразных задач, когда ему предоставляется контекст и инструкции.

Практические аспекты генерации текста включают в себя выбор подходящей архитектуры модели (например, трансформеры, RNN), обучение модели на соответствующих данных, настройку гиперпараметров, оценку качества генерации (например, BLEU, ROUGE для текста или музыкальные метрики для музыки), и управление качеством и стилем генерируемого контента.

Кроме того, необходимо учитывать этические аспекты, такие как возможность генерации ложных новостей или текстов, нарушающих авторские права. Следует обеспечить контроль и мониторинг за создаваемым контентом, чтобы он соответствовал нормам и стандартам.

### **Заключение.**

Таким образом, нейросетевые технологии, способные генерировать текст, представляют собой инновационное исследовательское направление, которое уже сегодня трансформирует область обработки естественного языка и создания контента. С развитием архитектур, таких как трансформеры и GPT, мы видим рост производительности и качества генерации текста, что открывает новые горизонты для автоматизации, машинного перевода, создания контента и других приложений. Однако важно помнить о этических и качественных аспектах в использовании этих технологий и продолжать исследования в этой области, чтобы обеспечить их устойчивое и ответственное внедрение в нашу цифровую среду. В статье был проведен анализ наиболее часто применяемых архитектур нейронных сетей для генерации текста. Выявлены их преимущества и недостатки. Проведен сравнительный анализ моделей BERT и GPT. Представлены области применения нейронных сетей, генерирующих текст.

---

## СПИСОК ЛИТЕРАТУРЫ

1. *Иванов А.В.* Применение нейросетей в генерации текста и его анализе // Научно-технический вестник информационных технологий, 2020, с. 45-51.
2. *Петров С.И.* Исследование современных методов генерации текста на основе нейронных сетей // Информационные технологии и вычислительные системы, 2019, с. 112-121.
3. *Смирнова Е.А.* Применение архитектур глубокого обучения в задачах текстовой генерации // Вестник компьютерных и информационных технологий, 2018, с. 54-61.
4. *Григорьев, Д.В.* Анализ и сравнение методов генерации текста с использованием нейронных сетей // Современные информационные технологии и ИТ-образование, 2017, с. 56-62.
5. 10 примеров использования ChatGPT и Midjourney в бизнесе и не только [Электронный ресурс]: // Обзор функционала и проблем популярных нейросетевых сервисов. – Режим доступа: [https://www.rbc.ru/spb\\_sz/11/06/2023/6483048b9a794751683574bf](https://www.rbc.ru/spb_sz/11/06/2023/6483048b9a794751683574bf), свободный. – Загл. с экрана. (дата обращения 11.09.2023).
6. Как правильно составлять запросы для нейросетей: формулы, шаблоны и примеры [Электронный ресурс]: // Описание способов составления запросов к нейронным сетям. – Режим доступа: <https://smmplanner.com/blog/kak-pravilno-sostavliat-zaprosy-dlia-nejrosietiei-formuly-shablony-i-primery/>, свободный. – Загл. с экрана. (дата обращения 11.09.2023).
7. *Митрофанов, А. О., Степанов, М. Н., Фатхулин, Т. Д.* Анализ нейросетевых методов генерации изображения по текстовому запросу // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2022. – № 1. – С. 19-23.

Т.Д. Фатхулин, Е.А. Лушин

### АНАЛИЗ РАЗВИТИЯ АВТОМАТИЧЕСКОЙ ГЕНЕРАЦИИ КОДА ДЛЯ WEB-СЕРВИСОВ

Ордена Трудового Красного Знамени федеральное государственное Бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», Москва, Россия

Ключевые слова: web-разработка, автоматизация, нейронные сети, машинное обучение, технологические инновации, код, анализ, искусственный интеллект.

В статье рассматривается автоматическая генерация кода для web-сервисов с помощью нейронных сетей, с представлением этапов её развитие от простых шаблонов до передовых технологий машинного обучения. Особое внимание уделено практическим аспектам применения, а также влиянию квантовых компьютеров на будущее данной области. Приведено комплексное представление текущих трендов и перспектив в автоматизации web-разработки с использованием искусственного интеллекта.

## ANALYSIS OF THE DEVELOPMENT OF AUTOMATIC CODE GENERATION FOR WEB-SERVICES

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: web development, automation, neural networks, machine learning, technological innovation, code, analysis, artificial intelligence.

The article discusses the automatic generation of code for web-services using neural networks, presenting the stages of its development from simple templates to advanced machine learning techniques. Particular attention is paid to the practical aspects of application, as well as the impact of quantum computers on the future of this field. A comprehensive presentation of current trends and prospects in the automation of web development using artificial intelligence is provided.

### **Введение.**

Современный мир web-разработки быстро меняется, а требования к качеству и скорости создания сайтов постоянно растут. В этой динамичной обстановке поиск путей автоматизации процессов разработки стоит на переднем плане. Один из наиболее обещающих и перспективных подходов – использование искусственного интеллекта, в частности, нейронных сетей, для автоматической генерации web-кода.

Такой подход позволяет не только ускорить разработку, но и предоставить возможность создавать сложные и оптимизированные решения без глубоких знаний в области программирования. Например, необходимо создать web-сайт: вместо долгих часов кодирования или работы с шаблонами, достаточно просто описать желаемую функциональность, а система на основе нейронных сетей сгенерирует необходимый код.

Цель работы - провести комплексное исследование прогресса в автоматической генерации web-кода с использованием нейронных сетей. Решаемые в исследовании задачи:

- исследовать историческую перспективу автоматической генерации web-кода, начиная с применения шаблонов и фреймворков.
- рассмотреть современные методы и технологии, применяемые для генерации кода, с акцентом на архитектуры нейронных сетей.
- проанализировать практические примеры применения нейронных сетей в автоматической генерации кода, выявить их преимущества и ограничения.
- оценить потенциальное влияние квантовых компьютеров и других перспективных технологий на будущее автоматического кодирования.
- сформулировать выводы о текущем состоянии автоматической генерации web-кода и ожидаемых трендах в этой области.

В данной статье будет рассмотрено, как развивалась концепция автоматической генерации web-кода, какие технологии и методы стоят за этим процессом, а также какие перспективы открываются перед web-разработчиками благодаря применению нейронных сетей.

Методологическая основа статьи: метод теоретического анализа, описательный метод, методы обобщения и систематизации.

### **Анализ развития автоматической генерации кода.**

Автоматизация web-разработки не является новой идеей. Десятилетиями разработчики искали способы упростить и ускорить процесс создания web-сайтов, начиная с простых шаблонов и заканчивая полноценными фреймворками [1].

В начале развития интернета создание сайта требовало ручного кодирования каждой страницы, что было трудоёмко и подвержено ошибкам [1]. Появление CMS (систем управления контентом) вроде WordPress, Joomla и Drupal облегчило задачу, позволяя пользователям создавать web-сайты с помощью графических интерфейсов без необходимости написания кода [2].

Однако с ростом сложности web-приложений и потребности в уникальных функциональных решениях, было ясно, что нужны более продвинутые инструменты. Фреймворки, такие как Angular, React и Vue.js, предоставили разработчикам инструментарий для создания сложных web-приложений, но все равно требовали знания кода [3].

Появление машинного обучения и, в частности, нейронных сетей открыло новые горизонты для автоматической генерации кода. Эти технологии позволили перейти от статичных шаблонов и ручного кодирования к динамической генерации кода на основе обученных моделей. Вместо того чтобы следовать жестко заданным правилам, системы на основе нейронных сетей могут "понимать" задачу и генерировать соответствующий код, учитывая контекст и требования проекта [4]. На рисунке 1 продемонстрирована историческая лента web-разработки с основными событиями в этой сфере за последние 30 лет.

Историческая лента веб-разработки			
1990-е: Ранний интернет	2000-е: Взлет CMS и фреймворков	2010-е: SPA и новые библиотеки	2020-е: Нейронные сети и автоматизация
1991: Введение HTML	2001: Появление Drupal	2010: Введение AngularJS	2020: Появление OpenAI Codex
1993: Появление первого графического браузера Mosaic	2003: Запуск WordPress	2013: React	2021: DeepMind и глубокое обучение
1995: JavaScript	2004: Появление Ruby on Rails	2016: Vue.js	2022: Рост инструментов автоматизации
	2008: Запуск Google Chrome		
	2009: Появление Node.js		

Рисунок 1. Развитие web-разработки

Такое развитие стало возможным благодаря комбинации технологического прогресса в области искусственного интеллекта и растущего спроса на быструю, эффективную и качественную разработку web-решений [1, 4].

### Основные рассматриваемые методы и технологии.

Нейронные сети представляют собой уникальный инструмент, способный обучаться на основе данных и применять полученные знания для различных задач, в том числе для генерации кода [7]. Основные методы и технологии в этой области включают:

1. *RNN (Рекуррентные нейронные сети)*:
  - эти сети содержат "память", позволяющую им учитывать предыдущие входные данные при обработке новой информации;
  - хорошо подходят для последовательных данных, например, текста, что делает их подходящими для генерации кода [4].
2. *LSTM (Долгосрочная память с короткосрочной перспективой)*:
  - разновидность RNN, которая эффективно решает проблемы с "затуханием" градиента [4];
  - благодаря своей структуре, LSTM отлично подходит для задач, требующих "памяти" о долгосрочных зависимостях в данных.
3. *Transformer и Attention механизмы*:
  - внедрены для оптимизации обработки последовательных данных, позволяя модели концентрироваться на наиболее важных частях входных данных [4];



- 
- особенно актуальны в последние годы и являются основой таких моделей как GPT и BERT.

Для обучения нейронных сетей для генерации кода используются большие наборы данных, состоящие из примеров кода. После обучения система способна генерировать код на основе предоставленных ей инструкций или описаний, пытаясь максимально приблизиться к "идеальному" коду, который бы создал человек [5].

Важно отметить, что автоматическая генерация кода с использованием нейронных сетей находится на стыке нескольких областей: программирования, дизайна, машинного обучения [6]. Это требует глубокого понимания каждой из этих дисциплин, а также умения интегрировать их знания для достижения наилучшего результата. Однако, несмотря на сложность этого процесса, достижения в этой области продолжают удивлять: автоматически сгенерированные сайты и приложения становятся все более сложными, функциональными и качественными [3].

### **Примеры практического применения.**

Использование нейронных сетей в автоматической генерации web-кода уже не является лишь теоретической идеей или экспериментом. На сегодняшний день многие инструменты и платформы успешно интегрируют этот подход, предлагая разработчикам и дизайнерам новые возможности [4, 7]. Рассмотрим их подробнее.

1. *OpenAI Codex*. Продукт от OpenAI, который может генерировать код на основе естественного языка [8]. Пользователь может задать вопрос или описание задачи, и Codex попытается предоставить соответствующий код [12]. Используется в различных интегрированных средах разработки для быстрого прототипирования и помощи в написании кода.
2. *DeepCode*. Инструмент, использующий машинное обучение для анализа и проверки кода, выявления уязвимостей и предложения решений для их устранения [9].
3. *GitHub Copilot*. Разработан в сотрудничестве с OpenAI, этот инструмент предлагает автоматические советы и решения при написании кода, учитывая контекст разработки [10]. Способен генерировать функции, классы и даже целые модули на основе краткого описания задачи [12].
4. *Wix ADI (Artificial Design Intelligence)*. Платформа для создания web-сайтов, использующая искусственный интеллект для автоматического дизайна на основе предпочтений пользователя [11].

Преимущества использования таких инструментов очевидны: ускорение процесса разработки, уменьшение количества ошибок, возможность быстро создавать прототипы и проверять идеи [2, 5]. Однако также существуют и ограничения. Автоматически сгенерированный код может не всегда соответствовать стандартам качества или быть оптимизированным для конкретных задач [6]. Также важно помнить о необходимости проверки и тестирования такого кода, особенно в критически важных приложениях [3].

Тем не менее, практическое применение нейронных сетей в генерации web-кода продолжает расширяться, и в ближайшем будущем мы можем ожидать появления новых инновационных решений в этой области [4, 7]. На рисунке 2 представлена диаграмма популярности вышеописанных инструментов на основе статистики посещаемости их сайтов.



Рисунок 2. Статистика популярности инструментов на основе посещаемости сайтов

### Перспективы и потенциальные проблемы.

Автоматическая генерация web-кода с использованием нейронных сетей предоставляет множество возможностей для индустрии web-разработки, но также влечёт за собой определенные вызовы и потенциальные проблемы [1].

1. *Демократизация разработки.* Одним из главных преимуществ является упрощение и ускорение процесса разработки [2]. Новички или представители не технических специальностей смогут создавать функциональные web-приложения без глубоких знаний в программировании [3]. С другой стороны, это может привести к снижению спроса на начальные позиции web-разработчиков [4].
2. *Качество кода.* Нейронные сети могут генерировать код быстро, но не всегда оптимально [1]. Для критически важных приложений или сложных проектов может потребоваться дополнительная оптимизация и рефакторинг [2].
3. *Этические вопросы.* Необходимо определиться, кто несет ответственность за ошибки или уязвимости в автоматически сгенерированном коде [5]. Возможны потери рабочих мест из-за автоматизации процессов [4].
4. *Обучение и адаптация.* Постоянное обновление и доработка моделей нейронных сетей требует доступа к большим объемам данных, что может вызвать проблемы с конфиденциальностью и безопасностью [6]. Разработчикам необходимо адаптироваться к новым инструментам и учиться работать в сотрудничестве с AI, а не против него [7].
5. *Зависимость от платформ.* Если индустрия будет слишком зависима от определенных AI-решений или платформ, это может привести к монополизации рынка и уменьшению инноваций [8].
6. *Стандартизация и универсальность.* Одной из основных проблем может стать отсутствие стандартизации кода [3]. Если каждая нейронная сеть будет генерировать код по-своему, это может усложнить работу команд разработчиков и привести к проблемам совместимости [9].
7. *Исключение человеческого фактора.* Автоматизация процесса разработки может привести к тому, что уменьшится роль креативного подхода и интуитивного понимания задачи, которое часто присуще человеческим разработчикам [7].

- 
8. *Экономический аспект.* Введение нейронных сетей в процесс разработки может значительно снизить затраты на разработку и поддержку web-приложений [2]. Однако это также может вызвать изменение структуры затрат, например, на лицензирование или обучение специалистов [9].
  9. *Ограничения текущих AI-моделей.* Не все задачи могут быть автоматизированы с помощью существующих на сегодняшний день моделей [7]. Некоторые уникальные или креативные задачи могут остаться вне доступа для автоматической генерации кода [1].
  10. *Потенциал для интеграции.* С возрастанием возможностей AI в области генерации кода возникает потребность в интеграции с другими системами и технологиями, такими как базы данных, системы управления контентом или другие web-сервисы [3].

Несмотря на потенциальные проблемы, перспективы автоматической генерации web-кода с использованием нейронных сетей выглядят многообещающими [1]. Однако ключ к успешному внедрению таких технологий лежит в балансе между автоматизацией и человеческим вмешательством, а также в постоянном обучении и адаптации к изменяющемуся технологическому ландшафту [6, 7].

### **Перспективы автоматической генерации web-кода.**

В мире технологий постоянно происходят изменения, и автоматическая генерация web-кода не является исключением. При прогнозировании будущего данной области стоит учитывать следующие аспекты.

1. *Инновации в ближайшие годы:*
  - Глубокая персонализация: нейронные сети могут начать генерировать код, который адаптируется к конкретным пользователям или демографическим группам, предлагая более индивидуализированный опыт [4, 7, 12].
  - Интеграция с AR и VR: возрастающая популярность виртуальной и дополненной реальности может привести к автоматической генерации кода для этих платформ.
  - Самооптимизирующийся код: алгоритмы могут начать оптимизировать сгенерированный код в реальном времени на основе поведения пользователя, скорости работы и других метрик [8, 10].
2. *Влияние квантовых компьютеров:*
  - Быстродействие: квантовые компьютеры обладают потенциалом обрабатывать информацию гораздо быстрее, что может значительно ускорить процесс генерации кода.
  - Решение сложных проблем. многие задачи, которые трудно решить с помощью классических компьютеров, могут быть решены на квантовых машинах, что приведет к созданию более сложных и функциональных приложений с автоматически генерируемым кодом.
  - Безопасность: квантовые технологии могут привести к созданию новых методов шифрования, что повысит безопасность web-приложений.
3. *Другие технологии и их влияние:*
  - Блокчейн: автоматическая генерация кода для создания децентрализованных приложений или смарт-контрактов.
  - Интернет вещей (IoT): генерация кода для устройств с ограниченными ресурсами или специфическими требованиями к функциональности.
  - Биоинформатика: использование нейронных сетей для создания кода, адаптированного для работы с биологическими данными или для моделирования биологических процессов.

---

В итоге, будущее автоматической генерации web-кода выглядит ярким и полным возможностей. Новые технологии и инновации будут продолжать трансформировать эту область, делая процесс разработки еще более эффективным и динамичным.

### **Заключение.**

Таким образом, современные технологии, основанные на использовании нейронных сетей, открывают новые горизонты в сфере web-разработки, предоставляя инструменты для автоматической генерации кода. Выявлено, что это не просто упрощает и ускоряет процесс разработки, но также предлагает новые подходы и возможности для бизнеса, образования и культуры. Показано, что в перспективе автоматическая генерация web-кода может стать стандартом индустрии. Но, как и с любой инновационной технологией, ключевым является правильное и осознанное применение. Сбалансированный подход, сочетающий автоматизацию с человеческим вмешательством, позволит достичь наилучших результатов. Важно отметить, что эволюция автоматической генерации кода еще только начинается. Ее потенциальное влияние на индустрию web-разработки будет масштабным, и каждый специалист в этой сфере должен быть готов к грядущим изменениям, чтобы оставаться востребованным в этом быстро меняющемся мире.

### СПИСОК ЛИТЕРАТУРЫ

1. *Berners-Lee T.* Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web // HarperBusiness, 1999. p. 256.
2. *Веллинг Л., Томсон Л.* PHP и MySQL. Разработка веб-приложений. – СПб.: Питер, 2008, 672 с.
3. *Sufyan bin Uzayr, Zeeshan Chawdhary, Tam Ho.* JavaScript Frameworks for Modern Web Development: The Essential Frameworks, Libraries, and Tools to Learn Right Now // Apress, 2019. p. 539.
4. *Goodfellow, I., Bengio, Y., & Courville, A.* The Deep Learning // MIT Press, 2016, p. 800.
5. *Воронцов К.В.* Машинное обучение и анализ данных. [Электронный ресурс]. – М.: МФТИ, 2014.  
[https://www.youtube.com/playlist?list=PLJOzdkh8T5kp99tGTEFjH\\_b9zq](https://www.youtube.com/playlist?list=PLJOzdkh8T5kp99tGTEFjH_b9zq)
1. EQiiBtC (дата обращения: 27.09.2023)
6. *Ameisen E.* Building Machine Learning Powered Applications: Going From Idea to Product // O'Reilly Media, 2020, p. 303.
7. *Хайкин С.* Нейронные сети: полный курс. 2-е изд., испр. - М.: Вильямс, 2006, 1103 с.
8. OpenAI. Codex: OpenAI's Code Generation Model. [Электронный ресурс]. OpenAI Blog, 2022. <https://openai.com/blog> (дата обращения: 27.09.2023).
9. DeepCode. DeepCode: Machine Learning for Code Analysis. [Электронный ресурс]. 2021. <https://snyk.io/> (дата обращения: 27.09.2023).
10. GitHub. GitHub Copilot: Your AI pair programmer. [Электронный ресурс]. 2022. <https://github.com/features/copilot> (дата обращения: 27.09.2023).
11. Wix. Wix ADI: The Future of Website Design. [Электронный ресурс]. 2020. <https://www.wix.com/blog/wix-artificial-design-intelligence> (дата обращения: 27.09.2023).
12. *Sutskever I., Vinyals O., & Le Q.V.* Sequence to sequence learning with neural networks // Advances in neural information processing systems, 2014, pp. 3104-3112.

**РАЗРАБОТКА МЕТОДИКИ ФОРМИРОВАНИЯ ЗАПРОСА К НЕЙРОСЕТИ С  
ЦЕЛЮ ГЕНЕРАЦИИ ИЗОБРАЖЕНИЙ С УЧЕТОМ РЕКОМЕНДАЦИЙ  
КОМПЬЮТЕРНОЙ ЛИНГВИСТИКИ**

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», Москва, Россия

Ключевые слова: методика, генерация, сервис, запрос, промпт, компьютерная лингвистика, нейронные сети, машинное обучение, искусственный интеллект.

В статье рассмотрены актуальные тенденции развития машинного обучения и нейронных сетей в частности, а также проблемы, возникающие при составлении текстового запроса к онлайн нейросетевым сервисам, генерирующим изображения. Предложена методика составления текстового запроса к нейронным сетям. Проведены эксперименты, апробирующие методику. В заключении сделаны выводы по полученным результатам экспериментов.

**T.D. Fatkhulin, G.G. Fatkhulina, M.V. Mentus**

**DEVELOPMENT OF A METHOD FOR FORMING A PROMPT TO A NEURAL  
NETWORK FOR THE PURPOSE OF GENERATING IMAGES BASED ON THE  
REQUIREMENTS OF COMPUTATIONAL LINGUISTICS**

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: methodology, generation, service, request, prompt, computational linguistics, neural networks, machine learning, artificial intelligence.

The article discusses current trends in the development of machine learning and neural networks in particular, as well as problems that arise when composing a text request to online neural network services that generate images. A technique for composing a text prompt to neural networks is proposed. Experiments were carried out to test the method. At the end conclusions are drawn based on the experimental results obtained.

**Введение.**

Машинное обучение (МО, Machine Learning – ML) на современном этапе проникает во все сферы человеческой деятельности [1-4]. К наиболее распространенным методам машинного обучения относятся те, которые базируются на искусственных нейронных сетях (НС, Neural Network – NN). Возможности использования нейронных сетей практически безграничны: поиск дефектов дорожного полотна [5-7], управление беспилотным транспортом [1,4,5,7], оптимизация маршрутизации в оптических сетях связи [8-12], составление долгосрочных экономических прогнозов [13]. Нейросети не только обрабатывают изображения, аудио и видео данные, но и сами создают тексты и изображения, которые могут посягаться с реальными объектами, созданными человеком. Эта способность позволила нейросетям стать полезным помощником авторов, редакторов, маркетологов, создателей рекламы [14]. Вышеперечисленные факты обуславливают актуальность выбранной для рассмотрения предметной области.

Цель работы – предложить методику составления текстовых запросов для онлайн сервисов генерации изображений, позволяющую ускорить процесс получения корректных результатов конечным пользователем. Для достижения поставленной цели требуется решить ряд взаимосвязанных задач:

- 
- проанализировать рассматриваемую предметную область генерации контента посредством нейросетевых сервисов и, в частности, генерации изображений;
  - выявить существующие проблемы создания контента нейросетевыми онлайн сервисами;
  - определить используемые в работе технологии и программные инструменты;
  - предложить методику, формализующую составление запроса к НС для описания объектов, процессов и явлений;
  - провести эксперименты для определения эффективности предложенной методики;
  - систематизировать полученные результаты и сделать выводы об эффективности предложенной методики.

Методы исследования, применяемые в работе: теоретический анализ, сравнительный анализ, описательный метод, метод эксперимента и методы систематизации и обобщения.

### **Проблемы использования искусственного интеллекта и нейронных сетей в креативных сферах жизни человека.**

В условиях внедрения нейросетей в самые разнообразные сферы жизни человека задача разработки научно-обоснованного подхода к формированию запросов по генерации качественного изображения становится крайне актуальной. Генерация нейросетью качественного изображения или текста начинается с правильного сформулированного человеком запроса/промта (от англ. *prompt* – запрашивать, побуждать) к искусственному интеллекту. Грамотно сформулированный промт позволит нейросети в считанные минуты написать деловое письмо, проанализировать целевую аудиторию, создать контрольные материалы к любому учебному пособию, сгенерировать идеи для новых текстов. Запрос или промт для генерации изображений поможет НС создать театральные декорации и костюмы, мультипликационных героев, дизайн общественного пространства, ювелирного изделия, необычную рекламу и т.п. Как отмечалось в статье «Десять примеров использования Chat GPT и Midjourney в бизнесе и не только», опубликованной Росбизнесконсалтингом (РБК), искусственный интеллект (ИИ, Artificial Intellect – AI) и НС применяются сегодня в творческих сферах и в бизнесе, а именно в архитектуре, анимации, театре, в производстве, SMM, ретейле, общепите и маркетинге [14]. Однако многие профессионалы отмечают, что формулировка запроса требует владения определенными знаниями, иначе на уточнения и исправления может уйти слишком много времени, так как полученный результат у неопытного пользователя может не соответствовать поставленной цели. Соответственно возникает необходимость разработки методики оптимальной формулировки запроса для быстрой и точной генерации изображения нейросетью. В настоящей работе будет разработана такая методика, которая является универсальной для различных архитектур нейросети.

### **Применяемые в исследовании технологии и программные инструменты.**

При выборе технологий и программных исследований для данного исследования за основу брались следующие требования: 1) используемая НС не требует от пользователя специальной подготовки или профессиональных знаний по настройке нейросети, 2) выбранная нейросеть должна использовать только бесплатные решения, открытые всем пользователям Интернета, 3) работа с сервисами проводится только в вопросно-ответной форме, где вопрос – это промт, а ответ – сгенерированное нейросетью изображение, 4) запросы формулируются только в словесной форме, дополнительные ключи, настройки, опции не используются.

В настоящее время наиболее широкое применение получили диффузионные сети [14, 16, 17]. Помимо диффузионных, для генерации изображений также используются генеративно-состязательные сети (GAN) [15].

---

Для данного исследования были выбраны два сервиса: «Kandinsky 2.2» - генеративно-состязательная сеть, разработанная компанией «Сбер» [19], и «Шедеврум» - диффузионная сеть, разработанная компанией «Яндекс» [18]. Выбор определялся двумя факторами: данные нейросети ориентированы на русскоязычную аудиторию, и «Kandinsky 2.2», и «Шедеврум» являются отечественными разработками, что в условиях санкций дает преимущества гарантированного доступа. «Шедеврум» по одному запросу генерирует сразу четыре изображения, из которых пользователь может выбрать наиболее подходящее к его запросу. «Kandinsky 2.2» генерирует одно изображение и дает возможность его корректировки перед сохранением на устройстве пользователя. Стоит упомянуть и зарубежные сервисы генерации изображений: «Stable Diffusion», «DALL-E», «Midjourney» [16, 17]. Наиболее популярная из них НС «Stable Diffusion» является платной и требует хороших знаний архитектуры от пользователей. В нашем исследовании зарубежные нейросети рассматриваться не будут.

### **Методика составления запроса для генерации изображения.**

Как было указано выше, целью исследования является разработка методики составления текстовых запросов для онлайн сервисов генерации изображений, позволяющей ускорить процесс получения корректных результатов конечным пользователем. С учетом того, что запрос *текстовый*, необходимо рассмотреть *лингвистический* аспект проблемы, включающий семантику (значение лексических единиц) и синтаксис (порядок слов) вводимого запроса/промпта. Профессионалы отмечают, что начинающий пользователь неизбежно сталкивается с проблемой непредсказуемости результата при генерации изображения нейросетью. Если запрос не понят НС, то изображение может оказаться совершенно отличным от того, какое ожидалось. Если идти путем проб и ошибок, то на получение нужного изображения может быть потрачено слишком много времени. Для того, чтобы нейросеть стала действительно удобным инструментом, необходимо разработать методику - ряд определенных требований, дающих стойкий верный результат.

Пользователь должен понимать, что естественный язык, которым пользуются люди при общении, содержит многие факторы, непонятные нейросети. К ним можно отнести полисемию (многозначность), идеоматические выражения или фразеологизмы (значение фразеологизма является переносным и не является суммой значение входящих в него лексических единиц), сленговые выражения, образные приемы (метафоры, эпитеты, гиперболы, метонимии и пр., в которых значение является переносным и требует образного мышления, свойственного только человеку). При формировании запроса все эти факторы должны быть исключены. Формулировки типа «грызть гранит науки», «рыбачить на косяке», «серебро волос», «голубые мундиры», «свинтить с уроков», «малиновый звон» неизбежно запутают нейросеть, принимающую каждую лексическую единицу запроса однозначно. Вопросами автоматизации обработки естественного языка (Natural Language Processing, NLP) и заполнения пробела между человеческим общением и компьютерным пониманием занимается специальная дисциплина - компьютерная лингвистика (Computational Linguistics, CL). Генерация текста относится к основным задачам компьютерной лингвистик. Чтобы избежать непонимания запроса к нейросети, необходимо формализовать естественно языковой запрос на основе ряда требований.

Формальное описание для промпта требует четкого, однозначного описания объекта, изображение которого необходимо получить. На первое место в запросе должен быть помещен сам объект, затем необходимо указать его существенные признаки, не перегружая при этом запрос излишней детализацией. Кроме этого простого требования к составлению промпта на настоящий момент накоплен большой опыт для разработки общей методики составления запроса для генерации изображения. Рассмотрим ее основные этапы:

1. Название объекта, явления, процесса (например, «торговый центр», «детский сад», «старик», «панда», «весна», «снегопад»);
2. Существенные признаки объекта (цвет, форма, возраст, состояние);
3. Если признак объекта обозначен не качественным, а относительным прилагательным (например: «медная кастрюля»), лучше употребить пост-позитивное определение («кастрюля из меди»);
4. Свойства объектов часто передают через предлоги («едущая на самокате девочка» или «девочка едет на самокате»);
5. Хороший результат дают запросы, где два объекта объединены с помощью дефиса («лев-царь», «ковер-самолет»);
6. Необходимо избегать запрос большого количества объектов, на промпт типа «десять машин на стоянке» нейросеть выдаст меньшее количество машин, при этом чем меньше объектов в запросе, тем выше качество полученного изображения (слов «много», «толпа» и т.п. также лучше избегать);
7. Употребление предлогов и слов с отрицательным значением приведет к обратному результату (при введении промпта «девушка без длинных локонов» нейросеть просто не обратит внимания на предлог «без» и на изображении наверняка будет девушка с длинными волосами. Для получения требуемого результата необходимо перефразировать запрос, опустив отрицание, например: «девушка с короткой стрижкой»);
8. Динамику объекту придаст введение в запрос глаголов «бежит», «смеется», «летит» и т.п.;
9. Необходимо помнить об отсутствии у нейросети образного мышления, свойственного человеку. Фразеологические выражения типа «грызть гранит науки» придется формализовать, перевести в язык машины, точно пояснив нейросети, что имеется в виду, например «студент, сидящий за столом, внимательно читает книгу» и т.п. В противном случае на изображении будет человек, сидящий рядом с камнем или грызущий камень, так как сеть понимает запрос прямолинейно и однозначно.

Кроме того, современные нейросети могут выполнить изображение в требуемом разрешении, с указанным уровнем детализации, в нужном стиле, на требуемом фоне [16, 17]. Следует отметить, что в мессенджере «Telegram» имеется возможность запуска чат-бота «Kandinsky 2.2». В нем при выборе генерации изображения по текстовому запросу после описания запрашиваемого контента сам чат-бот предлагает стиль генерируемого изображения или его качество (например, 4К) и соотношение сторон получаемого изображения (1:1, 16:9, 9:16 и т.д.), что немного упрощает решение поставленной задачи. Аналогично в приложении «Шедеврум» после написания промпта, если нажать на знак «?» в правом верхнем углу экрана, то появится подсказка с возможностью добавления визуальных эффектов, выбора стиля генерируемого изображения и т.п.

#### **Апробация предложенной методики генерации изображений.**

Определим эффективность разработанной методики на ряде следующих промптов:

- Промпт 1: «Панда сидит на дереве». Результаты, полученные по введенному Промпту 1 представлены на рисунке 1.
- Промпт 2: «Сидящая на дереве панда». Результаты, полученные по введенному Промпту 2 представлены на рисунке 2.
- Промпт 3: «Десять автомобилей в гараже». Результаты, полученные по введенному Промпту 3 представлены на рисунке 3.
- Промпт 4: «10 автомобилей в гараже». Результаты, полученные по введенному Промпту 4 представлены на рисунке 4.



- Промпт 5: «3 автомобиля в гараже». Результаты, полученные по введенному Промпту 5 представлены на рисунке 5.
- Промпт 6: «Девушка без длинных локонов». Результаты, полученные по введенному Промпту 6 представлены на рисунке 6.
- Промпт 7: «Девушка с короткой стрижкой». Результаты, полученные по введенному Промпту 7 представлены на рисунке 7.
- Промпт 8: «Студент грызет гранит науки». Результаты, полученные по введенному Промпту 8 представлены на рисунке 9.
- Промпт 9: «Студент, сидящий за столом, внимательно изучает книгу». Результаты, полученные по введенному Промпту 9 представлены на рисунке 9.

Все промпты представляли собой только текстовые запросы описания объектов, явлений или процессов. Никакие фильтры, настройки цветности, стили и дополнительные эффекты в промптах не указывались ни для НС «Шедеврум», ни для НС «Kandinsky 2.2». Было проведено порядка 15 итераций по каждому промпту, что обеспечивает корректность результатов, полученных в ходе эксперимента.

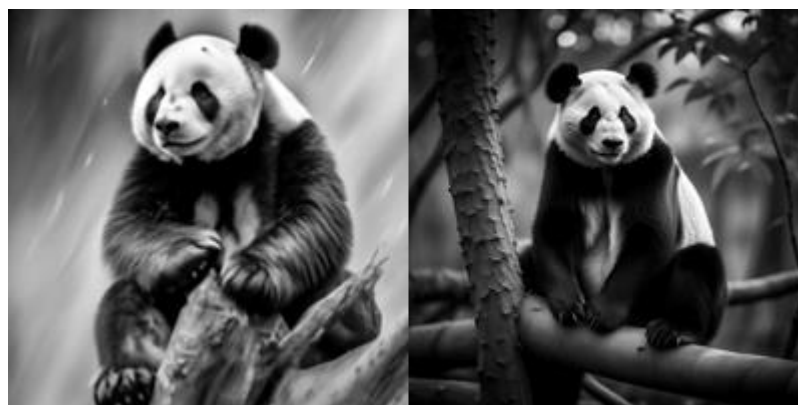


Рисунок 1. Результаты, полученные по введенному Промпту 1 (слева – результат НС «Шедеврум», справа – результат НС «Kandinsky 2.2»)



Рисунок 2. Результаты, полученные по введенному Промпту 2 (слева – результат НС «Шедеврум», справа – результат НС «Kandinsky 2.2»)

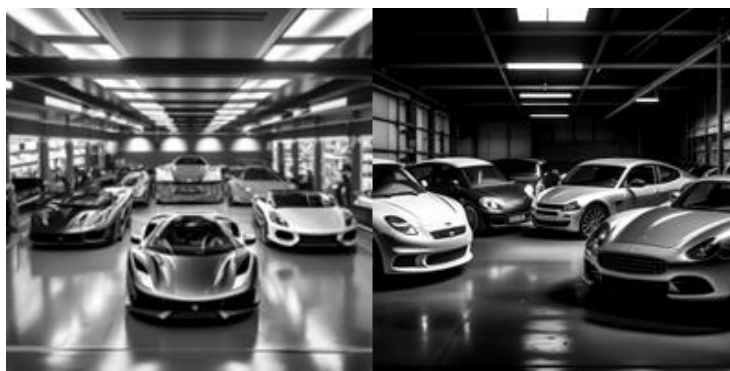


Рисунок 3. Результаты, полученные по введенному *Промпту 3* (слева – результат НС «Шедеврум», справа – результат НС «Kandinsky 2.2»)



Рисунок 4. Результаты, полученные по введенному *Промпту 4* (слева – результат НС «Шедеврум», справа – результат НС «Kandinsky 2.2»)



Рисунок 5. Результаты, полученные по введенному *Промпту 5* (слева – результат НС «Шедеврум», справа – результат НС «Kandinsky 2.2»)



Рисунок 6. Результаты, полученные по введенному *Промпту 6* (слева – результат НС «Шедеврум», справа – результат НС «Kandinsky 2.2»)



Рисунок 7. Результаты, полученные по введенному *Промпту* 7 (слева – результат НС «Шедеврум», справа – результат НС «Kandinsky 2.2»)



Рисунок 8. Результаты, полученные по введенному *Промпту* 8 (слева – результат НС «Шедеврум», справа – результат НС «Kandinsky 2.2»)



Рисунок 9. Результаты, полученные по введенному *Промпту* 9 (слева – результат НС «Шедеврум», справа – результат НС «Kandinsky 2.2»)

Как видно из полученных результатов, при запросе генерации *несложных объектов* (*Промпты* 1 и 2) обе нейросети выдали качественный результат. *Большое количество* запрашиваемых объектов приводит к ошибке, причем неважно, вводится ли числительное словом «десять машин на стоянке» или цифрой. В обоих случаях количество объектов отличается от ожидаемого, а их качество низкое, имеются *графические дефекты* изображения машин. При этом промпт с *небольшим количеством* объектов «Три машины на стоянке» выдает *верное и качественное* изображение. Промпты с *отрицательными частицами и предлогами* выдают результат *прямо противоположные* запрашиваемому. На всех сгенерированных изображениях по запросу «Девушка без длинных локонов» мы видим девушек с длинными локонами. Лишь *перифраз* »Девушка с короткой стрижкой» понимается нейросетью верно. Такого же уточнения и *формализации* требуют запросы, содержащие *идеоматические* выражения.

### Заключение.

В ходе проведенного исследования были выявлены следующие результаты: разработанная методика составления запросов к нейросетевым сервисам «Шедеврум» и «Kandinsky 2.2» позволяет в короткий промежуток времени получить требуемый корректный результат. Если при простых промптах разница в естественно языковом и формализованном согласно предложенной методике запросах не так очевидна, то в случаях с отрицательными частицами и предложениями, с относительными прилагательными, в запросах с большим количеством запрашиваемых объектов, с использованием абстрактных понятий и образных выражений предложенная методика составления запросов продемонстрировала свою эффективность. В перспективе предполагается развитие предложенной методики в условиях развивающихся возможностей современных нейросетевых сервисов.

### СПИСОК ЛИТЕРАТУРЫ

1. *M.G. Gorodnichev, M.D. Gromov, K.A. Polyantseva, M.S. Moseva.* Research and Development of a System for Determining Abnormal Human Behavior by Video Image Based on Deepstream Technology // 2022 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), St. Petersburg, Russian Federation, 2022, pp. 1-9, DOI: 10.1109/WECONF55058.2022.9803767.
2. *M.G. Gorodnichev, K.A. Dzhabrailov, K.A. Polyantseva, R.A. Gematudinov.* On Automated Safety Distance Monitoring Methods by Stereo Cameras // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2020, pp. 1-8, DOI: 10.1109/IEEECONF48371.2020.9078616.
3. *M.G. Gorodnichev, R.A. Gematudinov, K.A. Dzhabrailov, T.D. Potapchenko.* The Concept of an Automated Weight and Size Control System for Measuring the Mass of Freight Vehicles in a Traffic Flow (Weight-In-Motion) // 2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Russia, 2019, pp. 1-5, DOI: 10.1109/SYNCHROINFO.2019.8814120.
4. *O.I. Sheluhin, D.V. Kostin, M.G. Gorodnichev.* Monitoring Anomalous States of Computer Systems by Intellectual Analysis of Data of System Journals // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2020, pp. 1-6, DOI: 10.1109/IEEECONF48371.2020.9078632.
5. *K.A. Polyantseva, M.G. Gorodnichev, M.S. Moseva, T.D. Potapchenko.* On the Applicability of Neural Networks in the Tasks of Detecting Dangerous Movement // 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), 2019, pp. 1-4, doi: 10.1109/WECONF.2019.8840654.
6. *M.G. Gorodnichev, K.A. Polyantseva, M.S. Moseva, M.V. Yashina.* On Some Methods for Correcting Accelerometer and Gyroscope Data Using Machine Learning Algorithms // 2019 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS), 2019, pp. 186-191, doi: 10.1109/ITQMIS.2019.8928397.
7. *M.S. Moseva, M.G. Gorodnichev, K.A. Polyantseva, G.G. Vlasov, M.D. Gromov.* Development of a System for Fixing Road Markings in Real Time // 2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Arkhangelsk, Russian Federation, 2022, pp. 1-7, DOI: 10.1109/SYNCHROINFO55067.2022.9840971.
8. *Леохин Ю.Л., Фатхулин Т.Д.* Оценка возможности предоставления гарантированной скорости передачи данных в программно-конфигурируемой оптической сети // Вестник Рязанского государственного радиотехнического университета. – 2020. – № 71. – С. 45-59. – DOI 10.21667/1995-4565-2020-71-45-59. – EDN GQTGUP.

- 
9. *D. Perepelkin, T. Nguyen.* Research of Multipath Routing Processes in Software Defined Networks Based on Ant Colony Optimization // 2022 11-th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2022, pp. 1-6, DOI: 10.1109/MECO55406.2022.9797090.
  10. *Перепелкин Д.А., Нгуен В.Т.* Исследование и анализ процессов многопутевой маршрутизации и балансировки потоков данных в программно-конфигурируемых сетях на основе генетического алгоритма // Вестник Рязанского государственного радиотехнического университета. – 2022. – № 79. – С. 31-48. – DOI 10.21667/1995-4565-2022-79-31-48. – EDN XGSYWX.
  11. *Перепелкин Д.А., Фам А.М.* Математические модели планирования упорядоченного набора операций для распределения разнородных ресурсов в промышленных телекоммуникационных сетях // Вестник Рязанского государственного радиотехнического университета. – 2022. – № 79. – С. 56-67. – DOI 10.21667/1995-4565-2022-79-56-67. – EDN BMTQGM.
  12. *Перепелкин Д.А., Анисимов К.В.* Разработка архитектуры и системы нечетких метрик каналов связи программно-конфигурируемой сети устройств Интернета вещей // Вестник Рязанского государственного радиотехнического университета. – 2022. – № 80. – С. 53-66. – DOI 10.21667/1995-4565-2022-80-53-66. – EDN UPDKKO.
  13. *E.G. Kukhareno, I.A. Korkunov, M.G. Gorodnichev, T.U. Salutina.* On the Introduction of Digital Economics in the Transport Industry // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2019, pp. 1-5, DOI: 10.1109/SOSG.2019.8706797.
  14. 10 примеров использования ChatGPT и Midjourney в бизнесе и не только [Электронный ресурс]: // Обзор функционала и проблем популярных нейросетевых сервисов. – Режим доступа: [https://www.rbc.ru/spb\\_sz/11/06/2023/6483048b9a794751683](https://www.rbc.ru/spb_sz/11/06/2023/6483048b9a794751683)
  15. 574bf, свободный. – Загл. с экрана. (дата обращения 09.10.2023).
  16. *Митрофанов А.О., Степанов М.Н., Фатхулин Т.Д.* Анализ нейросетевых методов генерации изображения по текстовому запросу // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2022. – № 1. – С. 19-23. – EDN CWRLQA.
  17. Как правильно составлять запросы для нейросетей: формулы, шаблоны и примеры [Электронный ресурс]: // Описание способов составления запросов к нейронным сетям. – Режим доступа: <https://smmplanner.com/blog/kak-pravilno-sostavliat-zaprosy-dlia-nejrosietiei-formuly-shablony-i-primiery/>, свободный. – Загл. с экрана. (дата обращения 09.10.2023).
  18. Как формулировать запросы для нейросети [Электронный ресурс]: // Описание способов составления запросов к нейронным сетям для генерации изображений. – Режим доступа: [https://pikabu.ru/story/kak\\_formulirovat\\_zaprosyi\\_dlya\\_neyroseti\\_9980895](https://pikabu.ru/story/kak_formulirovat_zaprosyi_dlya_neyroseti_9980895), свободный. – Загл. с экрана. (дата обращения 09.10.2023).
  19. «Яндекс» представил нейросеть «Шедеврум» для превращения текста в изображения, и выпустил для неё приложения [Электронный ресурс]: // Описание функциональных возможностей нейросетевого сервиса «Шедеврум». – Режим доступа: <https://3dnews.ru/1084572/yandeks-predstavil-neyroset-shedevrum-dlya-generatsii-izobrazheniy-i-eyo-prilogeniya>, свободный. – Загл. с экрана. (дата обращения 09.10.2023).
  20. Новая нейросеть Kandinsky 2.1 от «Сбер» создает уникальные изображения на нескольких языках включая русский [Электронный ресурс]: // Описание функциональных возможностей нейросетевого сервиса «Kandinsky 2.1». – Режим доступа: <https://dzen.ru/a/ZCхXuqhnwGКCamvF>, свободный. – Загл. с экрана. (дата обращения 09.10.2023).

## МОБИЛЬНОЕ УСТРОЙСТВО НА НЕЙРОСЕТИ ДЛЯ ПОСТРОЕНИЯ КАРТЫ МЕСТНОСТИ В ГРАФИЧЕСКОМ ИНТЕРФЕЙСЕ

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: мобильное устройство, Arduino, микроконтроллер, нейронная сеть, карта местности

Данный проект реализует последовательное движение робота внутри закрытой территории для построения карты ее местности, которая может быть использована для проведения работ, требующих знания о расположенных препятствиях внутри зоны исследования. Устройство работает на базе платы Arduino Uno. Программирование микроконтроллеров Arduino на процессоре фирмы Atmel выполняется в среде IDE на языке программирования C++. Управление роботом реализовано с помощью обученной нейронной сети. Входные данные для нейросети собираются на основе показаний трех датчиков расстояния и трех датчиков черной линии.

М.М. Frolova, P.V. Lobzenko

## A MOBILE DEVICE ON A NEURAL NETWORK FOR BUILDING A TERRAIN MAP IN A GRAPHICAL INTERFACE

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: mobile device, Arduino, microcontroller, neural network, terrain map

This project implements the sequential movement of the robot inside a closed area to build a map of its terrain, which can be used to carry out work that requires knowledge of the obstacles located inside the study area. The device works on the basis of the Arduino Uno board. Programming of Arduino microcontrollers on an Atmel processor is performed in the IDE in the C++ programming language. Robot control is implemented using a trained neural network. The input data for the neural network is collected based on the readings of three distance sensors and three black line sensors.

В настоящее время развитие робототехники привело к активному росту интереса к мобильным роботам, предназначенным для решения широкого круга задач. В результате популяризации робототехнических средств, задача о построении схемы замкнутого пространства с препятствиями, а также позиционирование робота в пространстве представляют большой интерес для современного мира. Наличие схем препятствий позволяет мобильным устройствам самостоятельно принимать решение о дальнейшем передвижении, поэтому построение схематической карты необходимо для обеспечения автономности мобильным системам.

Для проведения тестов и моделирования задачи используется белый баннер с черной разметкой. Он выступает в роли подстилающей поверхности, по которой будет передвигаться мобильное устройство. Черная разметка имитирует потенциально опасные зоны для робота, будь то провалы, неровности на поверхности, температурные зоны и т.д. Также в роли препятствия могут выступать объемные объекты, превосходящие робота по габаритам.

Программа микроконтроллера мобильного устройства реализует трехслойную нейросеть обратного распространения с прямыми связями [1]. Опираясь на ее выходные

данные, формируются варианты движения мобильного устройства. Нейросеть состоит из трех видов слоев нейронов – входные, скрытые и выходные. Во входном слое располагается 4 нейрона, три из которых принимают конкатенируемые данные с датчиков препятствий, а оставшийся четвертый нейрон – нейрон состояния, на который поступает код, отвечающий за ориентацию в пространстве. В скрытом слое нейронной сети происходит большинство вычислений, в нем расположены 8 нейронов. Выходной слой состоит из двух нейронов. Такое количество нейронов на выходе обусловлено количеством разрядов в двоичном представлении числа вариантов движения робота. Обучение нейросети происходит на заранее отобранных паттернах данных, которые в совокупности являются обучающей выборкой.

Передача данных для построения карты местности происходит по протоколу Bluetooth [2]. На каждом шаге мобильное устройство (Master) с помощью Bluetooth модуля передает данные с датчиков на другой микроконтроллер (Slave), подсоединенный к компьютеру с включенным графическим интерфейсом [3]. Реализовать связь между двумя Bluetooth модулями позволяет прошивка с помощью AT-команд.

В качестве базы для мобильного устройства выступает плата Arduino Uno, в основе которой лежит микроконтроллер ATmega 328P. Также, в конструкции робота используется колесная платформа с двумя приводами, Bluetooth модуль HC-05 и шесть датчиков для обнаружения препятствий – три инфракрасных датчика черной линии и три ультразвуковых датчика расстояния. К плате Arduino Uno подсоединяется три платы расширения: плата для управления приводами, плата питания и плата расширения подключений. Данные с мобильного устройства передаются на второй микроконтроллер с таким же Bluetooth модулем HC-05, который в свою очередь передает эти данные с помощью последовательного COM-порта на компьютер для отрисовки карты территории. Принципиальная схема мобильного робота и платы, принимающей данные, представлена на рисунке 1.

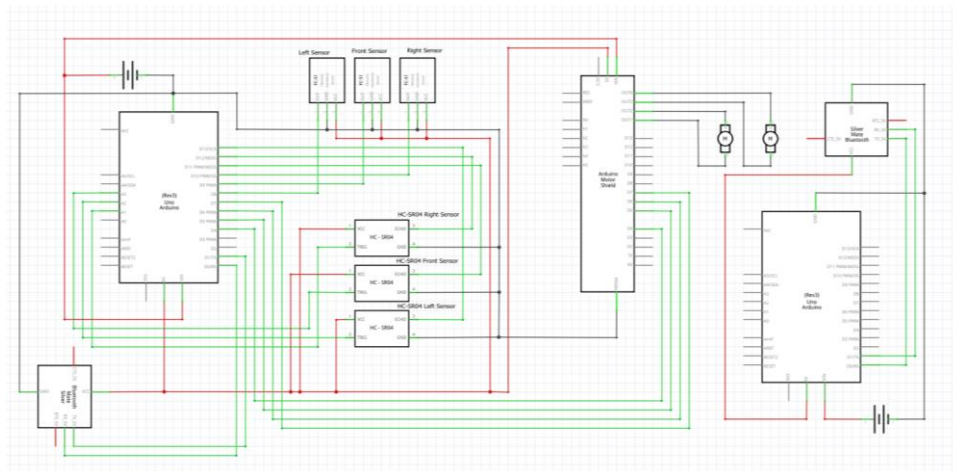


Рисунок 1. Принципиальная схема мобильного робота

Движение мобильного устройства выполняется пошагово. Длина одного шага равна диаметру колесной платформы робота. Карта местности представляет собой матрицу бинарных чисел, где 0 обозначает свободный для робота проезд, а 1 – препятствие на поверхности передвижения или объемный объект. Каждый элемент матрицы карты – это сегмент абстрактной сетки, которая делит территорию на безопасные и небезопасные зоны. Физически один сегмент представляет собой квадрат, сторона которого также равна диаметру колесной платформы робота или длине одного шага. Передвижение робота осуществляется «змейкой». Чтобы начать исследование территории, робота устанавливают в любой край карты. Размерность карты устанавливается в программе прошивки, опираясь на приближенные измерения длины и





---

## Листинг 1. Фрагмент скетча: сбор и отправка данных в нейросеть

```
void loop() {
  l10=digitalRead(8);
  l12=digitalRead(9);
  l13=digitalRead(10);

  vectorIn[0]=l10||imp(trigL,echoL);
  vectorIn[1]=l12||imp(trigF,echoF);
  vectorIn[2]=l13||imp(trigR,echoR);
  vectorIn[3]=dir;

  if (bufer){
    if (((dir==1) && watch(trigL, echoL, 8))||(dir==0) &&
watch(trigR, echoR, 10))){bufer++;}
    else{bufer = 0;}
  }
  /*ПЕРЕДАЧА ДАННЫХ В КАРТУ*/
  upr=netWork();

  Serial.print(vectorIn[0]);
  Serial.print(" ");
  Serial.print(vectorIn[1]);
  Serial.print(" ");
  Serial.print(vectorIn[2]);
  Serial.print(" ");
  Serial.print(vectorIn[3]);
  Serial.print(" ");
  Serial.println(upr);
}
```

Разработанное мобильное устройство имеет следующие преимущества:

- управление устройством осуществляется в автоматическом режиме;
- нейросеть не требует большого количества нейронов, что облегчает ее обучение;
- за счет выбранной модели движения экономится память в микроконтроллере;
- платы расширения для модели Arduino, используемой в проекте, обеспечивают удобный форм-фактор.

## СПИСОК ЛИТЕРАТУРЫ

1. Фролова М.М., Иванов А.Н., Лобзенко П.В. Прототип микроконтроллерного
2. Планетохода на нейросети // «ТРУДЫ СЕВЕРО-КАВКАЗСКОГО ФИЛИАЛА МОСКОВСКОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА СВЯЗИ И ИНФОРМАТИКИ» - 2023г.
3. Связываем две Arduino между собой с помощью bluetooth модулей. URL: <https://dzen.ru/a/ХуAUgcrquxjn8w7> (дата обращения 12.10.2023).
4. Arduino Two Way Communication Via Bluetooth (HC-05). URL: <https://www.instructables.com/Arduino-Two-Way-Communication-Via-Bluetooth-HC-05/> (дата обращения 14.10.2023)
5. Лескин К.А. Мобильная система для оптимального построения 2-D схемы замкнутого пространства с препятствиями на МК Arduino. URL:

- 
- <https://nauchkor.ru/pubs/mobilnaya-sistema-dlya-optimalnogo-postroeniya> (дата обращения 14.10.2023).
6. Visualization with Arduino and Processing. URL: <https://www.arduino.cc/education/visualization-with-arduino-and-processing> (дата обращения 17.10.2023)

**П.И. Ремигин, П.В. Лобзенко**

## **СЕТЕВОЕ ПРИЛОЖЕНИЕ ДЛЯ СЛУЖБЫ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: сетевое приложение, Visual Studio, ASP NET, базы данных.

Создано приложение для информационной поддержки администратора отдела технической поддержки предприятия. Приложение имеет удобную компоновку и размещается в сети предприятия. Приложением можно воспользоваться с помощью простого web браузера и оно содержит базу данных.

**P.I. Remigin, P. V. Lobzenko**

## **NETWORK APPLICATION FOR TECHNICAL SUPPORT SERVICE**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: network application, Visual Studio, ASP NET, databases.

An application has been created to provide information support to the administrator of the enterprise technical support department. The application has a convenient layout and is hosted on the enterprise network. The application can be used using a simple web browser and contains a database.

В настоящее время, специализированные программные продукты (ПП) для автоматизации рабочих мест создаются в 2-х вариантах- одно или многопользовательские, а также основанные на клиент-серверных структурах баз данных (БД) или на использовании БД, встроенных в офисные пакеты (например Access от Microsoft Office) по [1, 2].

Версии ПП, использующие сторонние базы данных, где, как обычно, присутствуют серверная и клиентская части [3, 4], стоят, обычно, дороже из-за необходимости иметь на рабочих местах дополнительное программное обеспечение (ПО) (в данном случае, необходимы системы управления базами данных (СУБД)).

Безусловно, использование открыто распространяемого ПО в качестве СУБД является сейчас все чаще избираемым путем экономного оснащения рабочих мест, что значительно снижает затраты на их оснащение.

Поэтому, поставлена задача разработать приложение и базу данных для автоматизированного учета и хранения информации по заявкам и выполненным работам для Технического отдела крупного государственного предприятия.

В силу того, что одной из главных задач технического отдела является реализация, установка и сервисное обслуживание компьютерной техники, поэтому, целью

бакалаврской работы является разработка программного обеспечения рабочего места менеджера отдела сопровождения компании.

Созданный ПП должен быть нацелен на улучшение хранения и обработки информации посредством учета заявок, выполненных работ, а также ведения документации в электронном виде.

Это обусловлено, во-первых, тем, что вся информация о заказах, клиентах, об исполнении заявок и т.п. должна быть, что называется «под рукой», чтобы вовремя выполнить запланированные работы или вмешаться в ход их выполнения.

Во-вторых, оперативность в приеме, поиске заявок, а также полнота информации, составляемой для клиентов о ходе их выполнения, делают обслуживание эффективным.

Для достижения поставленной цели решаются следующие задачи:

- сбор необходимой информации для построения модели данных задачи;
- разработка структуры данных задачи;
- подбор программного обеспечения для реализации модели базы данных и ее программной оболочки;
- разработка пользовательского интерфейса программной оболочки базы данных.

ПП создан с использованием современных инструментальных средств, разработки, таких как, интегрированные среды программирования и системы управления базами данных.

Приложение построено на использовании Windows Forms (рисунок 1).

The image shows a screenshot of a Windows Forms application. At the top, there is a button labeled "Добавить сотрудника". Below it is a table with two columns: "ФИО пользователя" and "Должность". The table contains the following data:

Петровский М.В.	Руководитель
Прутская К.Л.	бухгалтер
Верещагина Л.К.	бухгалтер
Ижевская К.Л.	зам. руководителя
Петровский М.В.	Руководитель

Below the table is a caption: "Добавить пользователя (все поля должны быть заполнены)".

Below the caption are four input fields labeled "ФИО", "Должность", "Отдел", and "Пароль".

Below the input fields are two buttons: "Добавить" and "Меню".

Below the buttons is a table with the following columns: "№.№", "ФИО", "Должность", "№ отдела", "Пароль", and "Действия". The table contains the following data:

№.№	ФИО	Должность	№ отдела	Пароль	Действия
3	Римский П.Н.	директор	1		<a href="#">Правка</a> <a href="#">Удалить</a>
4	Прутская К.Л.	бухгалтер	2	333	<a href="#">Правка</a> <a href="#">Удалить</a>
9	Петровский М.В.	Руководитель отдела	2	1221	<a href="#">Правка</a> <a href="#">Удалить</a>
12	Веринская М.В.	бухгалтер	2	111	<a href="#">Правка</a> <a href="#">Удалить</a>
13	Ижевская К.Л.	зам. руководителя отдела	2	591	<a href="#">Правка</a> <a href="#">Удалить</a>
14	Верещагина Л.К.	бухгалтер	2	753	<a href="#">Правка</a> <a href="#">Удалить</a>

Рисунок 1. Типовые формы приложения

Т.к., возможно размещение приложения на открытых сетевых ресурсах, то оно должно быть оснащено входом по логину и паролю. Алгоритм доступа к интерфейсу приложения включает заполнение логина и пароля на стартовой форме приложения, процедуру ввода данных и сверку их с данными, записанными в базе данных приложения.

Приложение разработано на языке C# и состоит из набора классов, каждый из которых, реализует взаимодействие с таблицами базы данных (рисунок 2).

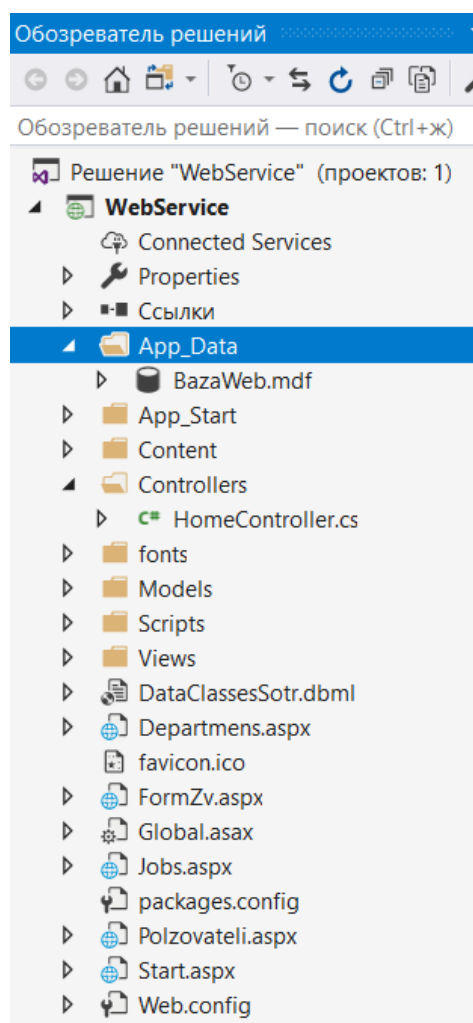


Рисунок 2. Состав приложения

Платформа ASP.NET, на базе которой разработан продукт, представляет собой набор библиотек и инструментов приблизительно таких же как и FrameWork для разработки web сайтов и приложений [4]. Это удобный инструмент для использования технологии MVC (model - view — controller). Т.е., в разработке приложение делится на три компонента:

- контроллер (controller) — класс, занимающийся связью базы данных с пользователем и обработкой текущей информации из базы данных;
- представление (view) — класс, обеспечивающий пользовательский интерфейс;
- модель (model) — класс для описания логики данных приложения.

Как любое приложение, содержащее интерфейсные формы, это приложение снабжено обработчиками событий. Типовой обработчик события нажатия на кнопку «Добавить» представлен в листинге 1.

---

### Листинг 1. Типовой обработчик события нажатия на кнопку «Добавить»

```
protected void Button1_Click(object sender, EventArgs e)
{
    DataClassesSotrDataContext db = new DataClassesSotrDataC-
ontext(); // создание экземпляра модели данных проекта
    Klientu kl = new Klientu(); // создание экзем-
плярa таблицы Klientu БД

    //Код добавления пользователя
    do
    {
        if (TextBox1.Text != "" && TextBox2.Text != ""
&& TextBox3.Text != "" && TextBox4.Text != "") // ввод не-пустых
данных
        {
            kl.Doljnost = TextBox2.Text; //
заполнение полей таблицы из текстовых полей
            kl.FioKl = TextBox1.Text;
            kl.NomOtd = int.Parse(TextBox3.Text);
            kl.Password = TextBox4.Text;

            db.Klientu.InsertOnSubmit(kl); //
экземпляр слушателя изменения данных в таблице Klientu БД
            db.SubmitChanges();

            GridView1.DataSourceID = "";
            GridView1.DataSource = db.Klientu; //
отображение содержимого таблицы в GridView
            GridView1.DataBind();
            //Label3.Text = "";
            Response.Redirect("/Polzovатели.aspx");
// отображение формы в Explorer
            break;
        }
    } while (true);
}
```

Разработанное приложение обладает:

1. Эффективной архитектурой.
2. Автоматизацией рутинных функций на рабочем месте.
3. Реализацией алгоритм отправки заявки на техническое обслуживание аппаратуры.
4. Информацией по выполняемым заявкам.
5. Понятным интерфейсом.

### СПИСОК ЛИТЕРАТУРЫ

1. Использование программного обеспечения в малом бизнесе. URL: <http://www.good-reklama.ru/upravlenie/184.html>. (дата обращения: 16.10.2023).
2. Илюхин И.В. Основные направления использования информационных систем в управлении предприятиями. URL: <http://cyberleninka.ru/article/n/osnovnyue>

---

napravleniya-ispolzovaniya-informatsionnyh-sistem-v-upravlenii-predpriyatiyami. (дата обращения: 16.10.2023).

3. Категории программных продуктов: «Раскрутка и реклама». URL: <http://www.softwizard.ru/catalog/categories/network-programs/advertising-software>. (дата обращения: 16.10.2023).
4. Иванова Г.С. Технология программирования: Учебник для вузов. - М.: Издательство МГТУ им. Н.Э. Баумана, 2002. - 320 с.

**Л.В. Пузырная, П.В. Лобзенко**

## **ОПТИМИЗАЦИЯ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ С ПОМОЩЬЮ МЕТОДА ВИРТУАЛИЗАЦИИ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: виртуализация рабочих столов, виртуализация серверной структуры, оптимизация IT-инфраструктуры, отказоустойчивый кластер, виртуальная машина, гипервизор Microsoft Server Hyper-V.

В статье разработана информационная система предприятия с использованием виртуализации пользовательского интерфейса.

**L.V. Puzyrnaya, P.V. Lobzenko**

## **OPTIMIZATION OF AN ENTERPRISE COMPUTER NETWORK USING THE VIRTUALIZATION METHOD**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Key words: desktop virtualization, server structure virtualization, IT infrastructure optimization, failover cluster, virtual machine, Microsoft Server Hyper-V hypervisor.

The article develops an enterprise information system using user interface virtualization.

Задача оптимизации вычислительной системы возникает по мере роста пользовательских станций в ней. В настоящее время вычислительные системы, практически всех, предприятий, оснащенных персональными компьютерами (ПК), возникает необходимость в оптимизации структуры вычислительной системы.

В связи с ростом потребности в вычислительных мощностях и скорости обработки информации, в организации количество пользовательских станций и приемо-передающей аппаратуры значительно возросло. Так, появились серверные шкафы, которые вмещали в себя десяток серверов, а далее и серверные комнаты, называемые узлами обработки информации (УОИ).

Поэтому, с увеличением количества оборудования в серверных комнатах, появился ряд серьезных проблем:

- сложность администрирования одним человеком большого количества узлов, что влечет понижение времени реакции на исправление возникающих неисправностей или на необходимую настройку системы;

- 
- увеличение количества узлов отказа, повышает шанс выхода из строя рабочего узла, что влечет к длительным простоям в работе организации;
  - нерациональное использование ресурсов сервера. До 70% ресурсов не используется сервером, и никогда не будет использовано, при выполнении им определенных ролей в вычислительной системе организации или ее филиала;
  - нерациональное использование дискового пространства при хранении информации. Более 40% дискового пространства не использовалось длительное время, либо вообще не могло быть заполнено теми данными, под которые этот раздел был назначен;
  - сложность сопровождения устаревшего программного обеспечения. Отсутствие кроссплатформенности, невозможность переноса на новое оборудование.

Для решения подобных задач уже достаточно давно разрабатываются виртуальные среды, которые позволяют связать физический узел, т.е. сервер как оборудование, с логической надстройкой таким образом, чтобы для исполняемых программ логическая среда была абсолютно прозрачной [1].

В таких системах программы могут взаимодействовать через виртуальные интерфейсы с физическими устройствами узла (ядрами процессора, оперативной памятью, устройствами ввода-вывода через разъемы, взаимодействия с физическими дисками).

Виртуализация открыла новую эру в области серверной инфраструктуры вычислительных сетей и хранения данных. Разработки в области виртуализации ведут известные крупные корпорации: Microsoft [2], VMware [3], Citrix [4]. Эти компании вкладывают огромные средства в новые разработки, методы виртуализации, и в расширение функционала, позволяющего расширить возможности одного человека, способного управлять целой инфраструктурой с помощью одного рабочего места через единый централизованный интерфейс. Этими компаниями был разработан функционал, позволяющий использовать ресурс физического узла на 99%, и использовать его настолько гибко, насколько это возможно в пределах физических характеристик.

В настоящее время все больше крупных компаний всего мира переходят на различные системы виртуализации. Так, крупнейший системный интегратор России, компания КРОК, внедрила несколько десятков крупнейших проектов по переносу ИТ-инфраструктуры в «облако» [5]. Среди этих проектов можно отметить создание платформы виртуальных машин, целью которого было создание инструмента, который позволил бы решить проблему быстрого выделения и перераспределения вычислительных ресурсов между существующими задачами высокой сложности (задачи ОАО «НефтеГаз»). Специалисты КРОК создали платформу, которая удовлетворяет бизнес-требованиям этих задач и обеспечивает высокую доступность ИТ-сервисов, их резервное копирование, мониторинг и защиту от несанкционированного доступа и несанкционированного воздействия. При проектировании системы была предусмотрена возможность ее расширения без потери качества обслуживания и устойчивости при тиражировании.

Такая отказоустойчивая платформа виртуальных машин может быть создана на аппаратной платформе производства HP с использованием программного обеспечения компании VMware.

Похожие решения используют службу единого каталога (Microsoft Active Directory) для аутентификации и идентификации пользователей и развернутые у генерирующей компании сетевые службы поддержки доменных имен и распределения адресов сети.

Внедрение аналогичных проектов значительно сокращает затраты на обслуживание ИТ-инфраструктуры, а также снижает риски простоя систем из-за нехватки вычислительных ресурсов.

Также, стоит отметить еще одного крупнейшего интегратора России, компанию Softline, который также ведет интенсивную работу с российскими компаниями по

---

переносу имеющихся вычислительных мощностей в виртуальную среду. Об этом говорят реализованные проекты, которые функционируют и выполняются все поставленные задачи [6].

На данный момент, системными администраторами предприятий, где парк ПК превышает 50 единиц тратится большое количество времени на ремонт вышедших из строя отдельных компонентов рабочих станций и серверной инфраструктуры, а также на логистику оборудования до места ремонта, либо сервисного центра. При нехватке физических ресурсов, организации тратят значительные средства на приобретение новых узлов, способствуя тому, что увеличение их количества ведет к высокой вероятности отказа работы оборудования.

Как правило в подобных ситуациях, отсутствует гибкость в управлении мощностями таких вычислительных структур. При необходимости увеличения производительности отдельных рабочих станций, обслуживающему персоналу требуется останавливать работу пользователей. В случаях, когда жизненный цикл работы оборудования подошел к концу, все данные вместе с операционной системой, драйверами невозможно перенести на новое оборудование при создании полного клона специализированными программными средствами.

Рассматриваемое в выпускной работе предприятие столкнулось с подобными проблемами. Поэтому, в работе предложено их решение посредством виртуализации серверной инфраструктуры и рабочих столов пользователей, которая решает большинство возникших задач, связанных с администрированием и сопровождением оборудования, позволяя высвободить людские ресурсы и сэкономить средства.

Это, в первую очередь, сокращает затраты на приобретение нового оборудования, которое, обычно, закупается с целью модернизации существующих серверов и систем хранения данных, увеличивая их емкость, мощность и производительность.

Система виртуализации серверов позволяет обеспечить кроссплатформенность приложений. При этом, обеспечивается использование виртуальной среды во всех физических серверах без их остановки.

Виртуализация рабочих столов позволяет, при необходимости, увеличивать пользователям вычислительные ресурсы без вскрытия системного блока и присутствия системного администратора на месте установки пользовательского компьютера, а также без остановки работы и перезагрузки операционной системы в критически важные моменты. Использование виртуальной среды позволяет преодолеть ограничения, связанные с трудностью переноса программ и данных между оборудованием различной конфигурации и архитектуры.

Современные системы конвертирования физической среды в виртуальную, позволяют не только перенести устаревшее программное обеспечение на современное оборудование без потери данных, но и даст возможность расширять вычислительные мощности, которыми было ограничено устаревшее оборудование.

Указанные виды виртуализации позволяют сократить расходы на электроэнергию путем сокращения физических узлов, потребляющих ее.

Реализация новой IT-инфраструктуры предприятия посредством внедрения системы виртуализации серверов и рабочих столов пользователей направлена:

- на повышение эффективности использования серверного оборудования;
- на снижение времени возникающих простоев вычислительной системы;
- на повышение скорости предоставления вычислительных ресурсов для новых задач;
- на увеличение централизации управления виртуальной инфраструктурой через единый интерфейс управления;
- на возможность выделять ресурсы хранения и вычислительные ресурсы из единой консоли;



- на ускорение поиска неисправностей и неоптимальных информационных узлов в виртуальной инфраструктуре;
- на возможность постоянного анализа эффективности использования существующей инфраструктуры и поиск возможностей ее повышения;
- на создание централизованного анализа большого объема неструктурированных данных от различных компонентов виртуальной инфраструктуры;
- на возможность значительно снизить затраты на электроэнергию.

Виртуальной средой управляет гипервизор Microsoft Hyper-V. Функция Microsoft Hyper-V изначально создавалась на основе новой микро-ядерной архитектуры (рисунок 1).

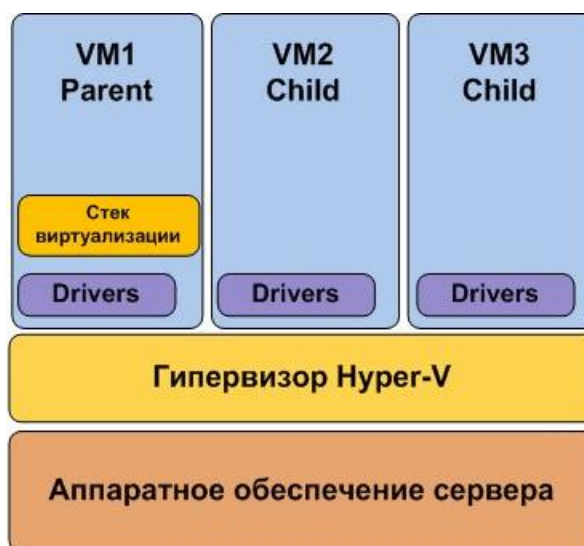


Рисунок 1. Архитектура виртуализации на базе гипервизора Microsoft Server Hyper-V

Гипервизор поддерживает разграничение по разделам. Раздел — это логическое разграничение, в котором работают гостевые операционные системы. Каждый экземпляр гипервизора должен иметь один родительский раздел, с запущенной операционной системой Windows Server 2019. Стек виртуализации запускается на родительском разделе (Parent) и обладает прямым доступом к аппаратным ресурсам устройства. Родительский раздел создает дочерние разделы (Child), на которых располагаются гостевые операционные системы. Дочерний раздел также может породить собственные дочерние разделы. Родительский раздел создает дочерние при помощи API интерфейса гипервизора, представленного в Microsoft Hyper-V.

Разработанная система обладает следующими преимуществами:

1. Централизованное администрирование.
2. Персонализация пользователей.
3. Экономия дискового пространства.
4. Автоматическое управление пулами виртуальных рабочих столов.

## СПИСОК ЛИТЕРАТУРЫ

1. Виртуальные машины дома и в бизнесе. URL: <http://www.ixbt.com/cm/virtualization-vm-home-business.shtml>. (дата обращения: 16.10.2023).
2. Microsoft. URL: <https://www.microsoft.com/en-us/server-cloud/solutions/virtualization.aspx>. (дата обращения: 16.10.2023).

- 
3. VMware. URL: <http://www.vmware.com/ru>. (дата обращения: 16.10.2023).
  4. Citrix. URL: <https://www.citrix.ru/>. (дата обращения: 16.10.2023).
  5. КРОК - системный интегратор. URL: <https://www.croc.ru/>. (дата обращения: 16.10.2023).
  6. Компания Softline – реализованные проекты. URL: <http://services.softline.ru/projects-filters>. (дата обращения: 16.10.2023).

**А.Б. Кожанов, П.В. Лобзенко**

### **КОМБИНИРОВАННАЯ CRM ОТДЕЛА ОБЕСПЕЧЕНИЯ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: комбинированная CRM, клиент-серверная архитектура, Visual Studio, ASP NET, база данных.

Создана CRM отдела снабжения предприятия. Система построена на основе сетевой разработки с базой данных.

**A.B. Kozhanov, P.V. Lobzenko**

### **COMBINED CRM OF THE SECURITY DEPARTMENT**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: combined CRM, client-server architecture, Visual Studio, ASP NET, database.

A CRM has been created for the enterprise's supply department. The system is built on the basis of network development with a database.

Разработанная CRM - Customer Relationship Management направлена на автоматизацию обработки заказов от филиалов компании.

Система удовлетворяет следующим требованиям:

- технически выполнена в форме web – разработки и размещается в сети компании;
- содержит функцию доступа посредством браузера с любых устройств, имеющих подключение к сети;
- реализованы функции учета, изменения и добавления следующих категорий: филиалы, поставки и накладные;
- реализован автоматический подсчет товарных остатков, доступных к заказу с учетом уже сделанных заказов;
- организованы 2 различные сессии: администратор и филиалы;
- схема и хранение данных в базе данных обеспечивает их целостность;
- интерфейс простой и понятным.

ПП, использующее сторонние базы данных, где, как обычно, присутствуют серверная и клиентская части, стоят, обычно, дороже из-за необходимости иметь на

рабочих местах дополнительное программное обеспечение (ПО) (в данном случае, необходимы системы управления базами данных (СУБД)).

Конечно, использование предустановленного ПО в качестве СУБД является сейчас все чаще избираемым путем экономного оснащения рабочих мест, что значительно снижает затраты на их оснащение.

Одной из основных характеристик используемого ПО сейчас рассматриваются его сетевые качества, т.е. на сколько оно используется в сети Интернет.

В этом отношении приложения разрабатываются и устанавливаются либо для мобильных устройств, либо имеют сайтовый вариант применения. Ко второму типу ПП относятся те, которые не требуют предустановки клиентской части на устройствах пользователей. Т.е., имея в распоряжении Интернет – соединение и любой из эксплореров можно использовать такое приложение, запущенное на определенном Интернет – ресурсе.

В качестве инструмента разработки используется язык C# и платформа ASP.NET, а редактором является Visual Studio [1,2]. Это удобные инструменты для использования технологии MVC (model - view — controller). Т.е., в разработке приложение делится на три компонента:

- контроллер (controller) — класс, занимающийся связью базы данных с пользователем и обработкой текущей информации из базы данных;
- представление (view) — класс, обеспечивающий пользовательский интерфейс;
- модель (model) — класс для описания логики данных приложения.

Реляционная база данных приложения представляет собой взаимосвязанные таблицы и реализована на встроенном Sql Server [3]. Состав ее модели показан на рисунке 1.

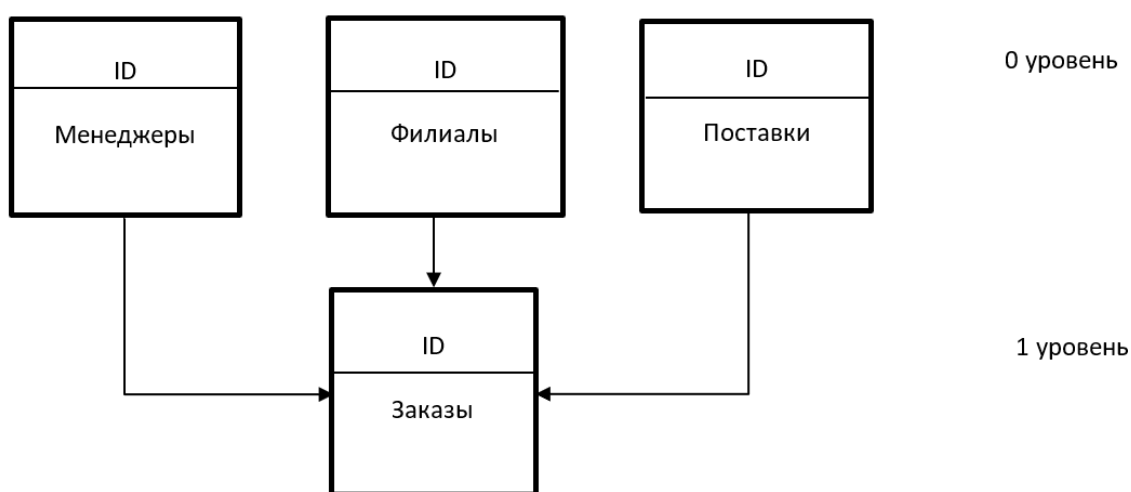


Рисунок 1 – Модель базы данных

Кроме стандартных запросов на добавление, удаление и редактирование, здесь реализовано снижение товарных остатков на величину зарезервированного товара в заказе. Это реализовано через считывание соответствующего поля таблицы Поставки и перезаписывание его, уменьшая на величину отложенного товара.

Программно это показано в соответствии с листингом 1.

```

Листинг 1. Фрагмент класса Postavky
numberTovar = int.Parse(TextBox3.Text);
tovZapas = int.Parse(arr[int.Parse(TextBox3.Text) - 1]); //
доступный остаток выбранного товара
ostatokTovar = tovZapas - int.Parse(TextBox4.Text);
string updateOstatok = "Update Tovar Set ZapasTovar= '" +
ostatokTovar + "' Where IdTovar='" + numberTovar + "'";
if (tovZapas >= int.Parse(TextBox4.Text))
// снижаем запас только, если он больше заказа
{using (SqlCommand cmd_update = new
SqlCommand(updateOstatok, conn1))
{cmd_update.ExecuteNonQuery();} }
else { Labell.Text = "Остаток меньше заказа. Заказ не
возможен"; }

```

Рабочая форма менеджера содержит необходимые данные для создания накладной на поставку товара (рисунок 2).

<u>№.№</u>	<u>Наименование</u>	<u>Цена</u>	<u>Текущий остаток</u>
1	Бульон Кари	45	850
2	Зеленая заправка	35	2000
3	Кетчуп Прованс	65	500
4	Конфеты Ив Роше	450	280
5	Печенье Шармэль	180	250
6	Масло слив. Слобода	140	3000
7	Печенье "Vig"	125	25

#### ЗАКАЗЫ

<u>№.№</u>	<u>№ ТП</u>	<u>№ Торг.точки</u>	<u>№ Товара</u>	<u>Кличество</u>	<u>Сумма заказа</u>	<u>Действия</u>
1	1	1	2	10	550	<a href="#">Правка</a> <a href="#">Удалить</a>
2	3	2	3	10	650	<a href="#">Правка</a> <a href="#">Удалить</a>
3	2	3	1	10	450	<a href="#">Правка</a> <a href="#">Удалить</a>
4	3	3	1	5	500	<a href="#">Правка</a> <a href="#">Удалить</a>
5	2	1	1	10	950	<a href="#">Правка</a> <a href="#">Удалить</a>
8	2	4	4	46	5000	<a href="#">Правка</a> <a href="#">Удалить</a>
9	2	3	6	50	17500	<a href="#">Правка</a> <a href="#">Удалить</a>
10	2	4	4	20	7000	<a href="#">Правка</a> <a href="#">Удалить</a>
11	2	4	4	20	7000	<a href="#">Правка</a> <a href="#">Удалить</a>
12	2	4	4	200	6600	<a href="#">Правка</a> <a href="#">Удалить</a>
13	7	3	7	75	7500	<a href="#">Правка</a> <a href="#">Удалить</a>

Рисунок 2. Форма для заказа

Разработанная CRM обладает следующими преимуществами:

- 
1. Реализует эффективный способ клиент-серверной системы.
  2. Обладает простым, понятным и удобным пользовательским интерфейсом.
  3. Реализует основные рутинные функции при формировании поставки.
  4. Полностью реализует алгоритм отправки заявки на доставку товаров.
  5. Предоставляет исчерпывающую информацию по выполняемым заявкам.

#### СПИСОК ЛИТЕРАТУРЫ

1. Джесс Либерти Программирование на C#. - Изд-во Символ – плюс: Москва, 2012.- 863 с.
2. Краткое описание Visual Studio. URL: <http://habrahabr.ru>. (дата обращения: 16.10.2023).
3. Справочное руководство по MySQL. URL: <http://www.mysql.ru/docs/man/Features.html>. (дата обращения: 16.10.2023).

**И.О. Зайцев, П.В. Лобзенко**

#### БАЗА ДАННЫХ АДМИНИСТРАТОРА ИТ КОМПАНИИ

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: сетевое приложение, клиент-серверная разработка, Visual Studio, ASP NET, база данных.

Создана база данных для автоматизации рабочего места администратора в компьютерной компании. Приложение отличается удобным доступом через web браузер с любого мобильного устройства, подключенного к сети Интернет и снабжено базой данных.

**I.O. Zaitsev, P.V. Lobzenko**

#### CAR SERVICE NETWORK DATABASE

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: network application, client-server development, Visual Studio, ASP NET, database.

A database has been created to automate the administrator's workplace in a computer company. The application is easy to access via a web browser from any mobile device connected to the Internet and is equipped with a database.

Главной задачей отдела сопровождения организации, для которого и разработано приложение, является реализация, установка и сервисное обслуживание компьютерной техники, поэтому, целью выпускной работы является разработка программного обеспечения рабочего места менеджера отдела сопровождения компании.

Созданный программный продукт (ПП) нацелен на улучшение хранения и обработки информации посредством учета заказов, выполненных работ, а также ведения документации в электронном виде. Это обусловлено, во-первых, тем, что вся информация

о заказах, клиентах, об исполнении заказов и т.п. должна быть, что называется «под рукой», чтобы вовремя выполнить запланированные работы или вмешаться в ход их выполнения. Во-вторых, оперативность в приеме, поиске заказов, а также полнота информации, составляемой для клиентов о ходе их выполнения, делают обслуживание эффективным.

Для достижения поставленной цели решены следующие задачи:

- сбор необходимой информации для построения модели данных задачи;
- разработка структуры данных задачи;
- подбор программного обеспечения для реализации модели базы данных и ее программной оболочки;
- разработка пользовательского интерфейса программной оболочки базы данных.

ПП создан с использованием современных инструментальных средств, разработки, таких как, интегрированные среды программирования и системы управления базами данных.

Т.о., возникает необходимость в автоматизации указанного бизнес – процесса, чтобы все данные хранились в общей сетевой базе и были доступны для совместного использования.

В качестве инструмента разработки используется язык C# и платформа ASP.NET, а редактором является Visual Syudio [1,2]. Это удобные инструменты для использования технологии MVC (model - view — controller). Т.е., в разработке приложение делится на три компонента:

- контроллер (controller) — класс, занимающийся связью базы данных с пользователем и обработкой текущей информации из базы данных;
- представление (view) — класс, обеспечивающий пользовательский интерфейс;
- модель (model) — класс для описания логики данных приложения.

Реляционная база данных приложения представляет собой взаимосвязанные таблицы и реализована на встроенном Sql Server [3]. Состав ее модели показан на рисунке 1.

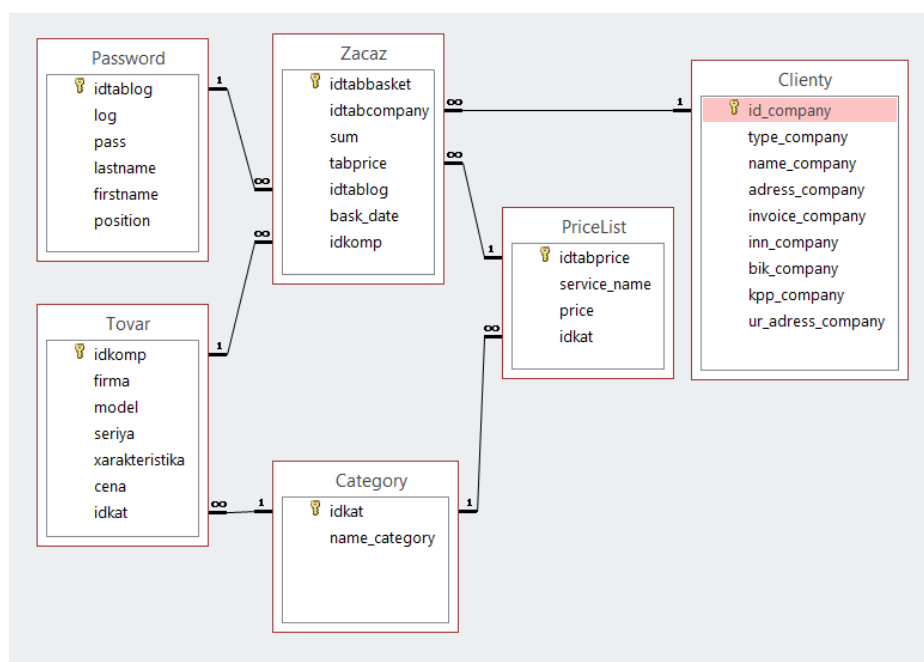


Рисунок 1. Модель базы данных

Созданное приложение включает несколько форм для выполнения заказа и для заполнения таблиц базы данных и главную форму (рисунок 2).

The screenshot shows a window titled "Журнал заказов товаров и услуг" (Journal of goods and services orders). It contains a table with the following columns: Тип (Type), Название (Name), Имя (Name), Фамилия (Surname), Должность (Position), Категория (Category), Услуга (Service), Цена услуги (Service Price), and Количество (Quantity). The table lists various orders for services like IP installation, network connection, and wall drilling, with details on the provider, price, and quantity.

Тип	Название	Имя	Фамилия	Должность	Категория	Услуга	Цена услуги	Количество
ООО	Кофе Интерн...	Владимир	Иванов	Программист	Услуга	Монтаж IP ка...	1800	4
ИП	Мельниченко ...	Владимир	Иванов	Программист	Услуга	Почасовая ра...	1000	4
ООО	Связь коннект	Владимир	Иванов	Программист	Услуга	Почасовая ра...	1000	6
ООО	Гвардейский	Владимир	Иванов	Программист	Услуга	Бурение стен ...	400	5
ООО	Гвардейский	Владимир	Иванов	Программист	Услуга	Обслуживание...	1000	8
ООО	Гвардейский	Владимир	Иванов	Программист	Услуга	Почасовая ра...	1000	8
ООО	Связь коннект	Владимир	Иванов	Программист	Услуга	Почасовая ра...	1000	3
ООО	Связь коннект	Владимир	Иванов	Программист	Услуга	Монтаж IP ка...	1800	2
ООО	Связь коннект	Владимир	Иванов	Программист	Услуга	Обслуживание...	1000	5
ИП	Брагов А.Л.	Владимир	Иванов	Программист	Услуга	Обслуживание...	1000	2
ИП	Меньшиков И.И.	Илья	Петров	Менеджер	Услуга	Обслуживание...	1000	3
ИП	Меньшиков И.И.	Илья	Петров	Менеджер	Услуга	Почасовая ра...	1000	4
ООО	Связь коннект	Илья	Петров	Менеджер	Услуга	Почасовая ра...	1000	4
ИП	Меньшиков И.И.	Илья	Петров	Менеджер	Услуга	Монтаж IP ка...	1800	2

Below the table, there is a sorting section labeled "СОРТИРОВАТЬ:" with dropdown menus for "По клиентам" and "По услугам", and a radio button for "Показать все".

Рисунок 2. Главная форма приложения

Разработанное приложение обладает следующими преимуществами:

1. Реализует эффективный способ клиент-серверной системы.
2. Обладает простым, понятным и удобным пользовательским интерфейсом.
3. Реализует основные рутинные функции продавца-товароведа.
4. Полностью реализует алгоритм отправки заявки на доставку товаров.
5. Предоставляет исчерпывающую информацию по выполняемым заявкам.

#### СПИСОК ЛИТЕРАТУРЫ

1. Джесс Либерти Программирование на C#. - Изд-во Символ – плюс: Москва, 2012.- 863 с.
2. Краткое описание Visual Studio. URL: <http://habrahabr.ru>. (дата обращения: 17.10.2023).
3. Справочное руководство по MySQL. URL: <http://www.mysql.ru/docs/man/Features.html>. (дата обращения: 17.10.2023).

**С.Э. Головинов, П.В. Лобзенко**

#### **АВТОЗАПОМИНАНИЕ НОВОГО МАТЕРИАЛА ПРИ ОБУЧЕНИИ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: обучающая программа, интерактивность, информационные технологии, дистанционное обучение.

Представлено разрешение проблемы формирования полноценного интерактивного пособия в среде объектно-ориентированного языка C#. Характерной, отличительной чертой исследования считается полноцикловый образ подачи материала вида «теория – практика – тест», что позволило обеспечить полностью самостоятельное изучение дисциплины.

## AUTO-STORING NEW MATERIAL WHEN LEARNING

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: training program, interactivity, information technologies, distance learning.

The resolution of the problems of forming a full-fledged interactive manual in the environment of the object-oriented language Delphi is presented. A characteristic distinctive feature of the study is the full-cycle image of the material of the "test-theory-practice-test" kind of material, which made it possible to provide a completely independent study of the discipline.

В наше время количество систем, предназначенных для обучения с использованием электронных форм передачи материала, неизменно увеличивается. Таким образом, в силу вступает новая тенденция обучения, основанная на развитии открытого, дистанционного образования, технологической основой которого являются информационные и телекоммуникационные технологии [1, 2]. Дистанционное обучение позволяет обучаться в своем темпе, исходя из личных потребностей в образовании. Поэтому, представленная разработка интерактивной обучающей программы по дисциплине «Технология программирования» является актуальной и востребованной.

В качестве языка программирования был выбран универсальный язык высокого уровня (ЯВУ) C# [3]. Он имеет возможность решения широкого класса задач, возможность работы с базами данных, простоту изучения.

Приложение построено на основе Forms, или их еще называют «Windows- Forms». При создании графического интерфейса пользователя (ГИП) происходит наследование класса TForm с обширным набором шаблонов создания ГИП. Далее, основная форма приложения наполняется необходимыми средствами управления и отображения материала (листинг 1).

Листинг 1. Фрагмент заполнения основной формы приложения

```
TForm1 = class(TForm)
    GroupBox1: TGroupBox;
    TreeView1: TTreeView;
    WebBrowser1: TWebBrowser;
    MainMenu1: TMainMenu;
    N1: TMenuItem;
    N2: TMenuItem;
    N3: TMenuItem;
    Splitter1: TSplitter;
```

Контент, наполняющий приложение, представляет файлы в формате html, в которых организовано ссылочное связывания блоков изучаемого материала. Это является очень удобным, т.к. материалы для изучения хранятся в отдельной директории и могут быть легко модифицированы, при необходимости.

Одним из главных достоинств обучающей программы является большое количество гиперссылок, которые позволяют после изучения теоретических основ перейти к практическим работам и при необходимости вернуться в необходимую часть лекции (рис. 1).



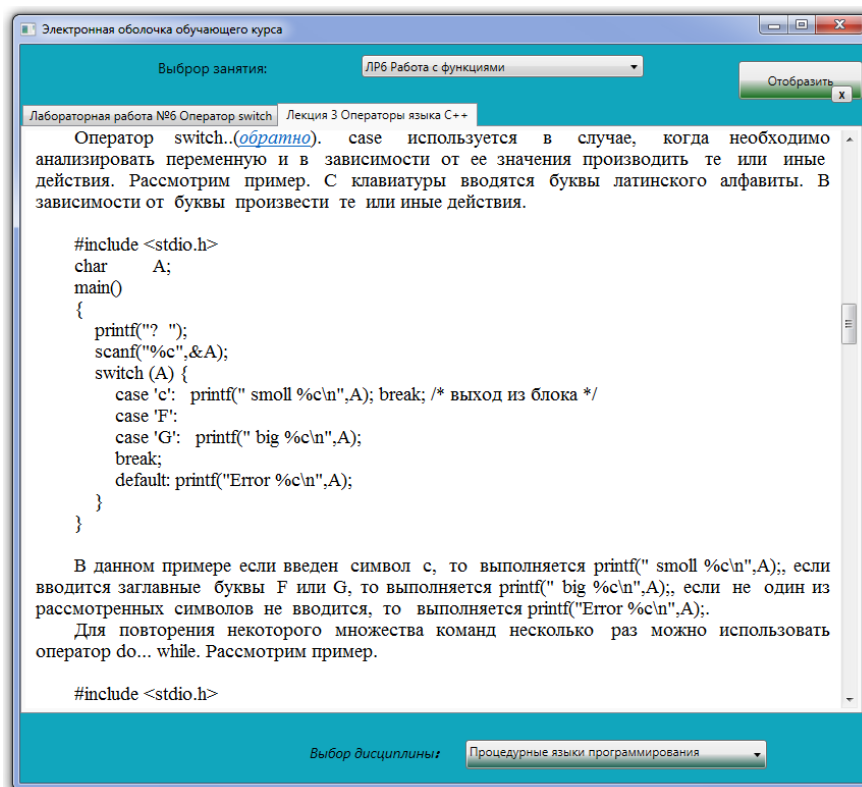


Рисунок 1. Пример перехода по гиперссылкам

В практической части приложения имеются тестовые варианты выполнения заданий. Они снабжены текстом программы, блок-схемой ее алгоритма и действующим ресурсом, куда можно ввести данные и получить результат решения задачи (рис.2).

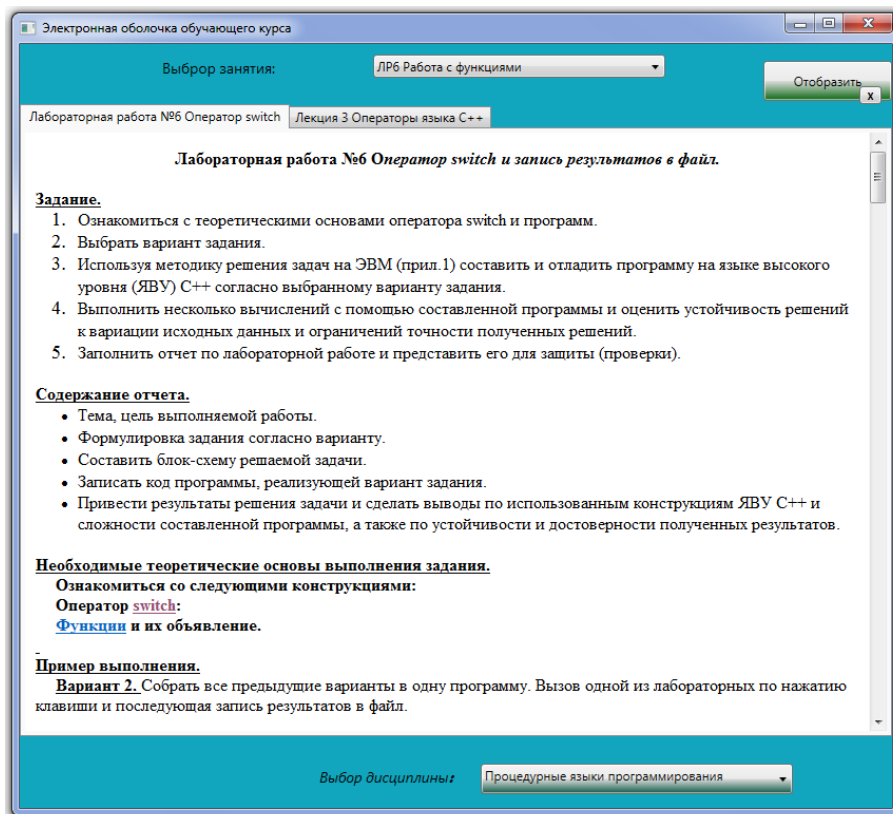


Рисунок 2. Интерфейс расчетного окна практической части приложения

---

В дополнение ко всему, имеется модуль тестирования, позволяющий проверить остаточные знания, а результаты проверки хранятся в базе данных и ими можно воспользоваться для определения материалов, требующих углубленной проработки.

Таким образом, разработанная обучающая программа имеет следующие преимущества:

1. Является интерактивной, что дает возможность обучающимся контролировать скорость прохождения учебного материала.
2. Имеет понятный, информативный, удобный интерфейс, не требующий отдельного обучения использованию.
3. Есть встроенная система тестирования обеспечивает возможность обучающимся проверить уровень своих знаний и тем самым следить за изучением материала.
4. Является простой в использовании и сопровождении (не требует затрат на ее создание и сопровождение).

#### СПИСОК ЛИТЕРАТУРЫ

1. Grand Class. Дистанционное обучение. URL: <http://grandclass.net/> (дата обращения 15.10.2023).
2. Дистанционные образовательные технологии. Филиал ВГУЮ. URL: <https://rostov.gpa-mu.ru/distancionnoe-obuchenie>. (дата обращения 15.10.2023)
3. Фаронов В., С#. Учебный курс – С.-Пб.: Питер, 2021.

**Н.Ю. Герцовский, П.В. Лобзенко**

#### **СЕРВЕР РАСПРЕДЕЛЕННОЙ ОБУЧАЮЩЕЙ СИСТЕМЫ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: обучающая система, интерактивность, информационные технологии, дистанционное обучение, сервер.

Разработан серверный модуль клиент-серверной системы для обучения программированию.

**N.Yu. Gertsovsky, P.V. Lobzenko**

#### **DISTRIBUTED TRAINING SYSTEM SERVER**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: training system, interactivity, information technology, distance learning, server.

A server module of a client-server system has been developed for teaching programming.

Современная система образования все активнее использует информационные технологии и компьютерные телекоммуникации. Особенно динамично развивается система дистанционного образования, чему способствует ряд факторов, и прежде всего -

оснащение образовательных учреждений мощной компьютерной техникой и развитие образовательных сообществ в сети Интернет. Электронные учебные сервисы могут использоваться как в целях самообразования, так и в качестве составной части дистанционного образования.

Большинство используемых в настоящее время средств обучения размещаются в сети Internet или в локальной сети обучающей организации. Это является удобным как для обучаемых – они всегда имеют доступ к единым актуальным обучающим материалам, так и для преподавателей (технического персонала организации) – имеется возможность просто и оперативно изменять и актуализировать контент для обучения [1]. В силу этого, получается, что такие распределенные сетевые системы обучения строятся по принципу клиент-серверных систем, когда обучающий контент расположен на сервере, на клиентских вычислительных машинах имеются клиентские части, снабженные пользовательским графическим интерфейсом и предназначенные для соединения с сервером, запроса необходимых данных и для отображения полученных от сервера материалов для пользователей [2].

В состав разрабатываемой обучающей системы входит сервер и несколько клиентских приложений, обучающих определённому языку программирования, с возможностью размещения обучающего контента, как на сервере, так и на стороне клиентской части (рисунок 1).

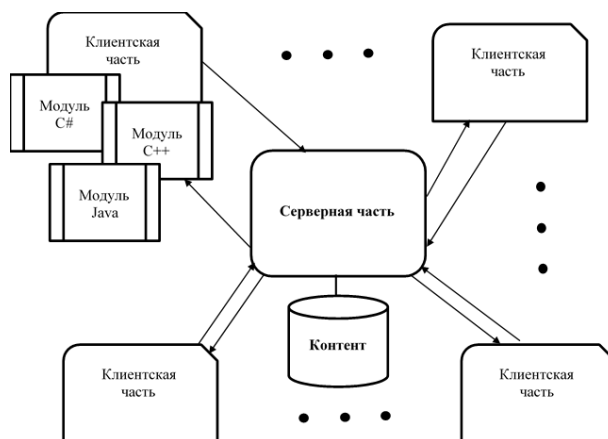


Рисунок 1. Структура клиент-серверной обучающей системы

Во-первых, создадим серверное соединение и используем для этого систему сокетов.

Сокеты — это концепция сетевого программирования, когда существуют два вида «программных разъемов»- сокетов: клиентские и серверные.

Серверный сокет как розетка, которая «висит на стене» готовая к работе, в ожидании, когда к ней подключат штекер. Точно так же серверный сокет переходит в режим ожидания подключения на определенном адресе и определенном порту.

Клиентский сокет как вилка, которую втыкают в розетку. Как только клиент подключается к серверному сокету, информация начинает передаваться между ними.

Для того чтобы создать виртуальное подключение между клиентом и сервером, надо знать место, где находится нужный нам серверный сокет.

В нашем случае, создается слушатель событий подключений в сети по протоколу TCP IP – TcpListener, в качестве параметра которому передается так называемая точка входа, которую определяет метод IPAddress из переданных ему IP адреса компьютера, на котором будет запущен сервер (пока это вариант localhost, т.е. IP 127.0.0.1) и номер порта Port, на котором создаваемой серверное подключение будет прослушивать подключения клиентов. Т.о., в конструкторе класса Server появится следующий слушатель (листинг 1).

---

### Листинг 1. Серверный слушатель подключения клиентов

```
TcpListener listner;

    public Program(int Port)
    {
        listner = new TcpListener(new
IPEndPoint(IPAddress.Parse("127.0.0.1"), Port));
        listner.Start();
        Console.WriteLine("Сервер запущен, ожидает подключений...");
        . . .
    }
}
```

Видно, что после запуска прослушивания сетевых подключений выдается сообщение о том, что сервер готов и ожидает подключений.

Далее, нужно в это подключение с помощью метода `AcceptTcpClient()` и создать новый поток для него с помощью метода `Thread` из одноименной библиотеки, которую нужно подключить заранее: `using System.Threading`.

В качестве параметра этому методу передается метод `clientThread`, в котором для каждого нового клиента открывается TCP соединение в новом потоке (листинг 2).

### Листинг 2. Метод создания нового TCP соединения для нового клиента

```
static void clientThread(Object StateInfo)
{
    new Client((TcpClient)StateInfo);
}
```

В итоге получим следующий текст класса `Server` (листинг 3).

### Листинг 3. Класс `Server`

```
class Server
{ TcpListener listner;
    public Server (int Port)
    { listner = new TcpListener(new
IPEndPoint(IPAddress.Parse("127.0.0.1"), Port));
        listner.Start();
        Console.WriteLine("Сервер запущен, ожидает подключений...");
        while (true)
        {
            TcpClient client = listner.AcceptTcpClient();
            // Создаем поток
            Thread Thread = new Thread(new
ParameterizedThreadStart(clientThread));
            // И запускаем этот поток, передавая ему принятого
клиента
            Thread.Start(client); } }
    static void clientThread(Object StateInfo)
    {
        new Client((TcpClient)StateInfo);
    }
    static void Main(string[] args)
    {
        new Program(12000); } }
```

Таким образом, разработанный сервер обладает следующими преимуществами:

- двухвариантное использование как в локальной информационной сети филиала, так и в сети Internet, что значительно упрощает доступ к обучающему контенту за счет централизации или индивидуального использования;

- 
- практическая часть модуля настроена на простые и понятные технические сообщения, отражающие процесс клиент-серверного взаимодействия;
  - приложение обладает минимальными аппаратно-программными требованиями к информационной системе, в которой будет размещаться и использоваться.

#### СПИСОК ЛИТЕРАТУРЫ

1. Grand Class. Дистанционное обучение. URL: <http://grandclass.net/> (дата обращения 15.10.2023).
2. Фаронов В., С#. Учебный курс – С.-Пб.: Питер, 2021.

**Е.А. Зайцев, Д.Л. Устименко**

#### **ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭЛЕКТРОЭНЕРГЕТИКЕ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: Искусственный интеллект (ИИ); электроэнергетика; электроподстанции.

В этой статье рассмотрены перспективы применения технологий ИИ по обеспечению защиты энергосистем от различного рода технологических нарушений.

**E.A. Zaytsev, D.L. Ustimenko**

#### **PROSPECTS FOR THE USE OF ARTIFICIAL INTELLIGENCE IN THE ELECTRIC POWER INDUSTRY**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: Artificial intelligence (AI); electric power industry; electrical substations.

This article discusses prospects for the use of AI technologies to ensure the protection of power systems from various kinds of technological violations in general.

#### **Введение**

Одним из принципов применяемых сегодня решений по обеспечению защиты энергосистем от всех видов технологических нарушений и поддержанию тем самым нормальной работы подстанций и потребителей является использование риск-идентифицируемых информационных моделей защищаемых объектов.

Эти модели создаются на основе анализа и изучения существующих операционных систем. Инженеры могут использовать эти модели на самых ранних стадиях проектирования. Такой подход позволяет заранее учесть возможные риски и существенно снизить затраты на исправление ошибок.

Однако ручное проектирование структурных и функциональных решений релейной защиты и автоматики для цифровых подстанций – сложный, трудоемкий и дорогостоящий процесс. Что же можно сделать для улучшения ситуации в электроэнергетике?

---

Ответ прост. Искусственный интеллект может помочь энергетикам сделать это быстро и легко.

### **Электрические подстанции**

Электрические подстанции - сложные технологические объекты, численность которых в России близка к миллиону, однако многие из них были сделаны ещё в советские времена и им необходима модернизация. На данный момент рынок АСУ ТП насчитывает десятки миллиардов рублей и с каждым годом этот процент увеличивается на 10-15%, из них 5-7% предоставляют услуги по реконструкции. По установленным срокам переустройство данных точек длится 10-12 месяцев. Чтобы провести массовую модернизацию, нужны новые методы.

Здесь используется не только SCADA-системы - собирает информацию о множестве удаленных объектов, поступающих с устройств контроля, но и отображает эту информацию в едином диспетчерском центре. Также она должна обеспечивать долгосрочное архивирование полученных данных. Диспетчер чаще всего имеет возможность не только наблюдать за объектом, но и управлять им, реагируя на различные ситуации. Так же тут эксплуатируются электронные устройства, которые осуществляют общую и (или) дополнительную защиту и автоматику электроустановок.

Трудоёмкость этих технологий заключается в том, что по нормативам документации время реагирования на любое технологическое нарушение в данных системах насчитывает несколько десятков миллисекунд. За такой короткий промежуток надо расспросить большое количество терминалов, датчиков, устройств и привести в исполнение сложные алгоритмы.

Медленное выполнение заданных мер зачастую приводит не только к неисправности оборудования, но и к системным авариям и отключениям электроэнергии. Например, задержка в несколько десятков миллисекунд в работе алгоритма может привести к потере синхронизации генераторов на электростанции, что, в свою очередь, может привести к сбою федерального масштаба. Это происходит потому, что в Российской Федерации очень большая энергосистема и все системы взаимосвязаны. В связи с этим последствия аварии в одном регионе могут отразиться на другом.

### **Проектирование цифровых подстанций с применением ИИ**

Новый метод цифрового проектирования подстанций с использованием искусственного интеллекта на основе стандарта МЭК 61850, разработанный специалистами Центра компетенции НТИ МЭИ, получил название ng.Grace.

Работает "Грейс" следующим образом. Пользователь загружает схему главной электрической системы подстанции, которая обрабатывается системой с использованием различных методов искусственного интеллекта, в результате чего получается комбинация программно-аппаратных структурных схем и алгоритмов релейной защиты.

В данном случае возможны два сценария использования:

1. Обеспечение выполнения заданных требований по надежности при минимизации затрат;
2. Достижение наиболее надежного подхода при заданных фиксированных затратах.

Система на основе логических рассуждений анализирует схему подстанции и на ее основе определяет правильную конфигурацию функций защиты, которые должны быть реализованы на подстанции. Учитывая все ограничения и требования, система позволяет назначить эти функции защиты контроллерам, правильно построить топологию ЛВС и объединить ее с распределением информационных потоков.

### **Перспективы работы ИИ с уникальными схемами**

Каждый элемент электрической сети имеет известные данные порта, содержащие конкретные значения параметров устройства, однако каждая схема уникальна и должна

---

обрабатываться с учетом того, как связаны между собой ее элементы. Используя механизм логического вывода, продукт может определить компоненты и связи между ними, необходимые для новой конфигурации сети, без написания собственных алгоритмов и больших объемов программного кода. Кроме того, существуют сетевые объекты, не существующие в базе данных "активов", но также требующие защитных мер. Именно механизм логических рассуждений позволяет найти эти связи и выразить необходимую функциональность.

Модель угроз" может быть получена путем добавления соответствующих типов повреждений к типам устройств и их связей с другими сетевыми устройствами. Исходя из спецификаций и требований, система с помощью логических рассуждений определяет количество коротких замыканий, которые могут возникнуть в каждом элементе технического оборудования. Таким образом, конкретному типу повреждения соответствует конкретная функция, которая может устранить этот тип повреждения.

Таким образом, анализируя сценарии, система может определить, что необходимо защитить (даже если это не "актив"), и определить полную конфигурацию функций защиты для различных видов технологического вмешательства.

#### Заключение

В данной статье было рассмотрена перспектива в защите электроэнергетики. Подводя итоги, можно сказать, что при правильном обучении ИИ, можно добиться не малых перспектив применения в защите электросетей(электроэнергетики) от технологических нарушений. Почему это перспектива применения? Потому что, рассмотрев в статье проблему с электрическими подстанциями, мы понимаем как человеку трудно справиться с их защитой, но благодаря ИИ эта проблема разрешается в разы легче.

#### СПИСОК ЛИТЕРАТУРЫ

1. Liu, X., Hao, X., Du, B., Zhang, H., & Wang, Z. (2020). A Survey on Smart Grids: Solutions and Techniques Based on Artificial Intelligence Paradigms. *Energies*, 13(19), 5151.
2. Chen, C., Kang, C., Luo, Z., Dong, Z. Y., & Zhang, Y. (2020). A Review of Artificial Intelligence Applications in Power Grid Operation and Control. *Applied Sciences*, 10(11), 3792.
3. Nguyen, T. A. T., Musa, M., & Thiruvankadam, S. (2021). A survey on artificial intelligence applications in power system operation and control. *Energies*, 14(5), 1280.
4. Lu, Z., Wang, H., Chen, G., & Ren, Z. (2021). A survey on big data analytics and artificial intelligence for power grid operations: Applications, challenges, and trends. *Electric Power Systems Research*, 185, 106757.
5. Behrangrad, M., & Koochakzadeh, R. (2020). An overview of big data analytics and artificial intelligence for smart grid. *Electric Power Systems Research*, 180, 106061.
6. Lai, C. H., Lee, C. T., Hong, C. M., & Wei, L. C. (2020). Artificial Intelligence Applications in Power Systems: A Survey. *Energies*, 13(19), 4997.
7. Abhari, R., & El-Fouly, T. (2020). A Review of Artificial Intelligence Applications in the Smart Grid. *Applied Sciences*, 10(8), 2862.
8. Dehnavi, S. R., & Sohrabi, F. (2021). Load forecasting in smart grids: A review of machine learning approaches and a novel hybrid LSTM-PSO model. *Electric Power Systems Research*, 190, 106820.
9. Dong, Z. Y., Wang, Z. X., Luo, Z., & Kang, C. (2021). A Review of Artificial Intelligence Applications in Power Distribution Systems. *Energies*, 14(13), 4071.
10. Ameli, A., Mohammadi, H., Karakouzian, M., & Siano, P. (2021). Smart grid and renewable energy sources: A survey on AI applications. *Renewable and Sustainable Energy Reviews*, 136, 110421.

## ЭТИЧЕСКИЕ АСПЕКТЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: искусственный интеллект, этика искусственного интеллекта

Статья представляет собой обзор научной литературы и нормативно-правовых актов, касающихся морально-этических аспектов использования искусственного интеллекта. Представлена краткая история вопроса, обоснована необходимость применения этических норм при внедрении технологий искусственного интеллекта, сделан вывод об актуальности данного вопроса.

M.P. Leonov, D.L. Ustimenko

## ETHICAL ASPECTS OF ARTIFICIAL INTELLIGENCE

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: artificial intelligence, ethics of artificial intelligence

The article is a survey of scientific publications and regulatory legal acts concerning moral and ethical aspects of artificial intelligence. The authors present brief history of the problem, substantiate application of ethical standards in AI-technology introduction. The authors draw a conclusion about the relevance of the problem.

### **Введение.**

В современном мире искусственный интеллект становится неотъемлемой частью повседневной жизни человека, проникая во все сферы деятельности. Многие задачи решаются при помощи технологий машинного обучения даже успешнее, чем вручную.

Вместе с тем обостряются некоторые аспекты его применения. Перед разработчиками остро стоят вопросы этики искусственного интеллекта. Необходимо научить его понятиям справедливости, морали, способности действовать объективно. Важным в обучении является анализ результатов деятельности с исправлением ошибок.

Понятие этики используется здесь в значении моральных принципов, ценностей и норм, регулирующих поведение индивидов. Этика определяет, что считается правильным или неправильным, добрым или злым, и служит основой для принятия этических решений. Она основывается на культурных и социальных установках. Этим обусловлена сложность применения этики к искусственному интеллекту. «Этика непосредственно начинается тогда, когда появляется способность реагировать на собственные ошибки, осуществлять рефлексию поведения, учитывая при этом мнения других людей. Такая же принципиальная возможность ошибки должна быть заложена и в работу искусственного интеллекта, чтобы можно было говорить о его этике в собственном смысле слова». [2]

### **Цель и задача работы. Методы исследования.**

Целью настоящей работы является изучение проблемы этики искусственного интеллекта: рассмотрение истории вопроса, его актуальности, отражения данной темы в политическом и правовом поле в России и в мире, и освещения ее в научной литературе.

Метод исследования – анализ научных источников и правовой документации.



---

### **История робоэтики. Сильный и слабый искусственный интеллект.**

Первые упоминания об этических проблемах искусственного интеллекта встречаются в середине XX в, когда писатель Айзек Азимов изложил три базовых закона робототехники: робот не должен причинять вред людям своими действиями или бездействием; он должен повиноваться приказам человека, кроме противоречащих предыдущему закону; он обязан заботиться и о своей безопасности, если это не противоречит двум предыдущим законам.

В начале 21 века роботы стали заменять человека, и тема робоэтики получила новое развитие. В 2004 г. в Италии прошел Международный симпозиум по робоэтике. В 2015 году появилась возможность обучать нейронные сети с использованием глубокого обучения (Deep Learning). Технология оказалась эффективной. Искусственный интеллект активно переходит из мира науки в повседневную жизнь.

Но уже в начале 70-х гг. 20 века появляются и неудачи: бесперспективным оказался, например, машинный перевод. Это побудило разделить искусственный интеллект на сильный и слабый. Сильный – это роботы, компьютеры, которые могут захватить власть, заменить человека; слабый – это программы, направленные на решение узких задач (распознавание номеров автомобилей, игра в шахматы, фильтрация спама и т.д.). Их и стали преимущественно развивать вплоть до последнего времени.

Однако в последние годы наблюдается новый всплеск интереса к сильному искусственному интеллекту. И вновь поднимаются вопросы этики, так как эту технологию можно применить там, где возможны серьёзные проблемы – от дискриминации и утечки персональных данных до гибели людей.

### **Правовое регулирование искусственного интеллекта.**

В 2017 г. Европарламент принял Европейскую хартию робототехники, где провозглашались принципы безопасности, сохранности персональных данных, обратимости предпринятых роботом действий.

В России выработка этических норм предусмотрена программой «Национальная стратегия развития искусственного интеллекта на период до 2030 года», утверждённой Указом Президента РФ от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». В ней отмечено, что результаты исследований направленных на прогнозирование этических аспектов использования искусственного интеллекта, должны учитываться при принятии управленческих решений (п. 57 Указа Президента РФ № 490).

В 2021 г. в России на Первом международном форуме «Этика искусственного интеллекта: начало доверия» подписан «Кодекс этики искусственного интеллекта», авторами которого являются Альянс в сфере искусственного интеллекта РФ, Аналитический центр при правительстве РФ и Минэкономразвития. Кодекс разработан на основе «Национальной стратегии развития искусственного интеллекта на период до 2030 года». Приоритетом в нем является защита интересов и прав людей. Россия одной из первых в мире выделила риски искусственного интеллекта: дискриминация, потеря приватности, потеря контроля над искусственным интеллектом, угроза человеку, неприемлемые цели применения. Эти риски отражены в Кодексе. В нем провозглашаются принципы применения искусственного интеллекта – прозрачность, правдивость, ответственность, надёжность, беспристрастность, безопасность и конфиденциальность. [1]

### **Источники этических проблем искусственного интеллекта.**

Остановимся подробнее на причинах пристального внимания к этической стороне внедрения рассматриваемой технологии.

Во-первых, это проблема безопасности и снижения рисков. Во-вторых, это проблема моральной ответственности за негативные последствия. В-третьих, необходимость перестройки общественных институтов так, чтобы они обезопасили общество при использовании искусственного интеллекта. [3]

---

Как уже было сказано, использование искусственного интеллекта влечёт за собой ряд нравственно-этических и тесно связанных с ними правовых проблем.

С точки зрения обычного человека это, прежде всего, безопасность личных данных, правомерность использования систем распознавания лиц и данных камер наблюдения, использования данных о покупательских предпочтениях организациями сферы продаж. Серьёзные опасения вызывают возможность угрозы для жизни людей, дискриминация, затруднения в определении субъекта, несущего ответственность за решения, принимаемые искусственным интеллектом. С глобальной точки зрения это разработка новых видов вооружений на базе искусственного интеллекта.

Как видим, любая технология, в том числе бытовая и промышленная, на основе искусственного интеллекта может нести угрозу, так как искусственный разум «не обладает осознанием самого себя, как не обладает и тем, что называется «эмпатией» - основой этики». [3] Моральные устои человека зависят от воспитания, окружения, у каждого есть некий «моральный компас». [3] У искусственного интеллекта такой «компас» отсутствует. Единственным моральным ориентиром, о котором можно говорить в данном случае – это разработчик алгоритма, который устанавливает правила о том, что хорошо и что плохо.

Принцип обучения искусственного интеллекта основан на анализе многочисленных образцов, и в этом кроется возможность предвзятости. Поясним это на примере компании Амазон, который приводит в своей статье Леонов В.А. Специалисты по управлению персоналом этой компании обнаружили, что их новая рекрутинговая машина «не одобряла» кандидатов-женщин. Дело в том, что компьютерные модели Amazon были обучены проверять кандидатов, собирая закономерности в резюме за предшествующие 10 лет. Большинство из кандидатов – мужчины, что является нормой в технологической индустрии. Компания редактировала программы и решила проблему. Но нет гарантии, что искусственный интеллект не придумает новый дискриминационный способ сортировки кандидатов. [3]

Ещё одной проблемой может стать использование искусственного интеллекта с потерей человеческого контакта. Для общества это риск десоциализации. Для компании это потеря чувства общности, что ведёт к снижению эффективности труда.

Внедрение искусственного интеллекта в производство может вызвать глобальную трансформацию рынка труда. Пока вытеснения человека роботом на рабочем месте не происходит, но такая возможность должна учитываться. Робот выполнит механическую работу более эффективно, и есть предположения, что к 2030 году роботы могут заменить до 30% человеческого труда, что может повлечь за собой рост безработицы. [3]

#### **Текущее состояние вопроса.**

В Российской Федерации работа по развитию этики искусственного интеллекта ведётся на правительственном уровне. Крупные мировые компании – Google, Microsoft, IBM – также начали работу над созданием этических принципов развития искусственного интеллекта. Это прозрачность, справедливость, честность, ненарушение прав, ответственность и конфиденциальность. [3] В различных сферах производства компании вводят должность директора по робототехнике, одной из задач которого является снижение беспокойства персонала из-за возможной потери рабочих мест и изменения качества труда. Совместно с отделом HR они будут разрабатывать принципы взаимодействия человека и робота, среди которых – адаптация работников к новой среде, исключение вреда здоровью, в том числе психическому, регулирование ответственности и т.д. [3]

#### **Выводы.**

В результате проведённого исследования мы выявили актуальность исследования и разработки принципов, которые будут определять моральное поведение искусственного

---

интеллекта. Необходимо контролировать деятельность искусственного интеллекта с целью недопущения нарушений общечеловеческих моральных принципов. Развитие этики искусственного интеллекта должно идти в направлении равных возможностей, гарантии занятости, конфиденциальности личных данных, неприкосновенность личной жизни и безопасность.

В мире в целом и в Российской Федерации в частности принимается целый ряд мер на разных уровнях, от правительственного до уровня отдельных компаний, с целью минимизации рисков и угроз, связанных с применением искусственного интеллекта.

#### СПИСОК ЛИТЕРАТУРЫ

1. Афанасьева Ж.С., Афанасьев А.Д. Этические аспекты применения технологий искусственного интеллекта. // Информационные технологии и математическое моделирование в управлении сложными системами. – 2022, №3 (15), с. 24-32.
2. Разин А.В. Этика искусственного интеллекта. // Философия и общество. – 2019, №1, с. 57-73.
3. Леонов В.А., Каштанова Е.В., Лобачёва А.С. Этика искусственного интеллекта: проблемы и инициативы в социальной сфере. // Управление персоналом и интеллектуальными ресурсами в России. – 2021, №2 (53), с. 5-12.

**Ю.И. Найденова<sup>1</sup>, И.В. Решетникова<sup>2</sup>, О.А. Сафарьян<sup>1</sup>**

#### **ПОСТРОЕНИЕ ЭКСПЕРТНОЙ СИСТЕМЫ ДЛЯ ОЦЕНКИ КРИПТОСТОЙКОСТИ АЛГОРИТМА ШИФРОВАНИЯ RSA**

Донской государственный технический университет, г. Ростов-на-Дону, Россия<sup>1</sup>  
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: экспертная система, алгоритм шифрования RSA

В статье предложен вариант практического применения динамической экспертной системы (ЭС) для выявления анализа уязвимости алгоритма шифрования RSA. Экспертная система будет определять уязвимость ключа с моделированием атаки направленной на алгоритм RSA.

**J.I. Naydenova<sup>1</sup>, I.V. Reshetnikova<sup>2</sup>, O.A. Safaryan<sup>1</sup>**

#### **CONSTRUCTION OF AN EXPERT SYSTEM FOR ASSESSING THE CRYPTO STRENGTH OF THE RSA ENCRYPTION ALGORITHM**

Don State Technical University, Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: expert system, RSA encryption algorithm

Abstract The article proposes a practical application of a dynamic expert system (ES) to identify the vulnerability analysis of the RSA encryption algorithm. The expert system will determine the vulnerability of the key by simulating an attack aimed at the RSA algorithm.

Интеграция информационных технологий в нашу повседневную жизнь привела к возникновению новых вызовов в обеспечении конфиденциальности и безопасности передаваемых данных. Шифрование — одно из наиболее эффективных средств защиты информации. Среди множества алгоритмов шифрования потоковые шифры занимают особое место. Они отличаются простотой реализации и высокой скоростью обработки данных, что делает их привлекательными для различных приложений, включая беспроводные коммуникации и защищенные соединения в интернете.

Блочный асимметричный алгоритм - это алгоритм шифрования, который использует пару ключей: открытый ключ для шифрования и закрытый ключ для расшифровки.

Алгоритм шифрования RSA (Rivest-Shamir-Adleman) - это криптографический алгоритм, который используется для шифрования и подписи сообщений [1].

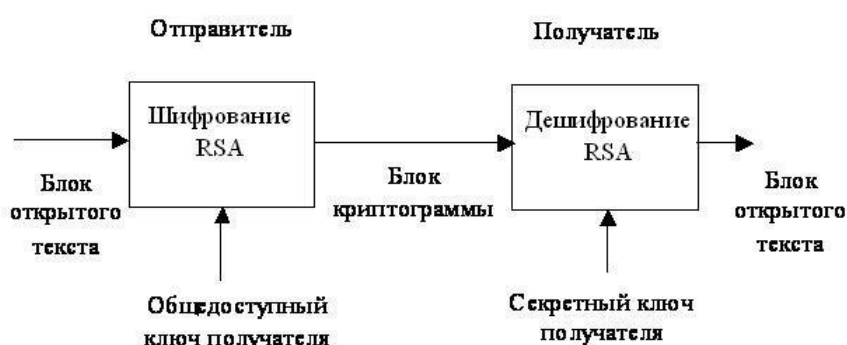


Рисунок 1. Алгоритм шифрования RSA

Алгоритм основан на сложности факторизации больших чисел, что делает его стойким к атакам.

На алгоритм RSA могут быть применены различные атаки, которые могут позволить злоумышленнику расшифровать зашифрованные данные. Некоторые из наиболее распространенных включают в себя:

- факторизация модуля  $N$ : Атакующая сторона пытается найти секретный ключ, разложив модуль  $N$  на его простые множители. Если была найдена эффективная алгоритмическая процедура для факторизации больших чисел, это могло бы позволить атакующим раскрыть секретный ключ и дешифровать зашифрованные сообщения. На данный момент самым известным алгоритмом факторизации больших чисел является алгоритм Квантового алгоритма Шора.
- атака подбором: Атакующая сторона может попытаться просто перебирать все возможные значения секретного ключа, пока не будет найдено верное значение. Однако, с учетом наличия достаточно длинных ключей, это требует экспоненциального количества вычислений и времени, что делает эту атаку практически неосуществимой.
- атака времени выполнения: Атакующая сторона может использовать различное время выполнения операций шифрования и дешифрования, чтобы вывести дополнительную информацию о секретном ключе. Эта атака возможна, когда реализация алгоритма RSA не выполняет одинаковое количество операций для всех входных данных или если используются алгоритмические оптимизации, которые могут утекать информацию о секретном ключе.
- атака посредника: Если злоумышленник может перехватить передачу зашифрованных сообщений между отправителем и получателем, он может выполнить атаку посредника. Это может позволить злоумышленнику изменять сообщения или даже выполнять атаку "man-in-the-middle" и передавать свои собственные сообщения, представляясь отправителем или получателем.

Для безопасности необходимо выбирать достаточно большие простые числа  $p$  и  $q$ , чтобы противодействовать известным атакам на RSA, таким как атака факторизации и атака подбора закрытого ключа.

Экспертная система по выявлению криптостойкости алгоритма RSA может помочь анализировать безопасность данного алгоритма и предоставить рекомендации или оценки уязвимостей [2].

Экспертная система - это компьютерная программа, которая использует знания и опыт эксперта в определенной предметной области для решения задач и предоставления рекомендаций. Она моделирует знания эксперта, анализирует информацию и принимает решения, аналогичные тем, которые принимал бы человек-эксперт. Такая система основана на обширной базе знаний, которая включает в себя правила и факты [3].



Рисунок 2. Структурная схема экспертной системы

Описание модели экспертной системы может включать следующие компоненты:

- хранилище знаний: ЭС содержит базу знаний, которая содержит представление экспертного знания о предметной области. Знания могут быть представлены в виде правил, фактов, процедур или деревьев принятия решений.
- механизм вывода: Это основной компонент экспертной системы, ответственный за обработку вопросов пользователя, применение знаний из базы и генерацию ответов и рекомендаций. Движок вывода может использовать различные методы, такие как прямой вывод, обратный вывод, цепочки правил или логический вывод.
- интерфейс пользователя: ЭС обычно имеет интерфейс, который позволяет пользователям взаимодействовать с системой и задавать вопросы. Интерфейс может быть текстовым, графическим или комбинированным, в зависимости от спецификаций системы.
- система поддержки принятия решений: Экспертная система может предоставлять поддержку принятия решений, основанную на своих знаниях и алгоритмах. Это может быть полезно для принятия сложных решений, анализа альтернатив и предоставления рекомендаций.
- мониторинг и отладка: ЭС может быть оснащена инструментами для мониторинга и отладки своих процессов и решений. Это помогает выявлять ошибки, улучшать производительность и повышать надежность системы.

В ходе работы экспертной системы алгоритм RSA будет подвержен различного вида атакам. Экспертная система будет определять уязвимость ключа с моделированием атаки направленной на алгоритм RSA. При верном дешифровании сообщения, можно будет сказать, что алгоритм подвержен атаке с данным размером ключа.

---

## СПИСОК ЛИТЕРАТУРЫ

1. Адаменко, Михаил Основы классической криптологии. Секреты шифров и кодов / Михаил Адаменко. - Москва: Высшая школа, 2014. - 256 с.
2. А.Н. Козлов «Интеллектуальные информационные системы»: учебник – Изд-во ФГБОУ ВПО Пермская ГСХА, 2013. – 278 с.
3. Е.В. Боровская, Н.А. Давыдова «Основы искусственного интеллекта»: учебное пособие – М.: Лаборатория знаний, 2020. – 130 с.

**В.Г. Кобак<sup>2</sup>, Д.И. Киянов<sup>2</sup>, Д.А. Жуковский<sup>1</sup>, Д.Е. Панков<sup>2</sup>**

### **ИСПОЛЬЗОВАНИЕ SYMPY ДЛЯ НАХОЖДЕНИЯ ХРОМАТИЧЕСКОГО ЧИСЛА ГРАФА МЕТОДОМ MAGU**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Донской государственный технический университет, Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: хроматическое число, NP-полная задача, SymPy, приведение к ДНФ.

В работе исследуется применение библиотеки SymPy для определения хроматического числа графа с использованием метода Magu. Метод Magu, базирующийся на приведении конъюнктивной нормальной формы (КНФ) в дизъюнктивную нормальную форму (ДНФ), представляет собой важный инструмент в графовой теории. Основное внимание уделяется процессу трансформации КНФ в ДНФ с использованием библиотеки SymPy и его применимости для определения хроматического числа графа. Проведен анализ эффективности метода на связном не ориентированном графе без петель, что позволяет сделать выводы о применимости SymPy в контексте задач оптимизации графов. Полученные результаты представляют интерес для исследователей в области графовых алгоритмов и искусственного интеллекта, предоставляя новый взгляд на использование символьных вычислений в решении задачи нахождения хроматического числа графа методом Magu.

**V.G. Kobak<sup>2</sup>, D.I. Kiyanov<sup>2</sup>, D.A. Zhukovsky<sup>1</sup>, D.E. Pankov<sup>2</sup>**

### **USING SYMPY TO FIND THE CHROMATIC NUMBER OF A GRAPH USING THE MAGOO METHOD**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Don State Technical University, Rostov-on-Don, Russia<sup>2</sup>

Keywords: chromatic number, NP-complete problem, SymPy, reduction to DNF.

This work investigates the application of the SymPy library to determine the chromatic number of a graph using Magoo's method. Magoo's method, which is based on the conversion of a conjunctive normal form (CNF) into a disjunctive normal form (DNF), is an important tool in graph theory. The focus is on the process of transforming CNFs into DNFs using the SymPy library and its applicability to the determination of the chromatic number of a graph. The effectiveness of the method on a connected undirected graph without loops is analysed, which

---

allows us to draw conclusions about the applicability of SymPy in the context of graph optimisation problems. The results obtained are of interest to researchers in the field of graph algorithms and artificial intelligence, providing a new perspective on the use of symbolic computation in solving the problem of finding the chromatic number of a graph by Magoo's method.

### **Введение.**

Исследование хроматического числа графа представляет собой актуальную задачу в области графовых алгоритмов. В данной работе рассматривается применение библиотеки SymPy для вычисления с помощью метода Magoo. Целью является анализ эффективности библиотеки для символьных вычислений и его применимости в реальных задачах оптимизации.

### **Постановка задачи.**

Для простого, неориентированного графа без петель и кратных ребер хроматическим числом называется количество цветов, в которые можно раскрасить граф, при условии, что соседние вершины не могут быть окрашены в один цвет.

Нахождение хроматического числа методом Magoo подразумевает 2 этапа:

Нахождение устойчивых множеств путем построения формулы смежности графа, с последующим приведением к ДНФ, выполнив все возможные поглощения.

Определение хроматического числа заданного графа. Для этого полученная формула ДНФ проходит преобразования, на выходе которых получится формула КНФ, которую необходимо преобразовать в ДНФ.

Таким образом, задача использования SymPy в методе Magoo подразумевает два преобразования формулы в ДНФ.

### **Способы использования SymPy.**

В библиотеке SymPy существует 2 способа:

- `sympy.logic.boolalg.to_dnf(expr, simplify=False, force=False)`. Данная функция создана исключительно для приведения к ДНФ. На вход принимает 3 параметра.  
`expr` – выражение, которое нужно привести к ДНФ.  
`simplify` – по умолчанию True. Если значение True, то приводит к простейшей ДНФ используя Метод Куайна — Мак-Класки. Может принимать True/False.  
`force` – по умолчанию False. Если в выражении больше 8 литералов, функция вызовет исключение. Чтобы функция вычисляла выражения, имеющие более 8 литералов, необходимо задавать значение True.
- `sympy.logic.boolalg.simplify_logic(expr, form=None, deep=True, force=False, dontcare=None)`. Данная функция создана для упрощений логических выражений. На вход принимает 5 параметров.  
`expr` – выражение, которое нужно упростить.  
`form` – по умолчанию None. Может принимать `cnf`, `dnf`, `none`. Если `cnf`, упростит к КНФ, если `dnf`, упростит к ДНФ, если `none`, упростит к форме, которая будет иметь наименьшее количество аргументов, как правило КНФ.  
`deep` – по умолчанию True. Разрешает рекурсивное упрощение любых небулевы функции, содержащиеся во входных данных. Может принимать True/False.  
`force` – по умолчанию False. Если в выражении больше 8 литералов, функция вызовет исключение. Чтобы функция вычисляла выражения, имеющие более 8 литералов, необходимо задавать значение True.  
`dontcare` – по умолчанию None. Принимает конструкцию SymPy, а именно литералы, значения которых неважны.

Оба способа идентичны при одинаково заданных параметрах. `simplify_logic(force=True, form='dnf')` вернет то же самое, что и `to_dnf(force=True, simplify=True)`. В дальнейшей работе будет использоваться способ `to_dnf`, как более прямолинейный.

Так же стоит отметить, что SymPy использует непривычные символы внутри булевых выражений. `~` означает отрицание, `|` означает логическое ИЛИ (дизъюнкция), `&` логическое И (конъюнкция)

### Метод Mapu.

Известно, что задачу нахождения хроматического числа в графе можно свести к задаче нахождения внутренне устойчивого подмножества в графе, дополненном к заданному [3] с последующими вычислениями. Для нахождения максимального внутренне устойчивого подмножества используется метод Mapu.

Для хранения информации о графе, будет использована библиотека NetworkX, которая предназначена для работы с графами. Для составления формулы смежности неэффективно составление матрицы смежности, это вызовет лишние вычисления. Формула смежности будет составляться проверкой наличия соседей вершин в графе. Матрица смежности будет выводиться для пользователя, однако время, потраченное на её составление не будет учтено.

Полученное выражение приведем к ДНФ. Все вершины, входящие в элементарную конъюнкцию, образуют множество внутренне устойчивые подмножества. Далее для каждой вершины составляется выражение нахождения её в подмножестве. Все выражения затем объединяются вместе, составляя новую КНФ, которую необходимо привести к ДНФ. Чтобы получить хроматическое число, достаточно будет посчитать количество литералов внутри дизъюнкта.

### Программная реализация.

Например, для графа G, представленном на рисунке 1.

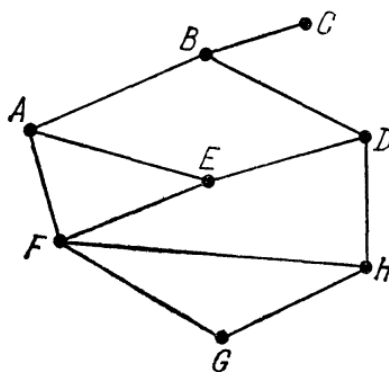


Рисунок 1. Граф G

Составим выражение смежности:

$$\begin{aligned}
 & (\sim A | \sim F) \& (\sim A | \sim E) \& (\sim A | \sim B) \& (\sim B | \sim A) \& (\sim B | \sim D) \& \\
 & (\sim B | \sim C) \& (\sim C | \sim B) \& (\sim D | \sim B) \& (\sim D | \sim E) \& (\sim D | \sim H) \& (\sim E | \sim A) \& \\
 & (\sim E | \sim D) \& (\sim E | \sim F) \& (\sim F | \sim A) \& (\sim F | \sim E) \& (\sim F | \sim H) \& (\sim F | \sim G) \& \\
 & (\sim G | \sim F) \& (\sim G | \sim H) \& (\sim H | \sim D) \& (\sim H | \sim F) \& (\sim H | \sim G)
 \end{aligned}$$

В программе данное выражение составляется в виде строкового значения. При переводе в выражение SymPy, дублирующийся конъюнкты упростятся. Перевод из строкового значения в SymPy будет выполнен с помощью функции `parse_expr`. Алфавит



выражения будет задан прямо, поскольку SymPy может воспринимать символы e, E как алгебраические константы.

После получения выражения, к нему применяется `to_dnf(formula, simplify=True, force=True)`.

На выходе будет выражение:

$$\begin{aligned}
 & (\sim B \ \& \ \sim E \ \& \ \sim F \ \& \ \sim H) \mid (\sim A \ \& \ \sim B \ \& \ \sim D \ \& \ \sim F \ \& \ \sim G) \mid \\
 & (\sim A \ \& \ \sim B \ \& \ \sim D \ \& \ \sim F \ \& \ \sim H) \mid (\sim A \ \& \ \sim B \ \& \ \sim E \ \& \ \sim G \ \& \ \sim H) \mid \\
 & (\sim A \ \& \ \sim C \ \& \ \sim D \ \& \ \sim F \ \& \ \sim G) \mid (\sim A \ \& \ \sim C \ \& \ \sim D \ \& \ \sim F \ \& \ \sim H) \mid \\
 & (\sim B \ \& \ \sim D \ \& \ \sim E \ \& \ \sim F \ \& \ \sim G) \mid (\sim A \ \& \ \sim C \ \& \ \sim D \ \& \ \sim E \ \& \ \sim G \ \& \ \sim H)
 \end{aligned}$$

Полученные дизъюнкты являются внутренне устойчивыми подмножествами.

Далее проходит проверка всех вершин на наличие внутри дизъюнктов. В случае их отсутствия, к их выражению добавляется запись `up`. В ходе проверки составляется следующее выражение:

$$\begin{aligned}
 & (y1 \mid y4) \ \& \ (y1 \mid y7) \ \& \ (y4 \mid y8) \ \& \ (y1 \mid y3 \mid y6) \ \& \ (y2 \mid y5 \mid y7) \ \& \\
 & (y5 \mid y6 \mid y8) \ \& \ (y2 \mid y3 \mid y5 \mid y6) \ \& \ (y1 \mid y2 \mid y3 \mid y4 \mid y7)
 \end{aligned}$$

Порядок скобок и названий вершин не совпадает, поскольку SymPy сам сортирует элементы внутри выражений в порядке возрастания. Так для вершины A выражением является `(y1 | y7)`.

После перевода в ДНФ предыдущего выражения, можно получить хроматическое число:

$$\begin{aligned}
 & (y1 \ \& \ y2 \ \& \ y8) \mid (y1 \ \& \ y4 \ \& \ y5) \mid (y1 \ \& \ y5 \ \& \ y8) \mid \\
 & (y4 \ \& \ y6 \ \& \ y7) \mid (y1 \ \& \ y2 \ \& \ y4 \ \& \ y6) \mid (y1 \ \& \ y3 \ \& \ y7 \ \& \ y8) \mid \\
 & (y1 \ \& \ y6 \ \& \ y7 \ \& \ y8) \mid (y3 \ \& \ y4 \ \& \ y5 \ \& \ y7) \mid (y3 \ \& \ y4 \ \& \ y7 \ \& \ y8)
 \end{aligned}$$

Минимальным количеством литералов внутри дизъюнкта будет хроматическое число = 3.

### Вычислительный эксперимент.

С помощью программного средства, написанного на языке программирования Python, был проведен вычислительный эксперимент, по проверке эффективности SymPy для поиска хроматического числа. Использовался компьютер с процессором Ryzen 5 5500 4.45 ГГц и оперативной памятью объемом 32гб DDR4. Исходными данными эксперимента являются, сгенерированные случайным образом, неориентированные графы без петель с числом вершин 4,6,8. Для каждой размерности было проведено 50 тестов. Результаты эксперимента представлены в таблице 1.

Таблица 1. Результаты вычислительного эксперимента

Число вершин	Среднее время работы, с	Максимальное время работы, с
4	0.159950	0.2321379
6	0.162119	0.2392566
8	0.225100	0.3440656

### Заключение.

Оценивая полученные результаты, можно сделать вывод о возможности использования SymPy для нахождения хроматического числа графа.

---

## СПИСОК ЛИТЕРАТУРЫ

1. SymPy // <https://github.com/sympy/sympy>
2. SymPy 1.12 documentation // <https://docs.sympy.org/latest/index.html>
3. А. Кофман/ Введение в прикладную комбинаторику. // Москва: Наука, 1975. — 480 с.
4. NetworkX documentation // <https://networkx.org/documentation/stable/index.html>
5. NetworkX // <https://github.com/networkx/networkx>

**Р.И. Комоцкий<sup>1</sup>, Н.В. Болдырихин<sup>2</sup>**

### ТЕХНОЛОГИЯ КОМПЬЮТЕРНОГО ЗРЕНИЯ НА ОСНОВЕ НЕЙРОСЕТЕЙ

Донской государственный технический университет, г. Ростов-на-Дону, Россия<sup>1</sup>  
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: информационные технологии, искусственный интеллект, компьютерное зрение, информационное общество.

В статье рассмотрены технологии компьютерного зрения, которые предназначены для решения различных задач, использующие современные методы контроля, прогнозирования и классификаций объектов.

**R.I. Komotskiy<sup>1</sup>, N.V. Boldyrikhin<sup>2</sup>**

### COMPUTER VISION TECHNOLOGY BASED ON NEURAL NETWORKS

Don State Technical University (DSTU), Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: information technology, artificial intelligence, computer vision, information society.

The article considers computer vision technologies, which are designed to solve various problems using modern methods of control, prediction and classification of objects.

Технология компьютерного зрения широко используется в различных областях науки, сельского хозяйства, робототехники, отраслях промышленности для определения многих характеристик: геометрических размеров объектов, контроля безопасности процессов и объектов, оценки состояния сельхозугодий и т.д. [1,2]. Информацию, которую можно получить с помощью методов компьютерного зрения можно разделить на цвет, размер, форму и текстуру и т.д. Такие методы могут использоваться для контроля и прогнозирования химических реакций, для классификации объектов по их цвету, форме, дефектам и однородности и т.д. [1,2].

Есть два основных подхода к решению этих задач. Классический подход и подход на основе использования искусственного интеллекта.

Классический подход включает использования 2D и 3D оптических систем.

Многие задачи решаются классическими 3D - системами, такими, например, как 3D - сканеры, которые очень хорошо справляются с формированием 3D – моделей,

---

измерением и контролем геометрических параметров, однако их точность недостаточна для проведения прецизионных измерений, кроме того, они непригодны для плоских объектов. Для таких объектов зачастую используют классические 2D-системы. Среди классических методов работы с изображениями выделяют такие, как: адаптивная бинаризация; морфологические преобразования; повышение контраста; выделение по цвету.

Такие методы позволяют проводить измерения с высокой точностью, однако они обладают рядом существенных недостатков. Классические 2D-системы плохо решают задачи в условиях высокой зашумленности, низкой контрастности изображений. В этих условиях гораздо лучше работают 2D-системы на основе искусственного интеллекта. Существует несколько концепций использования искусственного интеллекта в оптических системах: линейная регрессия, логистическая регрессия, деревья принятия решений и их ансамбли, градиентный бустинг, нейронные сети.

Главным преимуществом нейросетей является то, что по качеству удается достичь более высоких результатов в большинстве сложных задач, которые классическими методами решить довольно затруднительно. Это такие задачи, как распознавание, классификация объектов, локализация, обнаружение, сегментация и т.д. [1,2].

Достоинствами систем на нейросетях являются инвариантность к сдвигу объекта на изображении, изменению масштаба, к различным ротациям, низкая чувствительность к шумам. Эти неоспоримые достоинства обусловили быстрое развитие и широкое распространение нейронных сетей в оптических системах измерения, контроля и т.д.

Вместе с тем, с использованием нейронных сетей связаны некоторые трудности, которые часто играют значительную роль – это трудоемкость, длительность процесса обучения, сложность формирования обучающей выборки. Таким образом внедрение нейросети это долгий и сложный процесс. Так же необходимы большие вычислительные мощности при обучении сети, так и в процессе эксплуатации оптической системы на основе нейросети.

В связи с этим в промышленности для повышения эффективности решаемых задач зачастую используют комбинацию классических технологий компьютерного зрения и технологий на основе нейросетей.

Рассмотрим задачи, решаемые системами компьютерного зрения на основе нейросетей:

Мультиклассовая детекция объектов, т.е. обнаружение объектов в области изображения, в которой присутствуют какие-то объекты различных классов, в этой задаче точность решения не играет роли, просто необходимо определить объекты каких классов присутствуют, например человек, автомобиль, животное, строение и т.д. Нейронные сети являются универсальным средством аппроксимации функций, что позволяет их использовать в решении задач мультиклассовой детекции. При решении данных задач используются различные детекторы.

Правильный подбор оптической камеры, в сочетании с качественными 2D-алгоритмами компьютерного зрения, позволяет обеспечить высокое качество решения задач и оптимально спланировать затраты, не переплачивая за избыточный функционал.

Задача классификации — это задача маркирования изображений. Решение задачи помогает определить: содержится ли какой-либо объект на данном изображении. В настоящее время эта задача является вспомогательной, и решается после мультиклассовой детекции для уточнения её результатов. Для решения задачи классификации реализуется отдельная нейросеть - классификатор.

Сегментация — это процесс выделения на изображении интересующих объектов. Сегментация применяется во многих областях, например, в производстве для индикации дефектов при сборке деталей, в медицине для первичной обработки снимков, также для составления карт местности по снимкам со спутников.

Для каждой задачи применяются определенные архитектуры нейросетей.

---

Для начала рассмотрим достаточно простую задачу классификации.

Задачу классификации в упрощенном виде можно сформулировать как задачу предсказания по объекту: какому классу он принадлежит. Для сложных задач классификации используются многослойные полносвязные нейронные сети или многослойные персептроны. Такие персептроны позволяют получать распределение вероятностей принадлежности объекта тому или иному классу, затем можно выбрать тот класс, который соответствует максимальной вероятности и это будет наш финальный ответ на задачу классификации [1].

Рассмотрим еще один тип - рекуррентные нейронные сети. Рекуррентные сети учитывают последовательность поступления информации на вход. В традиционных нейронных сетях подразумевается, что все входы и выходы независимы. Но для многих задач это не подходит. Если необходимо предсказать следующее слово в предложении, то нужно учитывать предшествующие ему слова. Нейронные сети называются рекуррентными, потому что они выполняют одну и ту же задачу для каждого элемента последовательности, причем выход зависит от предыдущих вычислений.

По сути, используется выход нейрона на предыдущем шаге, складываем его с входом на текущем шаге и результат пропускается через функцию активации. В итоге получается выход нейрона на текущем шаге. Этот процесс продолжается во времени. Важной чертой такой системы является её неустойчивость к обучению: чем длиннее последовательность, тем хуже она обучается. Это связано с особенностью алгоритма обратного распространения ошибки. В результате эволюции этой архитектуры появились сети с нейронами долгосрочной и краткосрочной памяти, что позволило значительно повысить обучаемость сети [1,2].

Для решения задачи распознавания и классификации изображений часто используются свёрточные сети.

Название архитектура сети получила из-за наличия операции свёртки, суть которой в том, что каждый фрагмент изображения умножается на матрицу (ядро) свёртки поэлементно, а результат суммируется и записывается в аналогичную позицию выходного изображения [2]. Работа свёрточной нейронной сети обычно интерпретируется как переход от конкретных особенностей изображения к более абстрактным деталям, и далее к ещё более абстрактным деталям вплоть до выделения понятий высокого уровня. При этом сеть самонастраивается и вырабатывает сама необходимую иерархию абстрактных признаков (последовательности карт признаков), фильтруя маловажные детали и выделяя существенное.

Следует отметить, что для эффективного решения сложных задач могут использоваться комбинированные сети, содержащие, например, сверточные и полносвязные слои, или рекуррентные и сверточные. Такие сети могут использоваться при трекинге объектов в видеопотоке, где важно не только качественная детекция, но и учет последовательности движения объекта во времени.

## СПИСОК ЛИТЕРАТУРЫ

1. Короченцев Д.А. и др. Применение технологий искусственного интеллекта и теории поддержки принятия решений в задачах информационной безопасности. ДГТУ. Ростов-на-Дону, 2022.
2. Гильнич Д. С. Программа для нейросетевой обработки массива сенсорных данных. Сборник трудов научно-технических конференции «Интеллектуальные, сенсорные и мехатронные системы-2022» Белорусский Национальный Технический Университет Минск, Беларусь, 2022, С. 153-154.

---

**В.И. Юхнов<sup>1</sup>, А.И. Сосновский<sup>2</sup>, Н.В. Болдырихин<sup>2</sup>, И.А. Сосновский<sup>2</sup>**

**ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ РЕШЕНИЯ ЗАДАЧИ  
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ В СЕТЯХ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Федеральное государственное бюджетное образовательное учреждение высшего  
образования Донской государственной технической университет (ДГТУ).  
Город Ростов-на-Дону. Россия<sup>2</sup>

Ключевые слова: искусственный интеллект, нейронные сети, аномалии сетевого трафика, атака DDoS, системы обнаружения вторжений IDS.

В статье рассмотрены общие подходы к определению аномалий сетевого трафика при реализации злоумышленником сетевых атак на инфраструктуру компании с использованием нейронных сетей. Проанализированы имеющиеся на рынке как зарубежные, так и отечественные компании, профессионально занимающиеся разработкой нейросистем для отрасли кибербезопасности и их продукты.

**V.I. Yukhnov<sup>1</sup>, A.I. Sosnovskiy<sup>2</sup>, N.V. Boldyrikhin<sup>2</sup>, I.A. Sosnovskiy<sup>2</sup>**

**THE USE OF ARTIFICIAL INTELLIGENCE TO SOLVE THE PROBLEM OF  
ENSURING THE SECURITY OF INFORMATION TRANSMITTED IN NETWORKS**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Federal State Budgetary Educational Institution of Higher Education Don State Technical  
University (DSTU).  
The city of Rostov-on-Don. Russia<sup>2</sup>

Keywords: artificial intelligence, neural networks, network traffic anomalies, DDoS attack, IDS intrusion detection systems.

The article discusses general approaches to determining network traffic anomalies when an attacker implements network attacks on a company's infrastructure using neural networks. Both foreign and domestic companies professionally engaged in the development of neural systems for the cybersecurity industry and their products are analyzed on the market.

В современном мире компьютерные сети находятся в центре нашей деятельности, и их безопасность становится все более важной. В то же время, киберугрозы продолжают эволюционировать, становясь все более сложными и совершенными. В таких условиях обеспечение безопасности сети требует постоянного совершенствования.

Искусственный интеллект (ИИ) – это область компьютерной науки, которая изучает, как компьютеры могут имитировать человеческое мышление и разум. Он предлагает инновационные решения для решения многих сложных проблем, включая безопасность сети.

Применение ИИ в обеспечении безопасности сети может помочь в выявлении и предотвращении кибератак. ИИ-системы могут анализировать огромные объемы данных и выявлять аномалии, которые могут указывать на возможные атаки или угрозы. Это позволяет операторам сети реагировать на такие угрозы значительно быстрее, чем это делали бы ручные методы анализа.

Одним из примеров применения ИИ является система обнаружения вторжений (IDS). IDS использует алгоритмы машинного обучения для анализа сетевых данных и

---

выявления необычной активности (аномалий), которая может указывать на взлом или другую кибератаку. Это позволяет операторам сети реагировать на угрозы еще до того, как они причинят серьезный ущерб [1].

Аномалии сетевого трафика включают различные типы ненормального или подозрительного поведения, которые могут указывать на наличие угрозы безопасности или проблем с сетевой инфраструктурой.

Аномалии можно выявить при реализации злоумышленником различного вида атак. Некоторые примеры аномалий сетевого трафика могут включать:

1. Атаки отказа в обслуживании (DDoS). Это атаки, при которых злоумышленники создают высокую нагрузку на целевую сеть путем отправки огромного количества запросов или пакетов данных. Это может вызвать отказ в обслуживании легитимных пользователей или ослабление производительности сети.
2. Сканирование портов. Злоумышленники сканируют открытые порты на серверах или устройствах сети, чтобы найти уязвимости или проблемы безопасности. Сканирование портов может указывать на потенциальную атаку или злоумышленный поиск уязвимостей.
3. Аномальная передача данных. Если сетевая активность не соответствует ожидаемому шаблону трафика или активности, это может указывать на аномалию в сетевом трафике. Например, если большой объем данных передается с одного сервера на другой без видимых причин, это может быть маркером того, что происходит аномальная активность.
4. Незащищенная аутентификация или доступ. Аномальный трафик может включать неудачные попытки входа в систему или обнаружение попыток несанкционированного доступа к сетевым ресурсам. Это может указывать на взлом или попытки несанкционированного доступа в сеть.
5. Нестандартные или аномальные протоколы. Аномальный трафик может включать использование необычных или незащищенных протоколов, которые не соответствуют стандартам или политикам безопасности сети. Это может указывать на атаку или попытку обойти защиту сети.

Выделение и описание конкретного вида аномалий в сетевом трафике в значительной степени зависит от решаемой задачи.

Для поиска аномалий в трафике данных можно использовать некоторые типы нейронных сетей. В частности, рекуррентные нейронные сети (РНС), хорошо подходят для анализа последовательных данных, таких как временные ряды. Они могут быть использованы для обнаружения аномалий в трафике данных, основываясь на истории предыдущих данных о трафике.

В свою очередь, сверточные нейронные сети (СНС), часто используются для обработки изображений, но они также могут быть применены к трафику данных. Они могут использоваться для поиска аномалий в данных, основываясь на структуре и форме пакетов данных.

Также можно выделить такие нейросети как глубокие автоэнкодеры (ГАЭ). Это нейронные сети, которые могут использоваться для изучения скрытых представлений данных. Они могут быть использованы для поиска аномалий в трафике данных, идентифицируя различия между входными данными и их восстановленными версиями.

Ну и безусловно, что при решении задачи поиска аномалий могут использоваться гибридные модели нейросетей. Возможно, лучший подход - это комбинирование нескольких типов нейронных сетей, чтобы получить лучшую производительность при обнаружении аномалий в трафике данных. Например, можно использовать сочетание РНС и СНС для учета как последовательной природы данных, так и их структуры.

---

Безусловно, что перечисленные нейросети являются только набором инструментов для решения задачи. Важно подобрать модель, которая в наибольшей степени соответствует специфике и требованиям рассматриваемого трафика данных.

На сегодняшний день есть ряд компаний, профессионально занимающихся разработкой нейросистем для отрасли кибербезопасности.

Компания Deep Instinct использует глубокие нейронные сети для обнаружения и предотвращения различных видов киберугроз, включая известные и неизвестные вредоносные программы и атаки [2]. Они используют свои нейросети, обученные на больших наборах данных о вредоносных действиях, для прогнозирования аномалий в реальном времени и предупреждения пользователей.

Компания Vectra AI использует глубокое обучение для обнаружения скрытых угроз и аномалий в сети. Их система анализирует сетевой трафик и обнаруживает аномалии, такие как незащищенный доступ к ресурсам, атаки с боковых каналов и подмена сетевого трафика [3].

Помимо зарубежных компаний в данном секторе рынка активно учувствуют Российские компании. На данный момент в России разрабатывается и применяется несколько систем обнаружения вторжений IDS на основе нейросетей. Например, IDS "Аналитик", разработанный Международным центром информационной безопасности. "Аналитик" использует методы машинного обучения и нейросетевой анализ для обнаружения кибератак. Также известны IDS "Континент", разработанный Институтом системного анализа РАН. IDS "Armada" разработанная компанией Positive Technologies.

Искусственный интеллект также может быть использован для создания прогнозных аналитических моделей, которые помогают предсказывать уязвимости и угрозы безопасности сети. Это особенно полезно для компаний и организаций, которые хотят предотвратить угрозы до их возникновения. С помощью ИИ-систем предупреждение о будущих атаках становится возможным и позволяет реагировать на них даже до их начала.

Помимо уже рассмотренных, ИИ-технологии могут быть использованы для реализации различных методов идентификации и аутентификации пользователей. Номенклатура таких задач весьма обширна. Это и распознавание лица, распознавание отпечатков пальцев, голосовая биометрия, распознавание поведения, определение и распознавание биометрической структуры.

Необходимо отметить, что использование ИИ-технологий в идентификации и аутентификации пользователей имеет преимущества по сравнению с традиционными методами, такими как пароли или PIN-коды. Они обеспечивают более высокий уровень безопасности, так как характеристики и поведение пользователя сложнее подделать или скопировать. Кроме того, ИИ-системы могут автоматически адаптироваться к изменениям в поведении или физических характеристиках пользователя, обеспечивая более удобный и надежный опыт.

Таким образом, эффективное применение ИИ может значительно улучшить процессы, способствующие повышению безопасности передаваемых по сети данных. Однако, несмотря на все преимущества, есть и некоторые вызовы, с которыми сталкиваются ИИ-системы в контексте обеспечения безопасности сети. Интеллектуальные атаки и контрмеры могут использоваться для обмана ИИ-систем и превышения их возможностей. Поэтому разработчики должны постоянно обновлять свои алгоритмы и модели, чтобы оставаться впереди киберугроз.

## СПИСОК ЛИТЕРАТУРЫ

1. Сосновский И.А., Коршун А.М., Сосновский А.И., Коробенко С.В. Подход к построению защищённых инфокоммуникационных сетей связи. // «ИНФОКОМ 2021» / Труды Северо-Кавказского филиала Московского технического

- 
- университета связи и информатики - Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2021, с. 290 – 293.
2. Сайт компании Deepinstinct – URL: <https://www.deepinstinct.com> (дата обращения: 24.09.2023).
  3. Сайт компании ectra – URL: <https://www.vectra.ai> (дата обращения: 24.09.2023).

**В.Г. Кобак<sup>2</sup>, Д.И. Киянов<sup>2</sup>, С.А. Швидченко<sup>1</sup>, С.Д. Ермакова<sup>2</sup>**

## **СРАВНЕНИЕ ЖАДНОГО АЛГОРИТМА NETWORKX С МЕТОДОМ MAGU**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Донской государственный технический университет, Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: хроматическое число, NP-полная задача, NetworkX

В работе сравнивается точность и время вычисления хроматического числа для связных неориентированных графов без петель с использованием библиотеки NetworkX и метода Magu. Полученные результаты обеспечивают важные сведения о применимости обоих методов в ограниченном контексте, что имеет значимость для эффективного решения практических задач графовой оптимизации.

**V.G. Kobak<sup>2</sup>, D.I. Kiyanov<sup>2</sup>, S.A. Shvidchenko<sup>1</sup>, S.D. Ermakova<sup>2</sup>**

## **THE COMPARISON OF THE GREEDY NETWORKX ALGORITHM WITH THE MAGOO METHOD**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Don State Technical University, Rostov-on-Don, Russia<sup>2</sup>

Keywords: chromatic number, NP-complete problem, NetworkX.

This work compares the accuracy and computation time of the chromatic number for connected undirected graphs without loops using the NetworkX library and Magoo's method. The results provide important insights into the applicability of both methods in a restricted context, which is significant for efficiently solving practical graph optimisation problems.

### **Введение.**

В современном мире графовых структур задачи оптимизации играют ключевую роль в различных областях, начиная от социальных сетей и заканчивая логистикой. Одной из таких задач является определение хроматического числа графа, которое требует минимального числа цветов для раскраски вершин графа так, чтобы никакие две смежные вершины не имели одинаковый цвет. При этом точные вычисления данного числа являются вычислительно сложной задачей, особенно в случае больших графов.

В данной работе фокус сосредотачивается на двух методах решения этой задачи: библиотеке NetworkX, широко используемой в анализе графов, и методе Magu, основанном на приведении конъюнктивной нормальной формы (КНФ) в дизъюнктивную нормальную форму (ДНФ). Исследование ограничивается анализом точности и времени выполнения обоих методов на связных неориентированных графах без петель.



---

Цель данного исследования - сравнить эффективность обоих методов в ограниченном контексте их применения и выявить наилучший подход для данного типа графов. Работа вводит в анализ оптимизации графовых структур, исследуя возможности и ограничения различных методов.

#### **Постановка задачи.**

Для простого, неориентированного графа без петель и кратных ребер хроматическим числом называется количество цветов, в которые можно раскрасить граф, при условии, что соседние вершины не могут быть окрашены в один цвет.

Нахождение хроматического числа методом Магу подразумевает 2 этапа:

Нахождение устойчивых множеств путем построения формулы смежности графа, с последующим приведением к ДНФ, выполнив все возможные поглощения.

Определение хроматического числа заданного графа. Для этого полученная формула ДНФ проходит преобразования, на выходе которых получится формула КНФ, которую необходимо преобразовать в ДНФ.

Более быстрый, но в то же время менее точный метод строен в известную библиотеку NetworkX, которая разработана для работы с графами и их анализом.

Таким образом, суть задачи в сравнении времени и точности методов, для этого необходимо применить оба метода к одному графу, сравнить их результат и время выполнения.

#### **Жадный алгоритм в NetworkX.**

Библиотека NetworkX разработана для работы с графами. Она позволяет хранить графы и их связи, включая вес связи. Также позволяет применить ряд уже разработанных методов для анализа, включая `greedy_color(G, strategy='largest_first', interchange=False)`. На вход принимает параметра. `G` – объект класса NetworkX graph, принимает граф, для которого будет предпринята попытка раскрасить вершины графа минимально возможным количеством цветов.

`strategy` – по умолчанию `largest_first`. Определяет стратегию нахождения раскраски. Может принимать значения: `'largest_first'`, `'random_sequential'`, `'smallest_last'`, `'independent_set'`, `'connected_sequential_bfs'`, `'connected_sequential_dfs'`, `'connected_sequential'` (псевдоним предыдущей стратегии), `'saturation_largest_first'`, `'DSATUR'`. В данной работе будет сделан упор на `largest_first`, поскольку данное значение является значение по умолчанию, а в задачу работы не входит сравнение стратегий жадного алгоритма.

`interchange` - по умолчанию `False`. Может принимать `True`. В случае `True`, будет использоваться альтернативный алгоритм чередования цветов, описанный Мацей М. Sysło (Maciej M. Sysło, Discrete Optimization Algorithms with Pascal Programs, 415-424, 1983. ISBN 0-486-45353-7). В данной работе будет использоваться значение по умолчанию.

На выходе возвращается словарь, ключем являются вершины, а значения являются использованными цветами. Максимальное значение словаря +1 является хроматическим числом графом. +1 поскольку номера цветов начинаются с нуля.

#### **Программная реализация.**

Например, для графа `G`, представленном на рисунке 1.

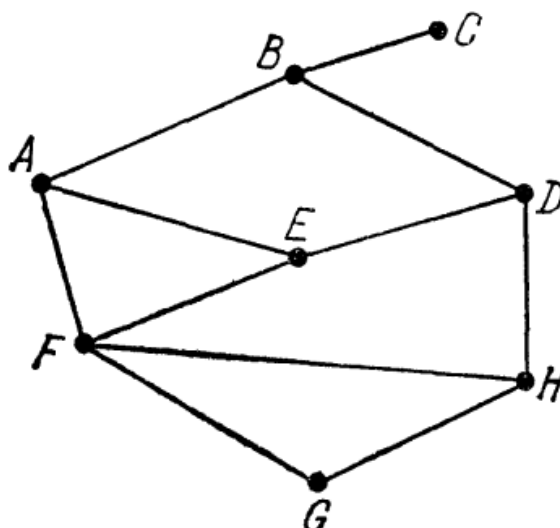


Рисунок 1. Граф G

Создается элемент класса NetworkX graph. Используя `add_node()` и `add_edge()` вносятся информация о графе. Используя `time`, происходит запись системного времени системы, применяется `greedy_color()`. К полученному словарию применяется `max(greedy_color().values()) + 1`. После получения числа, читается новое системное время, из которого вычитается ранее записанное.

После аналогичным образом, записывается время выполнения методом `MaGu`. Запись времени, выполнение алгоритма метода `MaGu`, чтение нового времени с последующим вычитанием ранее записанного времени.

Для сравнения точности, по окончании вычисления происходит сравнение результатов. В случае их отличия, к счетчику прибавляется единица.

#### Вычислительный эксперимент.

С помощью программного средства, написанного на языке программирования Python, был проведен вычислительный эксперимент, по проверке эффективности `SymPy` для поиска хроматического числа. Использовался компьютер с процессором Ryzen 5 5500 4.45 ГГц и оперативной памятью объемом 32Гб DDR4. Исходными данными эксперимента являются, сгенерированные случайным образом, неориентированные графы без петель с числом вершин 4,6,8. Для каждой размерности было проведено 100 тестов. Результаты эксперимента представлены в таблице 1.

Таблица 1. Результаты вычислительного эксперимента

Число вершин	Среднее время работы networkX, с	Среднее время работы метода MaGu, с	Количество отличий на 100 графов.
4	0.000010052	0.165355792	0
6	0.000010321	0.165993495	1
8	0.000010769	0.229661176	3

#### Заключение.

Оценивая результаты тестирования, можно сделать вывод о возможности использования отличного от жадного алгоритма, для точного нахождения хроматического числа графов, число вершин которого больше 6.

---

## СПИСОК ЛИТЕРАТУРЫ

1. SymPy // <https://github.com/sympy/sympy>
2. SymPy 1.12 documentation // <https://docs.sympy.org/latest/index.html>
3. А. Кофман/ Введение в прикладную комбинаторику. // Москва: Наука, 1975. — 480 с.
1. 4.NetworkX documentation // <https://networkx.org/documentation/stable/index.html>
4. NetworkX // <https://github.com/networkx/networkx>

**А.И. Дубровина**

### **ДЕТЕКЦИЯ ИНЦИДЕНТОВ ПРИ ВОЗНИКНОВЕНИИ СБОЕВ В СИСТЕМЕ «УМНЫЙ ДОМ»**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,  
Ростов-на-Дону, Россия

Ключевые слова: умный дом, инциденты информационной безопасности.

Искусственный интеллект (ИИ) играет важную роль в управлении системой безопасности умного дома. Использование ИИ позволяет создать интеллектуальные и адаптивные системы безопасности.

В настоящей работе представлены и проанализированы основные аспекты систем безопасности «умного дома» комбинация моделей и алгоритмов которых могут обеспечить оптимальную производительность и эффективность данных систем.

**A.I. Dubrovina**

### **DETECTION OF INCIDENTS WHEN FAILURES OCCUR IN THE SMART HOME SYSTEM**

Federal State Budgetary Educational Institution of Higher Education  
«Don State Technical University», Rostov-on-Don, Russia

Keywords: smart home, threat model, information security incidents.

Artificial intelligence (AI) plays an important role in managing the security system of a smart home. The use of AI allows you to create intelligent and adaptive security systems.

This paper presents and analyzes the main aspects of smart home security systems, the combination of models and algorithms that can ensure optimal performance and efficiency of these systems.

#### **Введение.**

Детекция инцидентов в системах умного дома становится все более актуальной в связи с ростом популярности этих систем. Умные дома предоставляют возможность автоматизировать и контролировать различные устройства и процессы, что делает жизнь человека более комфортной и безопасной.

Однако, как и в любой системе, возможны инциденты, такие как сбои в работе устройств, потеря связи с сервером, несанкционированный доступ к системе и т.д. В таких

---

случаях своевременное обнаружение инцидентов и принятие мер по их устранению становится критически важным.

Детекция инцидентов позволяет выявить и устранить проблемы на ранней стадии, что может предотвратить более серьезные последствия и сэкономить время и ресурсы. Кроме того, системы умного дома становятся все более популярными среди злоумышленников, поэтому обеспечение безопасности и своевременное обнаружение несанкционированного доступа также является важной задачей [1].

В целом, детекция инцидентов в умном доме становится все более важным направлением развития технологий, позволяющим обеспечить безопасность и комфорт пользователей.

#### **Постановка задачи.**

Методы исследования. Обнаружение инцидентов в умных домах является сложной задачей из-за большого количества устройств и возможных сбоев. Однако, с помощью современных технологий и методов, можно эффективно обнаруживать и устранять инциденты.

Цель обнаружения инцидентов заключается в обеспечении безопасности и надежности систем умного дома. Для ее достижения необходимо определить методы и инструменты обнаружения и устранения инцидентов. Методы заключаются в анализе данных с устройств, мониторинге активности пользователей, обнаружение аномалий в работе системы.

Для достижения поставленной цели работы были поставлены следующие задачи детекции инцидентов в системе «умный дом»:

- обнаружение сбоев в работе устройств и систем;
- выявление несанкционированного доступа к данным и системе;
- мониторинг активности пользователей и выявление подозрительных действий;
- разработка мер по предотвращению утечек конфиденциальной информации;
- обеспечение своевременное информирования пользователей о возникших проблемах;
- разработка рекомендаций по улучшению безопасности системы.

#### **Анализ использования ИИ в системах умного дома.**

Искусственный интеллект (ИИ) играет важную роль в управлении системой безопасности умного дома. Использование ИИ позволяет создать более интеллектуальные и адаптивные системы безопасности. Вот несколько способов, которыми ИИ применяется в управлении системой безопасности умного дома:

1. Распознавание лиц: Система безопасности с ИИ может обладать функциями распознавания лиц. С помощью камер и алгоритмов ИИ система может идентифицировать различные лица, допущенных к доступу в дом, и предоставлять им автоматическую разблокировку дверей или управление другими устройствами в доме. ИИ также может автоматически настраивать уровень безопасности на основе распознанного лица.
2. Обнаружение инцидентов: ИИ может анализировать видеопотоки с камер и автоматически обнаруживать подозрительные или необычные события. Например, ИИ может определить вторжение или неправильное поведение и сразу же сигнализировать об этом, отправлять уведомление владельцу или активировать систему тревоги.
3. Анализ аудио: ИИ может также анализировать аудиопотоки в помещении и распознавать звуки, которые могут указывать на потенциальную угрозу или опасность, например, звук разбития стекла или сигнал пожарной сигнализации. ИИ может активировать соответствующие устройства или системы сигнализации при необходимости.
4. Предупреждение о возможных опасностях: ИИ может на основе анализа данных сочетать информацию о погоде, пожаре, взломе и других опасностях,

---

чтобы предупредить владельца умного дома о возможных угрозах и предложить соответствующие рекомендации по действиям.

5. Умные замки и системы безопасности: ИИ может управлять умными замками, сенсорами и другими устройствами безопасности в доме. ИИ может контролировать состояние замков, настраивать режимы доступа, отправлять оповещения о входе или выходе из дома, а также вести учет и анализировать данные безопасности для последующего применения.

Эти примеры показывают, как ИИ в системе повышения продуктивности системы умного дома может помочь улучшить безопасность и создать более автоматизированную и защищенную среду для жильцов, что подчеркивает актуальность настоящей работы.

Система повышения продуктивности системы «умный дом» может быть построена на основе следующих принципов:

1. Автоматизация и управление: Основным принципом умного дома - это автоматизация и управление различными устройствами. Система должна быть способна контролировать и управлять освещением, кондиционированием воздуха, безопасностью, электроприборами и другими устройствами в доме. Автоматизация позволяет пользователям настраивать определенные сценарии и задачи, которые выполняются автоматически по расписанию или по определенным событиям.
2. Интеграция различных устройств: Система «умный дом» должна быть способна интегрировать различные устройства и технологии. Это может включать в себя умные датчики, камеры видеонаблюдения, управляемые розетки, системы безопасности и другие. Интеграция позволяет создавать связанные системы, которые взаимодействуют между собой и предоставляют единый интерфейс для управления всеми подключенными устройствами [2].
3. Безопасность и защита данных: Одним из важных принципов в системе «умный дом» является безопасность и защита данных. Вся информация, собираемая и обрабатываемая системой, должна быть защищена от несанкционированного доступа. Она также должна иметь механизмы обнаружения и предотвращения взлома, а также обеспечивать безопасность при выполнении сценариев и задач автоматизации [3].
4. Аналитика и оптимизация: Система «умный дом» может использовать аналитику и оптимизацию для определения использования ресурсов, управления энергопотреблением и прогнозирования тенденций или потребностей пользователей. Анализ данных и прогнозирование позволяют системе быть эффективной и адаптивной к изменяющимся условиям и предпочтениям пользователей.
5. Использование искусственного интеллекта: Искусственный интеллект (ИИ) играет важную роль в системе «умный дом». Он обеспечивает распознавание и анализ данных, предсказание и принятие решений на основе собранных данных. ИИ позволяет сформировать интеллектуальную систему, которая может учитывать предпочтения пользователей и работать в автономном режиме для оптимизации комфорта и эффективности умного дома [4].

Эти принципы позволяют создать систему «умный дом» с повышенной продуктивностью, удобством, безопасностью и эффективностью. Они обеспечивают лучший контроль, комфорт и оптимизацию использования ресурсов в умном доме.

#### **Обнаружение инцидентов и событий в системах умного дома.**

Одной из возможных причин нарушения корректной работы в системах умного дома являются сбои в работе устройств, которые могут привести как к частичному, так и к полному выводу системы из строя.

На основе анализа выявлены следующие основные способы обнаружения сбоев в работе устройств и систем умного дома:

- 
1. Мониторинг датчиков и устройств в реальном времени: с помощью приложения умного дома или голосового помощника, такого как, например, «Алиса» от компании Yandex, можно отслеживать состояние различных устройств и датчиков в режиме реального времени. Если устройство перестает отвечать на команды или перестает передавать данные, это может указывать на сбой в его работе [5].
  2. Уведомления о событиях: Многие системы умного дома отправляют уведомления на смартфон или другое устройство при возникновении определенных событий, таких как открытие двери, изменение температуры или срабатывание датчика движения. Если система перестает отправлять уведомления, это может быть признаком сбоя.
  3. Использование журнала событий. В приложении умного дома часто есть возможность просмотра истории событий, произошедших в системе. Если какое-то событие не отображается в журнале или отображается некорректно, это может свидетельствовать о сбое в работе системы [6].
  4. Самодиагностика и автоматическое уведомление. Некоторые системы умного дома имеют встроенные функции самодиагностики, которые могут обнаружить и уведомить пользователя о возможных сбоях.
  5. Регулярное обслуживание и обновление устройств. Во избежание сбоев в работе устройств умного дома, также необходимо регулярно обновлять их программное обеспечение и проводить техническое обслуживание [7].

#### **Заключение.**

Таким образом, благодаря ИИ появились возможности детектировать инциденты на ранних стадиях, тем самым позволяя, предотвратить возможный ущерб, наносимый автоматизированным системам.

#### **СПИСОК ЛИТЕРАТУРЫ**

1. Choi, Sangho et al. Smart Home Security: An Overview of Technologies and Issues. Communications Magazine, IEEE, vol. 54, no. 12, 2016, pp. 16-22.
2. Alrawais, Abdulaziz et al. A Survey on Smart Home Technologies and Internet of Things (IoT) Frameworks." Journal of Network and Computer Applications, vol. 97, 2017, pp. 1-29.
3. Ali, Syed Taha et al. «Security and Privacy Approaches in Internet of Things (IoT) based Smart Home Systems: A Review.» Journal of Network and Computer Applications, vol. 116, 2018, pp. 1-27.
4. Jin, Haoning et al. Concurrency-Related Smart Home Security in Internet of Things. IEEE Internet of Things Journal, vol. 7, no. 6, 2020, pp. 5158-5173.
5. Xiong, Ping et al. "A Review of the Security of Smart Home Systems based on Low-Power Wireless Protocols. Future Generation Computer Systems, vol. 111, 2020, pp. 253-267.
6. Alotaibi, Abdulrahman H. et al. A Comprehensive Survey of Security Solutions in Smart Home Environments. Computers & Electrical Engineering, vol. 87, 2020, Article 106844.
7. Qadir, Junaid et al. Securing Internet of Things-based Smart Homes: A Review. Journal of Network and Computer Applications, vol. 168, 2020, Article 102736.

## ИСПОЛЬЗОВАНИЕ ИНПЕЙНТИНГА В КОМПЬЮТЕРНОЙ ГРАФИКЕ: СОЗДАНИЕ РЕАЛИСТИЧНЫХ ВИРТУАЛЬНЫХ МИРОВ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»

Ключевые слова: инпейнтинг, компьютерная графика, виртуальные миры, реалистичность, алгоритмы, машинное обучение, глубокое обучение.

В данной работе исследуется использование инпейнтинга в компьютерной графике для создания виртуальных миров. Она охватывает различные алгоритмы и методы, которые позволяют заполнять пропуски и удалять объекты из изображений, достигая высокой степени реалистичности. Результаты исследования могут быть применены в различных областях, включая не только виртуальную реальность, но компьютерные игры и визуализацию данных.

M.V. Kutuzov

## USING INPAINTING IN COMPUTER GRAPHICS: CREATING REALISTIC VIRTUAL WORLDS

Federal State Budget Educational Institution of Higher Education  
"Don State Technical University"

Keywords: inpainting, computer graphics, virtual worlds, realism, algorithms, machine learning, deep learning.

This topic explores the use of inpainting in computer graphics for creating virtual worlds. It covers various algorithms and methods that enable the filling of gaps and removal of objects from images, achieving a high degree of realism. The research findings can be applied in various domains, including not only virtual reality, but also computer games and data visualization.

### **Введение.**

Тема использования инпейнтинга в компьютерной графике для создания реалистичных виртуальных миров является актуальной в современном мире. С развитием технологий компьютерной графики и виртуальной реальности, пользователи становятся все более требовательными к визуальному опыту. Использование инпейнтинга позволяет достичь более реалистичных и убедительных визуальных эффектов, что важно для создания увлекательных виртуальных миров.

Инпейнтинг является эффективным инструментом для заполнения пропусков в изображении, что может быть полезно при работе с большими объемами данных или при восстановлении деталей в текстурах и окружающей среде. Это позволяет улучшить качество визуализации и создать более реалистичные сцены.

Использование инпейнтинга в компьютерной графике имеет практическую значимость для различных областей, включая разработку игр, фильмов, виртуального моделирования и дизайна. Реалистичный и убедительный визуальный опыт, достигаемый с помощью инпейнтинга, может повысить привлекательность продуктов и сделать их более конкурентоспособными на рынке.

Целью работы является рассмотрение основных принципов и методов инпейнтинга, а также его применение в создании виртуальных миров, для создания более реалистичного визуального опыта для пользователей

---

## **Применение виртуальной реальности.**

Инпейнтинг — это техника, которая находит применение не только в восстановлении поврежденных изображений, но и в компьютерной графике для создания реалистичных виртуальных миров. Он позволяет заполнять пропущенные области изображений и создавать непрерывные и гармоничные сцены.

Инпейнтинг находит широкое применение в сфере виртуальной реальности (VR). Виртуальная реальность стремится создать максимально реалистичные и убедительные визуальные эффекты для погружения пользователя в виртуальный мир. Однако, создание полностью реалистичных сцен требует огромного объема данных и вычислительных ресурсов. Инпейнтинг позволяет заполнять пропущенные области сцен и создавать более естественные и убедительные визуальные эффекты [1, 2].

## **Примеры технологий.**

### **1. DeepDream.**

DeepDream — это технология, разработанная Google, которая использует инпейнтинг для создания гиперреалистичных изображений. Она использует нейронные сети и глубокое обучение для заполнения пропущенных областей изображений и создания новых деталей и текстур. DeepDream позволяет создавать уникальные и фантастические визуальные эффекты.

DeepDream основан на глубоких нейронных сетях, которые обучены на больших наборах изображений. Эти нейронные сети учатся выявлять образы и структуры в изображениях, а затем применяют полученные знания для заполнения пропущенных областей и генерации новых деталей.

Одной из ключевых особенностей технологии является её способность создавать гиперреалистичные и фантастические визуальные эффекты. Это достигается путем применения различных фильтров и эффектов к изображению, которые изменяют его визуальное представление и придают ему новые детали и текстуры [3, 4].

### **2. Content-Aware Fill**

Content-Aware Fill — это функция, доступная в графическом редакторе Adobe Photoshop, которая использует инпейнтинг для автоматического заполнения пропущенных областей изображений на основе содержимого окружающих пикселей. Она позволяет легко удалять нежелательные объекты или заполнять пробелы в изображениях, сохраняя при этом естественный вид.

Content-Aware Fill работает следующим образом: пользователь выделяет область, которую нужно удалить или заполнить, а затем выбирает опцию Content-Aware Fill. Photoshop анализирует содержимое окружающих пикселей и на основе этого создает новые пиксели, чтобы заполнить выбранную область. Результатом является естественное и незаметное заполнение или удаление объектов.

Эта функция особенно полезна при удалении нежелательных объектов, таких как провода, автомобили или люди, из сцены. Она также может быть использована для заполнения пробелов, созданных при редактировании изображений или при удалении элементов. Content-Aware Fill позволяет сохранить естественный вид и структуру изображения, делая результаты незаметными [5].

### **3. Neural Style Transfer**

Neural Style Transfer — это технология, которая использует инпейнтинг для комбинирования стиля одного изображения с содержимым другого. Она позволяет создавать уникальные и художественные визуальные эффекты, применяя стиль известных художников.

При использовании Neural Style Transfer (NST), два изображения называются "контентом" и "стилем". Контентное изображение содержит объекты и сцены, которые мы



---

хотим сохранить, а стилевое изображение представляет собой художественный стиль, который мы хотим применить к контенту. Нейронная сеть обрабатывает эти изображения и создает новое изображение, которое сочетает контент из одного изображения с художественным стилем из другого.

Основой для NST являются глубокие нейронные сети, такие как сверточные нейронные сети (CNN). Эти нейронные сети обучены выделять различные структуры и элементы изображения, такие как текстуры, цвета и формы. При применении Neural Style Transfer, контентное и стилевое изображения проходят через предварительно обученную нейронную сеть, которая извлекает их характеристики и создает новое изображение на основе этих характеристик.

Результатом Neural Style Transfer является изображение, которое сочетает контент из одного изображения с художественным стилем из другого. Это позволяет создавать уникальные и художественные визуальные эффекты, которые отражают стиль известных художников или создают совершенно новые визуальные интерпретации.

Применение NST может быть широким, включая создание искусства, графический дизайн, а также улучшение визуальных эффектов в фильмах и видео. Эта технология открывает новые возможности для творчества и экспериментов с визуальными эффектами, позволяя создавать уникальные и впечатляющие результаты [6, 7].

### **Прогресс и будущие возможности.**

Инпейнтинг — это мощная техника в области компьютерной графики, которая позволяет заполнять пропущенные области изображений и создавать естественные и реалистичные визуальные эффекты. Применение инпейнтинга в виртуальной реальности и других областях компьютерной графики открывает возможности для создания убедительных и захватывающих визуальных миров.

### **Преимущества DeepDream по сравнению с аналогами:**

- Уникальность визуальных эффектов. DeepDream создает уникальные и абстрактные визуальные эффекты, которые могут придать изображениям необычный и художественный вид.
- Исследовательский инструмент. Этот алгоритм может использоваться исследователями и художниками для изучения внутренних признаков и паттернов нейронных сетей, что делает его полезным инструментом для понимания работы искусственного интеллекта.
- Легкость внедрения. DeepDream доступен в виде открытого исходного кода, и его реализацию можно настроить для различных задач и целей [8].

### **Преимущества Content-Aware Fill по сравнению с аналогами:**

- Автоматизация. Content-Aware Fill позволяет удалять объекты и заполнять пустое пространство с минимальными усилиями со стороны пользователя. Это делает процесс ретуширования быстрым и удобным.
- Сохранение окружающего контента. Алгоритм учитывает окружающий контент, чтобы создать естественное заполнение. Это делает результаты более реалистичными по сравнению с простым клонированием [9].

### **Преимущества Neural Style Transfer по сравнению с аналогами:**

- Создание художественных эффектов. NST позволяет создавать изображения с художественными стилями, что делает его полезным инструментом для художников и дизайнеров.
- Уникальность результатов. Каждая комбинация стиля и содержания создает уникальное изображение. Это позволяет создавать индивидуальные художественные работы.

- Простота использования. Многие реализации NST доступны в виде готовых приложений и инструментов, что делает его доступным для широкого круга пользователей, не обязательно обладающих глубокими знаниями в области машинного обучения.
- Исследование стилей и креативность. NST может использоваться для изучения различных художественных стилей и экспериментов в области визуального искусства.
- Автоматизация процесса. Приложения NST автоматически применяют стиль к содержимому, что позволяет пользователям легко создавать художественные эффекты, не требуя сложных ручных операций [10].

### **Заключение.**

Использование этих трех технологий в инпейтинге в компьютерной графике позволяет достичь более реалистичных и убедительных визуальных эффектов, что является важным аспектом создания увлекательных виртуальных миров. Они предоставляют возможности для экспериментов с различными стилями, создания уникальных и креативных визуальных эффектов и заполнения пропусков в изображениях. Также они позволяют ускорить и облегчить процесс создания и улучшить визуальное качество конечного продукта. Благодаря этим технологиям, разработчики могут создавать виртуальные миры, которые выглядят еще более реалистичными и захватывающими, что делает их более привлекательными для пользователей и способствует созданию уникального и неповторимого визуального опыта. [1, 2].

### **СПИСОК ЛИТЕРАТУРЫ**

1. Нейросети в компьютерной графике // 27-01-2023 // URL: <https://dzen.ru/a/Y9QTa1yyhVhQ3wxA>
2. Deep Dream Generator // URL: <https://deepdreamgenerator.com/about>
3. TensorFlow // 26-01-2022 // URL: <https://www.tensorflow.org/tutorials/generative/deepdream?hl=ru>
4. Adobe // 26-07-2023 // URL: <https://helpx.adobe.com/photoshop/using/content-aware-fill.html>
5. Neural Style Transfer: Everything You Need to Know // Pragati Baheti // 08-09-2021 // URL: <https://www.v7labs.com/blog/neural-style-transfer>
6. TensorFlow // 26-01-2022 // URL: [https://www.tensorflow.org/tutorials/generative/style\\_transfer?hl=ru](https://www.tensorflow.org/tutorials/generative/style_transfer?hl=ru)
7. Генератор Deep Dream: быстро создавайте уникальные высококачественные изображения с помощью искусственного интеллекта. // URL: <https://vivevirtual.es/ru/inteligencia-artificial/deep-dream-generator-genera-rapidamente-imagenes-unicas-y-de-alta-calidad-con-ia/>
8. Photoshop и функция Content Aware Fill // 13-10-2023 // URL: <https://cluecove.ru/photoshop-i-funktsiya-content-aware-fill/?ysclid=lnyj7dbyls922313831>
9. Neural Style Transfer // URL: <https://www.engati.com/glossary/neural-style-transfer>

## ОБЗОР СУЩЕСТВУЮЩИХ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И ИХ СРАВНЕНИЯ С ТОЧКИ ЗРЕНИЯ ЭФФЕКТИВНОСТИ СБОРА И ОБРАБОТКИ ДАННЫХ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет», Ростов-на-Дону, Россия

Ключевые слова: система электронного документооборота, СЭД, сравнительный обзор, обработка данных.

Статья представляет собой обзор современных систем электронного документооборота (СЭД) и проводит сравнительный анализ их эффективности с точки зрения сбора и обработки данных. В статье рассматриваются различные аспекты СЭД, такие как функциональность, интеграция, безопасность, и удобство использования. Авторы анализируют плюсы и минусы каждой системы, выделяя их основные особенности и преимущества.

Данная статья представляет ценную информацию для бизнес-лидеров, ИТ-специалистов и всех заинтересованных в оптимизации процессов сбора и обработки данных с использованием современных систем электронного документооборота.

D.V. Miroshnichenko

## OVERVIEW OF EXISTING ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS AND THEIR COMPARISON IN TERMS OF DATA COLLECTION AND PROCESSING EFFICIENCY

Federal State Budgetary Educational Institution of Higher Education "Don State Technical University", Rostov-on-Don, Russia

Keywords: electronic document management system, EDMS, comparative review, data processing.

The article presents an overview of modern electronic document management systems (EDMS) and conducts a comparative analysis of their effectiveness in terms of data collection and processing. The article discusses various aspects of EDMS, such as functionality, integration, security, and usability. The authors analyze the pros and cons of each system, highlighting their main features and advantages.

This article provides valuable information for business leaders, IT specialists and everyone interested in optimizing the processes of data collection and processing using modern electronic document management systems.

### **Введение.**

В современном мире электронный документооборот (ЭДО) становится все более важным инструментом для ведения бизнеса. Это связано с тем, что ЭДО позволяет существенно сократить время на обработку и хранение документов, а также снижает вероятность ошибок, связанных с человеческим фактором. В этой статье мы рассмотрим несколько популярных систем электронного документооборота и сравним их между собой.

Целью данного исследования является обзор существующих систем электронного документооборота и сравнение их по эффективности сбора и обработки данных. Для достижения этой цели необходимо решить следующие задачи:

- 
- изучить основные принципы и подходы к электронному документообороту.
  - проанализировать различные системы электронного документооборота и выделить их основные функции.
  - сравнить выбранные системы по таким параметрам, как эффективность сбора и обработки данных, стоимость лицензий и удобство использования.
  - разработать рекомендации по выбору оптимальной системы электронного документооборота для конкретного предприятия.

### **Обзор основных понятий и принципов электронного документооборота (ЭДО).**

Электронный документооборот (ЭДО) — это процесс создания, обработки, передачи и хранения документов в электронном виде. Он включает в себя различные технологии и инструменты, которые позволяют автоматизировать работу с документами и повысить эффективность работы предприятия.

Общепринятой аббревиатурой является СЭД. Наравне с ней также используется аббревиатура СЭДО. Также иногда эти системы называют САД (система автоматизации делопроизводства) или САДО (система автоматизации документооборота).

За рубежом такого рода системы называются по-иному: Системы EDMS (Electronic Document Management Systems) – системами управления электронными документами. EDMS - это система управления документами компании. Предназначение данных систем схоже с СЭД. Подобные системы предназначены для ввода-вывода информации на всем протяжении её жизненного цикла, для работы с ней, для её архивирования, поиска введенной в документы информации. Также EDMS решают задачи, связанные с управлением версиями и подверсиями документов, разграничением прав доступа и т.д.

Основными принципами ЭДО являются:

- использование электронных документов вместо бумажных;
- автоматизация процессов обработки документов;
- использование электронной подписи для подтверждения подлинности документов;
- хранение документов в электронном архиве;
- интеграция с другими системами, такими как системы управления предприятием или бухгалтерского учета.

ЭДО позволяет сократить время на обработку документов, уменьшить затраты на их хранение и транспортировку, а также повысить безопасность данных.

Подходы к электронному документообороту могут быть разными в зависимости от специфики предприятия и его потребностей. Некоторые из наиболее распространенных подходов включают:

- Автоматизация процессов создания, редактирования и отправки документов. Этот подход позволяет сократить время, затрачиваемое на выполнение рутинных задач, и повысить эффективность работы сотрудников.
- Использование облачных сервисов для хранения документов. Облачные сервисы предоставляют доступ к документам с любого устройства, подключенного к интернету, что упрощает работу с ними и снижает затраты на хранение.
- Интеграция ЭДО с другими информационными системами, что помогает автоматизировать работу между отделами и подразделениями, повышая эффективность.
- Безопасность работы с данными, используя шифрование и двойную аутентификацию.

В зависимости от требуемых параметров выбирается подход к электронному документообороту, например, от требований к безопасности данных.

---

## **Классификация систем ЭДО.**

Существуют следующие виды классификации ЭДО в зависимости от их признаков:

- по типу правовых отношений: внутренние (внутри компании), внешние (компания с контрагентами), ЭДО с государственными органами (сдача отчетности);
- по характеру документов: архивные, производственные, кадровые и др.;
- по функционалу: систему управления контентом, системы управления информацией, системы управления потоками работ и др.

Каждая ЭДО имеет свои особенности и выполняет определенные задачи. Например, системы управления контентом необходимы для создания, доступа и управления контентом и доставку контента до получателя.

## **Описание и анализ основных функциональных возможностей систем ЭДО.**

### **1С: Документооборот**

Система 1С: Документооборот является современной ЭДО системой, которая необходима для управления документооборотом на предприятии. С ее помощью пользователь может производить работу с документами (создание, редактирование, хранение и отправка получателю). Имеет широкие возможности в интеграции с другими системами 1С.

Главная особенность данной ЭДО – возможность использовать ЭЦП (электронную цифровую подпись), что облегчает процесс документооборота в больших компаниях, а также повысить безопасность данных.

Администратор имеет все права на модификацию документов и их перемещение. Сами файлы можно отправлять, как внутри системы, так и с помощью электронной почты или веб-сервисы.

Так как данный вид ЭДО предназначен для крупных предприятий, то имеется возможность использования мобильного приложения.

### **Битрикс 24**

Еще одним вариантом ЭДО является Битрикс24, который предоставляет свои услуги для бизнеса. Данная система построена таким образом, что документы хранятся в архиве, доступ, к которому можно настроить с помощью разграничения прав пользователей.

В данной системе пользователи могут общаться по видеосвязи или в чатах, также производить модификацию документов, вести календарь событий или собрать почту на одном диске.

Система имеет большой функционал для автоматизации бизнес-процессов, что позволяет пользователям легко разобраться в ней.

### **СЭД от Сбербанка**

Данная СЭД (система электронного документооборота) разработана для документооборота банков, позволяя производить любые манипуляции с данными (редактирование, создание и отправка). Главная особенность данной ЭДО – технология блокчейна, что повышает безопасность данных. Система является высокопроизводительной и имеет возможность расширения, благодаря чему можно обрабатывать большой объем документов.

## **Определение критериев для выбора оптимальной системы ЭДО для конкретного предприятия или организации.**

Существуют следующие критерии выбора ЭДО:

- функционал системы: какие функции необходимы для выполнения задач предприятия;
- удобство использования: насколько просто и быстро сотрудники смогут освоить систему;

- стоимость системы: сколько предприятие готово потратить на нее;
- интеграция с другими системами;
- безопасность данных: проверка степени защиты данных в системе;
- поддержка и обновление ЭДО техническими системами;

С помощью данных критериев предприятие может выбрать наиболее подходящую ЭДО для него. В таблице представлена сравнительная характеристика описанных выше систем.

Таблица 1.

	1С: Документооборот	Битрикс24	СЭД от Сбербанка
Функционал системы	Архив, организация документооборота, контроль и редактирование файлов, цифровая подпись, почтовый клиент	Архив, организация документооборота, контроль и редактирование файлов, голосование, цифровая подпись	Архив, организация документооборота, контроль и редактирование файлов, голосование, согласование, цифровая подпись
Удобство использования	Настройка системы может потребовать некоторых навыков и времени, но после настройки она работает достаточно быстро и эффективно.	Имеет более простой и интуитивно понятный интерфейс, который может быть удобен для начинающих пользователей.	Сложнее, чем интерфейс Битрикс24, но предоставляет больше возможностей для настройки и кастомизации.
Стоимость системы	От 42,5 тыс. рублей	От 6,9 тыс в месяц	Бесплатно (есть ограничения)
Интеграция с другими системами	Имеется	Имеется	Имеется
Безопасность данных	Имеется	Имеется	Имеется
Поддержка и обновление	Имеется	Имеется	Имеется
Недостатки	Сложная настройка системы	Возможности бесплатного тарифа сильно ограничены	Бесплатно только для клиентов Сбера

### **Заключение: выводы по исследованию и рекомендации по выбору системы ЭДО.**

В заключение можно сказать, что все три системы электронного документооборота - 1С:Документооборот, Битрикс24 и СЭД от Сбербанка - имеют свои преимущества и могут быть полезны для разных предприятий. Выбор конкретной системы должен основываться на потребностях предприятия, его бюджете и особенностях работы. Для небольших предприятий может быть достаточно системы Битрикс24, в то время как крупные предприятия могут выбрать систему 1С:Документооборот или СЭД от Сбербанка. В любом случае, перед выбором системы электронного документооборота рекомендуется провести тщательное сравнение и анализ всех возможных вариантов.

### **СПИСОК ЛИТЕРАТУРЫ**

1. Системы электронного документооборота [Электронный ресурс]. – Режим доступа: <https://studfile.net/preview/4431239/page:17/>
2. 11 лучших систем электронного документооборота (СЭД) в 2023 году [Электронный ресурс]. – Режим доступа: <https://www.kp.ru/money/biznes/luchshie-sistemy-ehlektronnogo-dokumentoorobota/>
3. Система электронного документооборота (СЭД) [Электронный ресурс]. – Режим доступа: <https://astral.ru/business/elektronnyy-dokumentoorobot/sistema-ehlektronnogo-dokumentoorobota/>

## ОБЗОР ПЛАТФОРМ ДЛЯ РАЗРАБОТКИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ НА ANDROID

Донской государственной технической университет, Ростов-на-Дону, Россия

Ключевые слова: мобильное приложение, платформа, разработка, Android, кроссплатформенность.

В статье представлен обзор платформ для разработки мобильных приложений на операционной системе (ОС) Android и проведен сравнительный анализ таких характеристик, как язык программирования, кроссплатформенность, интеграция с Android SDK, поддержка эмулятора, поддержка графического интерфейса и документация. Проводится анализ достоинств и недостатков каждой платформы, выделены их основные особенности и преимущества, выявлена актуальность разработки на ОС Android.

А.А. Mikhailova

## REVIEW OF PLATFORMS FOR THE DEVELOPMENT OF MOBILE APPLICATIONS ON THE ANDROID

Don state technical university, Rostov-on-Don, Russia

Keywords: mobile application, platform, development, Android, cross-platform.

The article provides an overview of platforms for developing mobile applications on the Android operating system (OS) and provides a comparative analysis of such characteristics as programming language, cross-platform, integration with Android SDK, emulator support, graphical interface support and documentation. The advantages and disadvantages of each platform are analyzed, their main features and advantages are highlighted, and the relevance of development on the Android OS is revealed.

### Введение.

Мобильные приложения стали неотъемлемой частью нашей повседневной жизни. Они помогают нам во многих сферах – от развлечений и общения с близкими до покупок и управления финансами. С каждым годом сфера разработки мобильных приложений становится все более востребованной, динамичной и инновационной. В этой статье рассмотрим платформы для разработки мобильных приложений на ОС Android.

Целью данного исследования является обзор существующих платформ для разработки мобильных приложений на ОС Android и их сравнение. Для достижения этой цели необходимо решить следующие задачи:

- проанализировать различные платформы для разработки мобильных приложений на ОС Android и выявить их плюсы и минусы.
- сравнить выбранные платформы по характеристикам, таким как языки программирования, кроссплатформенность, интеграция с Android SDK, поддержка эмулятора, поддержка графического интерфейса и документация.
- выявить актуальность разработки мобильных приложений на ОС Android.
- разработать рекомендации по выбору платформы для разработки мобильных приложений на ОС Android.

### Основной раздел.

Android – это полноценная операционная система, в основе которой положено ядро Linux. Поэтому вычислительные сервисы и широкие функциональные возможности

---

Android позволяют создавать приложения, далеко выходящие за рамки сегмента мобильных устройств [1].

Разработка мобильных приложений для операционной системы Android остается актуальной и важной сферой в современном мире, потому что объем продаж устройств на базе Android в 2022 году достиг 1,57 млрд. штук, заметно увеличившись по сравнению с 0,98 млрд. штук в 2021 году. Большие возможности предоставляет разработчикам множество способов монетизации приложений, включая рекламу, платные загрузки, внутриигровые покупки и подписки. По оценкам, потребительские расходы в магазинах приложений в 2022 году составили приблизительно \$167 млрд. Мобильная реклама принесла в 2022 году приблизительно \$336 млрд [2].

Android является более открытой платформой по сравнению с некоторыми другими мобильными ОС и связано это с тем, что размещение своего приложения в Google Play проще, чем в AppStore. В среднем, каждый месяц в Google Play выпускается более 100 000 новых приложений, а в Apple App Store – более 30 000 [3].

### **Описание и анализ основных платформ для разработки мобильных приложений на операционной системе (ОС) Android.**

Android Studio – это интегрированная среда разработки (IDE), которая предоставляет разработчикам мощный набор инструментов и ресурсов для проектирования, разработки, отладки и развертывания мобильных приложений на платформе Android.

Проект Android Studio начал разрабатываться в 2003 году как часть компании Android Inc. Основатели Энди Рубин, Рич Майн и Ник Сирс рассматривали создание операционной системы для мобильных устройств. В 2005 году Google приобрела Android Inc. и внесла крупные инвестиции в разработку Android. Android Studio была анонсирована на конференции Google еще в первой половине 2013 года [4].

Плюсами Android Studio является то, что она бесплатна и это делает ее доступной для всех разработчиков, а также Google регулярно выпускает обновления Android Studio, обеспечивая поддержку последних версий Android.

Минусами Android Studio является то, что платформа требовательна к ресурсам компьютера, особенно при работе с большими проектами, а встроенные симуляторы Android могут работать медленно на некоторых компьютерах, что может замедлить процесс разработки и тестирования программы. Ориентирована исключительно на разработку под ОС Android, что делает ее ограниченной в плане кроссплатформенности.

Eclipse – интегрированная среда разработки (IDE), используемая для разработки приложений, позволяющая разработчикам создавать расширения и плагины для различных языков программирования.

Сначала начали появляться коммерческие реализации на основе Eclipse, среди которых была среда WebSphere Studio Application Developer 4.0. Затем IBM передала разработку платформы Eclipse в открытый исходный код (Open Source), и проект был выпущен в конце 2001 года [5].

Из достоинств можно отметить, что Eclipse доступна бесплатно и распространяется под лицензией Eclipse Public License (EPL). Eclipse обладает обширным количеством плагинов и предоставляет большой набор инструментов для разработки, включая отладку, поддержку версий и многое другое.

Минусами является то, что иногда платформа требует установки и настройки большого количества плагинов, чтобы соответствовать требованиям конкретного проекта, что может вызвать трудности при разработке. Eclipse может потреблять много системных ресурсов, особенно при работе над крупными проектами, что может привести к замедлению работы компьютера.

React Native – это фреймворк для разработки мобильных приложений, который позволяет создавать приложения для iOS и Android, используя синтаксис JavaScript и



---

React. React Native получил анонс на конференции React.js Conf в начале 2015. Его исходный код разработчики открыли в конце весны того же года [6].

Этот фреймворк был создан на основе библиотеки React, которая изначально использовалась для веб-разработки. Основная идея заключалась в том, чтобы разработчики могли использовать знакомые им язык программирования JavaScript и библиотеку React для создания мобильных приложений, а не обучаться новым языкам и технологиям.

Одним из плюсов данной платформы можно выделить то, что приложения, созданные с использованием React Native, обычно имеют простой и приятный вид, потому что они используют компоненты нативных приложений. React Native позволяет разработчикам создавать мобильные приложения для iOS и Android, используя один и тот же код и за счет повторного использования кода и гибкости React Native, разработка приложений может быть значительно ускорена.

Несмотря на использование нативных компонентов, React Native может иметь некоторые ограничения в производительности и при обновлении React Native или его зависимостей могут возникнуть проблемы с совместимостью, что требует дополнительных усилий по поддержке приложения. Документация может быть не так обширна, как у полностью нативных платформ.

Flutter – открытая платформа для разработки мобильных приложений, которая основывается на языке программирования Dart и позволяет создавать удобные и высокопроизводительные приложения с помощью виджетов.

Первая версия Flutter была известна как «Sky» и работала в операционной системе Android. Платформа первый раз была представлена на саммите Dart Developer Summit в 2015 году, а первая стабильная версия Flutter появилась в декабре 2018 года [7].

Одним из основных преимуществ Flutter является возможность разработки приложений, которые работают на Android и iOS, с использованием общего кода. Flutter использует графический движок Skia, который обеспечивает высокую производительность и предоставляет разнообразные виджеты и стили для создания красивых интерактивных пользовательских интерфейсов.

Данная платформа имеет некоторые специфические функции доступные только на этой платформе, которые могут потребовать дополнительной настройки и кода. Приложения, созданные с использованием Flutter, могут иметь больший размер по сравнению с приложениями, созданными на других нативных платформах.

Несмотря на свой быстрый рост в популярности, Flutter все еще считается относительно новым фреймворком, и некоторые компании предпочитают использовать более устоявшиеся технологии.

Xamarin – платформа для разработки кроссплатформенных мобильных приложений, которая позволяет разработчикам использовать C# и .NET.

Компания Xamarin была основана в мае 2011 года штаб-квартирой в Сан-Франциско и офисом разработки в Кембридже, Массачусетс. Xamarin создала Xamarin Platform, которая включает в себя Xamarin Studio, и плагин для Visual Studio, которые могут быть использованы для разработки мобильных приложений с использованием .NET Framework. В 2016 году Microsoft приобрела Xamarin и интегрировала ее технологии в Visual Studio [8].

Из достоинств отметим, что Xamarin позволяет создавать приложения для операционных систем iOS и Android, используя общий код. Разработчики могут использовать знакомый им язык программирования и систему .NET, что уменьшает время на обучение новым технологиям. Также Xamarin позволяет создавать нативные пользовательские интерфейсы и имеет доступ к множеству встроенных функций.

Из недостатков можно выделить необходимость включать runtime-среду Mono в приложение, размер APK/IPA-файлов может быть больше, чем у нативных приложений, созданных на других платформах. Xamarin иногда может иметь проблемы в поддержке

---

новых функций, поскольку требуется время на их адаптацию и для полноценной разработки в Xamarin могут потребоваться лицензии, что может увеличить стоимость разработки. В некоторых случаях производительность приложений, созданных на Xamarin, может быть ниже, чем у нативных приложений.

### **Определение характеристик для выбора платформы для разработки мобильных приложений на ОС Android.**

Для выбора платформы для разработки мобильных приложений на ОС Android необходимо определить следующие характеристики:

- языки программирования: влияет на производительность, разработку и поддержку приложения.
- кроссплатформенность: возможность приложения поддерживаться на разных операционных системах.
- интеграция с Android SDK: дополнительный набор инструментов, которые помогают написать код, запустить тестирование и отладку, проверить работу приложения на различных версиях операционной системы и оценить результат в реальном времени.
- поддержка эмулятора: возможность проверять приложение на различных эмуляторах для разных устройств и версий ОС.
- поддержка графического интерфейса: возможность обеспечить удобство использования, сделать понятный и красочный интерфейс приложения.
- документация: наличие хорошей документацией позволит разработчику лучше понять инструменты платформы.

На основе этих характеристик можно выбрать наиболее подходящую платформу для разработки мобильного приложения. Сравним выбранные платформы.

#### **Android studio**

- языки программирования: Java, Kotlin.
- кроссплатформенность: Android.
- интеграция с Android SDK: полная, прямая интеграция.
- поддержка эмулятора: да, встроенный эмулятор.
- поддержка графического интерфейса: Android XML Layouts.
- документация: обширная.

#### **Eclipse**

- языки программирования: Java.
- кроссплатформенность: Android.
- интеграция с Android SDK: полная, плагин.
- поддержка эмулятора: да.
- поддержка графического интерфейса: Android XML Layouts.
- документация: ограниченная.

#### **React Native**

- языки программирования: JavaScript, TypeScript.
- кроссплатформенность: Android, iOS.
- интеграция с Android SDK: частичная, не прямая интеграция.
- поддержка эмулятора: да, встроенный эмулятор.
- поддержка графического интерфейса: JavaScript XML, компоненты React.
- документация: обширная.

#### **Flutter**

- языки программирования: Dart.
- кроссплатформенность: Android, iOS.

- интеграция с Android SDK: полная, прямая интеграция.
- поддержка эмулятора: да, встроенный эмулятор.
- поддержка графического интерфейса: Собственный набор виджетов Flutter.
- документация: обширная.

#### Xamarin

- языки программирования: C#.
- кроссплатформенность: Android, iOS.
- интеграция с Android SDK: полная, прямая интеграция.
- поддержка эмулятора: да, встроенный эмулятор.
- поддержка графического интерфейса: Xamarin.Forms, нативные компоненты Android.
- документация: обширная.

### **Рекомендации по выбору платформы для разработки мобильных приложений на ОС Android.**

В заключение можно сказать, что все платформы, которые используются для реализации мобильных приложений, имеют свои преимущества и недостатки, основываясь на их характеристиках. Выбор конкретной платформы должен обосновываться навыками разработчика, потребностями интеграции мобильного приложения на другие операционные системы, выбором языка программирования, возможностями использования эмулятора и опытом работы с определенными платформами. Например, если разработчик только начинает знакомиться с мобильной разработкой на Android, то скорее всего ему подойдет Android Studio, потому что у него хорошая и полная документация, много обучающих видеороликов, прямая интеграция с Android SDK, а также есть возможность использования эмулятора для проверки работы своего приложения. А если разработчик уже имеет опыт и может потратить время на изучение новой платформы, или же если перед ним встал вопрос о кроссплатформенности приложения, то конечно же ему стоит уделить внимание таким платформам как React Native или Flutter. Важно отметить, что перед принятием окончательного решения по выбору платформы следует провести тщательное сравнение и анализ всех доступных вариантов.

### СПИСОК ЛИТЕРАТУРЫ

1. Бердышев С.С. Обзор и анализ сред разработки приложений для ос Android / С.С. Бердышев. – Текст: электронный // Актуальные вопросы экономики и агробизнеса: сборник статей VIII Международной научно-практической конференции. – 2017. – №3. – С. 277-280. – URL: <https://www.elibrary.ru/item.asp?id=29798360> (дата обращения: 10.10.2023).
2. App Mobile Applications in the Global Market [Электронный ресурс] // tadviser: [сайт]. – URL: [https://tadviser.com/index.php/Article:Mobile\\_Applications\\_\(Global\\_Market\)#Global\\_mobile\\_gaming\\_market\\_sank\\_5.25\\_due\\_to\\_inflation](https://tadviser.com/index.php/Article:Mobile_Applications_(Global_Market)#Global_mobile_gaming_market_sank_5.25_due_to_inflation) (дата обращения: 11.10.2023).
3. Статистика мобильных приложений 2021: загрузки, тренды и доходность индустрии [Электронный ресурс] // VC: [сайт]. – URL: <https://vc.ru/marketing/245003-statistika-mobilnyh-prilozheniy-2021-zagruzki-trendy-i-dohodnost-industrii> (дата обращения: 11.10.2023).
4. Как пользоваться Android Studio? [Электронный ресурс] // sravni: [сайт]. – URL: <https://www.sravni.ru/kursy/info/kak-polzovatsya-android-studio/> (дата обращения: 02.10.2023)

- 
5. Платформа разработки Eclipse [Электронный ресурс] // osp: [сайт]. – URL: <https://www.osp.ru/os/2005/03/185394> (дата обращения: 05.10.2023).
  6. React: описание и основы работы [Электронный ресурс] // OTUSJOURNAL: [сайт]. – URL: <https://otus.ru/journal/react-opisanie-i-osnovy-raboty> (дата обращения: 05.10.2023).
  7. Flutter (программное обеспечение) [Электронный ресурс] // cyclowiki: [сайт]. – URL: [https://cyclowiki.org/wiki/Flutter\\_%28программное\\_обеспечение%29](https://cyclowiki.org/wiki/Flutter_%28программное_обеспечение%29) (дата обращения: 07.08.2023).
  8. Xamarin [Электронный ресурс] // stackoverflow: [сайт]. – URL: <https://ru.stackoverflow.com/tags/xamarin/info> (дата обращения: 09.10.2023).

**Э.А. Ядрец<sup>1</sup>, М.В. Карпенко<sup>1</sup>, Н.В. Болдырихин<sup>2</sup>**

### **ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК КЛЮЧЕВОЙ ЭЛЕМЕНТ В ОЦЕНКЕ РИСКОВ СОВРЕМЕННЫХ АНТИФРОД РЕШЕНИЙ**

Донской государственной технической университет, г. Ростов-на-Дону, Россия<sup>1</sup>  
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: информационные технологии, искусственный интеллект, бизнес-процессы, информационное общество.

В статье рассмотрены системы антифрод, которые позволяют предотвратить рост мошеннических операций, который возник в последние годы, также представлены возможные варианты данных систем.

**E.A. Yadrets<sup>1</sup>, M.V. Karpenko<sup>1</sup>, N.V. Boldyrikhin<sup>2</sup>**

### **ARTIFICIAL INTELLIGENCE AS A KEY ELEMENT IN RISK ASSESSMENT OF MODERN ANTIFRAUD SOLUTIONS**

Don State Technical University (DSTU), Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: information technologies, artificial intelligence, business processes, information society.

The article considers antifraud systems, which allow to prevent the growth of fraudulent operations, which has arisen in recent years, and also presents possible variants of these systems.

Системы Антифрод (Antifraud) – представляют собой интегрированные инфраструктурные решения, централизованно направленные на мониторинг, анализ и превентивное вмешательство в отношении потенциальных угроз, возникающих в ходе выполнения бизнес-процессов.

Основной задачей данных систем является предотвращение мошеннических операций, осуществляющихся в режиме реального времени. Для достижения высокой степени эффективности в детекции и реагировании на аномалии, системы антифрод активно интегрируют современные технологии искусственного интеллекта.

Эти технологии позволяют динамически идентифицировать отклонения от стандартизированных или утвержденных бизнес-процессов, обеспечивая тем самым своевременное обнаружение и реагирование на индикаторы финансовых нарушений или потенциальных уязвимостей. Искусственный интеллект в контексте антифрод систем приобретает особую актуальность, учитывая его способность к быстрой адаптации к меняющимся условиям, модификации логики бизнес-процессов, а также возможность к применению передовых, оптимизированных практик отрасли в целях улучшения качества защиты[1].

Системы антифрод собирают данные о транзакциях, активности пользователей и других факторах. Эти данные анализируются для выявления необычных или подозрительных паттернов.

Принципы работы искусственного интеллекта в антифрод системах включает в себя алгоритмы машинного обучения, применяемые для обучения моделей на основе собранных данных. Такие модели могут выявлять аномалии и предсказывать возможные мошеннические активности. В свою очередь, часто используют алгоритмы классификации, такие как, логистическая регрессия, решающие деревья, служащие для определения, является ли транзакция легитимной. Кластеризация применяется для выявления групп похожих транзакций. Если одна из транзакций в группе считается мошеннической, остальные также могут быть рассмотрены как потенциально мошеннические. Алгоритмы One-Class SVM или Isolation Forest, помогают определить аномальное поведение, отличающееся от «нормальных» паттернов[2].

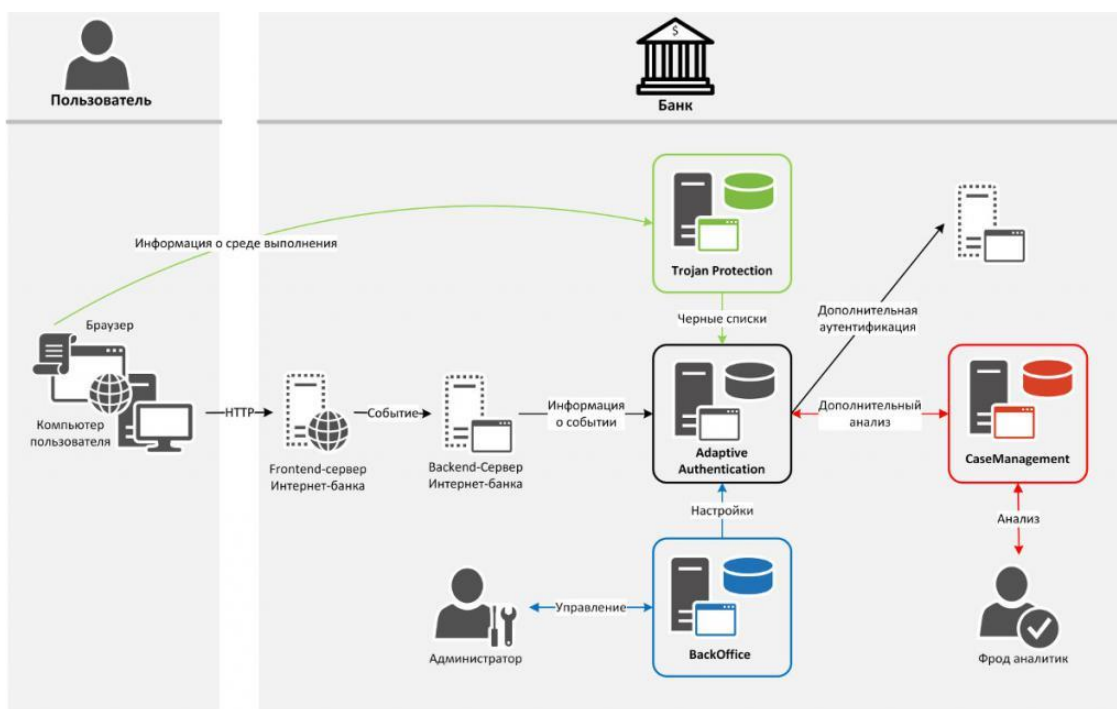


Рисунок 1. Принцип работы антифрод системы

Примерами существующих антифрод систем могут служить:

- Kaspersky Fraud Prevention – в его основе лежит машинное обучение, применяются методы кластеризации, деревья решений и искусственные нейронные сети, позволяя реагировать на случаи мошенничества в режиме реального времени и улучшая уровень безопасности[3].
- BI.ZONE AntiFraud (BAF) обеспечивает аналитику сессий и транзакций с учетом данных об угрозах из различных источников. Продукт подходит как для банков, так и для онлайн-сервисов, и позволяет создавать поведенческие модели клиентов для выявления мошенничества. Применяя машинное

---

обучение и статистику, распознает новые мошеннические схемы и предоставляет доступ к самым актуальным данным по угрозам[4].

- Group-IB Fraud Hunting Platform, работая в режиме реального времени, проводит анализ поведения пользователя на веб-сайтах и в мобильных приложениях. С помощью алгоритмов машинного обучения и поведенческого анализа, система формирует уникальные цифровые отпечатки устройств, ассоциируя их с конкретными пользователями и их аккаунтами. Это позволяет с высокой точностью определять действия пользователя и отличать их от попыток мошенничества, даже если мошенник получил доступ к его устройству или платежной информации[5].
- Cybertonica предлагает решение противодействия фроду, разработанное для банков, эквайеров, платежных агрегаторов и интернет-магазинов. Данная платформа, используя технологии машинного обучения, в режиме реального времени оценивает риски, формируя адаптивные правила безопасности и создавая цифровой профиль пользователя. Она анализирует паттерны поведения клиента в браузере или приложении и технические характеристики используемых им устройств[6].

Таким образом, искусственный интеллект выступает ключевым элементом в сфере антифрод решений, основным преимуществом которого, является его способность быстро обрабатывать огромные массивы данных в режиме реального времени, а его высокая степень оперативности позволяет системам немедленно выявлять и реагировать на мошеннические действия, обеспечивая высокий уровень безопасности.

#### СПИСОК ЛИТЕРАТУРЫ

1. Шабанов А. Применение технологий искусственного интеллекта в информационной безопасности / Шабанов А. [Электронный ресурс] // ANTI-MALWARE : [сайт]. — URL: [https://www.anti-malware.ru/analytics/Technology\\_Analysis/using-artificial-intelligence-technologies-in-information-security](https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security) (дата обращения: 30.09.2023).
2. Выявление мошенничества с помощью алгоритмов случайного леса, нейронного автокодировщика и изолирующего леса / [Электронный ресурс] // Хабр : [сайт]. — URL: <https://habr.com/ru/companies/nix/articles/478286/> (дата обращения: 30.09.2023).
3. Kaspersky Fraud Prevention / [Электронный ресурс] // Kaspersky Fraud Prevention : [сайт]. — URL: <https://kfp.kaspersky.com/wp-content/uploads/2020/09/RU-WEB-Fraud-Prevention-Brief.pdf> (дата обращения: 30.09.2023).
4. Антифрод-решение BI.ZONE AntiFraud — система противодействия мошенничеству / [Электронный ресурс] // BI.ZONE : [сайт]. — URL: <https://bi.zone/catalog/products/antifraud/> (дата обращения: 30.09.2023).
5. Group-IB Fraud Hunting Platform защитит «цифровую личность» пользователя / [Электронный ресурс] // Group-IB : [сайт]. — URL: <https://blog.group-ib.ru/fhp> (дата обращения: 30.09.2023).
6. Машинное обучение, аналитика поведения, цифровые отпечатки устройств и рабочее место команды безопасности в одной платформе / [Электронный ресурс] // Cybertonica - антифрод для роста бизнеса : [сайт]. — URL: <https://cybertonica.ru> (дата обращения: 30.09.2023).

## САЙТ ДЛЯ ПОИСКА И ХРАНЕНИЯ ШАБЛОНОВ ЮРИДИЧЕСКИХ ДОКУМЕНТОВ

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: веб-разработка, шаблоны, юридические документы.

В статье рассматривается метод реализации веб-приложения для сбора, систематизации и хранения шаблонов юридических документов. Создание централизованного ресурса упрощает и ускоряет поиск качественных шаблонов, способствует разработке юридических документов высокого качества в соответствии с актуальными требованиями.

L.G. Megribanyan, A.N. Chikalov

## WEBSITE FOR SEARCHING AND STORING TEMPLATES LEGAL DOCUMENTS

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: web development, templates, legal documents.

The article discusses the method of implementing a web application for collecting, systematizing and storing templates of legal documents. The creation of a centralized resource simplifies and accelerates the search for high-quality templates, contributes to the development of high-quality legal documents in accordance with current requirements.

В современном мире юридические документы играют важную роль во многих сферах деятельности, будь то бизнес, государственная служба или повседневная жизнь обычных граждан. Часто возникает необходимость в создании определенных юридических документов, и для этого нужны шаблоны, которые могут быть использованы в качестве основы для создания новых документов.

Люди все чаще прибегают к тому, чтобы быстро найти и воспользоваться каким-либо юридическим шаблоном. Однако поиск подходящего шаблона может быть затруднительным и требовать значительных временных ресурсов. Возникает необходимость в создании централизованного ресурса, где юристы и другие заинтересованные лица смогут найти широкий выбор качественных юридических шаблонов на различные случаи.

Разработка сайта-хранилища шаблонов для юридических документов имеет большую практическую значимость и потенциал для повышения эффективности работы юристов, поскольку поможет сократить время, затрачиваемое на составление документов, и обеспечить их качество и соответствие требованиям.

Основными преимуществами разработки такого сайта являются удобство использования, экономия времени и ресурсов, повышение качества юридической работы и снижение возможных рисков. Пользователи смогут быть уверены в актуальности и правильности предоставляемых шаблонов, так как сайт-хранилище будет поддерживаться и обновляться регулярно.

При создании сайта использована СУБД MySQL в силу ряда особенностей:

- MySQL имеет долгую историю развития и широкое распространение в среде веб-разработчиков [1];

- 
- имеет обширную документацию, что может быть полезно при возникновении вопросов или проблем;
  - предоставляет простой и интуитивно понятный язык запросов, который легко поддается изучению и использованию;
  - может обрабатывать большие объемы данных и обеспечивать быстрый доступ к ним. Это особенно важно для сайтов-хранилищ, где происходит хранение и поиск большого количества шаблонов и данных;
  - совместимость с популярными языками программирования, такими как PHP, который будет использован для создания сайта.

По своей организации был создан универсальный сайт для хранения шаблонов, чтобы новичкам в юридической сфере было легко искать нужные шаблоны в различных отраслях, будь то исковое заявление, ходатайство, соглашение или другие документы. Чтобы обеспечить удобство пользователей, сайт должен быть бесплатным и предоставлять доступ ко всем шаблонам. По своим функциональным возможностям он должен быть прост, логически понятен, иметь возможности для расширения и редактирования, позволять вести поиск по ключевым словам.

Организация сайта предполагает последовательное уточнение требований к искомому документу для быстрого и направленного поиска. Поэтому изначально в меню выбирается тип документа с последующим погружением на страницы с соответствующей дополнительной информацией. Такой механизм реализован на основе обобщенного алгоритма, представленного на рис.1.

Используемая база данных была построена на основе практического опыта с юридической документацией, практики поиска и разработки юридических документов. Были изучены достоинства и недостатки различных сайтов областных судов, организаций, специализирующихся в работе с документами узкой направленности и узких видов деятельности, универсальных сайтов типа "Консультант плюс". В разных сочетаниях они имеют много достоинств с точки зрения диапазона поиска, дизайна, объема хранящейся информации, юридической актуальности документов.

Однако в качестве основных недостатков следует отметить следующие:

- платность некоторых предоставляемых услуг;
- не всегда удобный и затратный по времени поиск;
- избыточность и повторяемость документов;
- вместо шаблона предлагаются рекомендации по их составлению;
- отсутствие функции поиска по шаблонам.

Все эти недостатки затрудняют работу юристов, тем более начинающих, приводят нерациональному расходованию времени, длительному согласованию текстов с руководством, досадным возвратам и отказам в законных по своей сути процессуальных требованиях.

Поэтому база данных шаблонов ориентирована на направленный и быстрый поиск документа. В соответствие с основными классифицирующими признаками она включает только основные объекты, хранящие и накапливающие данные:

- о типе документа (заявление, ходатайство, справка, жалоба и др.);
- о юридическом направлении, определяющим области юридической практики или сферу применения. Например, гражданское право, уголовное право, трудовое, налоговое, семейное законодательство и т.д.;
- об организации или компании, которая использовала представленные шаблоны. Такой информационный объект важен с точки зрения идентификации данных, углубленного изучения особенностей его применения, дальнейшего уточнения различных характеристик и хронологии его использования при необходимости.



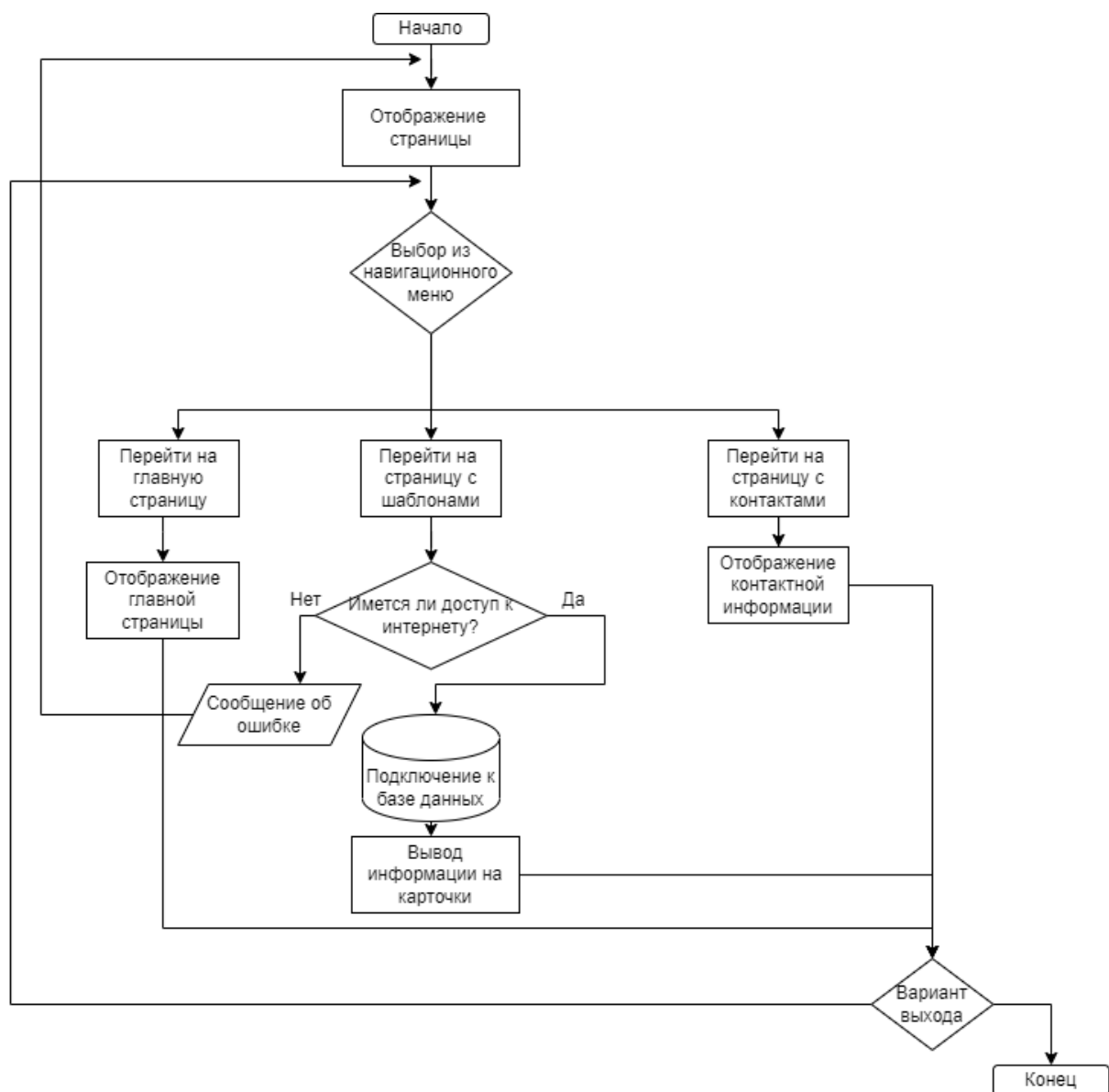


Рисунок 1. Обобщенный алгоритм работы сайта

Программная реализация сайта основана на комбинации CSS и HTML форматов. Они определяют визуальное расположение блоков и элементов сайта, ссылки на внешние файлы, стили и библиотеки шрифтов.

Переключение на различные страницы сайта осуществляется с помощью меню. Количество вариантов ограничено для исключения непродуктивных переключений.

Секция "newsitem" представляет собой новостной портал. Здесь пользователи могут ознакомиться с последними новостями и актуальной информацией в области права.

На основной странице существует блок "Footer", который содержит логотип и кнопку "Наверх". Нажатие на эту кнопку позволяет мгновенно переместиться к началу страницы. Реализация данной функции осуществляется с помощью якоря. Якорь представляет собой закладку с уникальным именем на определенном месте веб-страницы, которая создает возможность перехода к ней по ссылке:

<footer>

```

<div class="footer__flex">
  <div class="footer__items">
    <a name="logo"></a>
  </div>
  <ul class="footer__items" >
    <a href="#logo">Наверх</a>
  </ul>
</div>
</footer>

```

Для ускорения ненаправленного поиска реализован поиск по ключевым словам. Файл "search.php" является скриптом, отвечающим за поиск шаблонов на основе совпадения слов и отображение соответствующих карточек с заявлениями.

При обращении к данному файлу, пользователь может ввести ключевые слова или фразы в поле поиска. В результате, "search.php" возвращает карточки с заявлениями, которые содержат совпадения с введенными ключевыми словами.

Этот скрипт позволяет пользователям быстро находить нужные заявления на основе поискового запроса, упрощая процесс навигации и предоставляя удобную возможность доступа к необходимым шаблонам. Кодовая реализация представлена ниже:

```

<?php
require_once 'connect.php';
mysqli_set_charset ($conn, "utf8");
$searchTerm = $_GET['search'];
$sql = "SELECT * FROM `shabloni` WHERE `Opisanie` LIKE
'%" . $searchTerm . "%'";
$result = $conn->query($sql);
?>

```

В программе предусмотрена адаптация под мобильные устройства, которая была осуществлена в файле style.css. Для этого были применены медиа-запросы (media queries). Медиа-запросы представляют собой конструкции, которые позволяют определить, какие стили должны применяться на веб-странице на основе определенных условий. Это позволяет адаптировать внешний вид и макет страницы к различным размерам и типам устройств, включая мобильные устройства [2].

Благодаря медиа-запросам, можно определить, какие стили следует применять для мобильных устройств, чтобы обеспечить оптимальное отображение и удобство использования. Это включает изменение размеров, размещения элементов, использование различных шрифтов и т.д. Адаптация под мобильные устройства позволяет улучшить пользовательский опыт и обеспечить более удобное взаимодействие с веб-страницей на различных устройствах.

Главная страница сайта отображается корректно для десктопной и мобильной версии устройств.

Чтобы получить доступ к шаблонам, необходимо выбрать соответствующий пункт "Шаблоны" в меню хэдера. Это приведет к переходу на страницу, где отображаются шаблоны заявлений для скачивания. Внешний вид данной страницы "Шаблоны" представлен на рис.2. На странице карточек доступных шаблонов отображаются названия и ссылки для их скачивания. При переходе по ссылкам пользователь будет перенаправлен на Google Диск, где размещены соответствующие заявления. Скачивание возможно в форматах PDF и DOC, и в зависимости от выбора, пользователь будет перенаправлен на ссылку для ознакомления и загрузки. Кроме того, на этой странице имеется функция поиска для удобства поиска. Поиск осуществляется по ключевым словам.

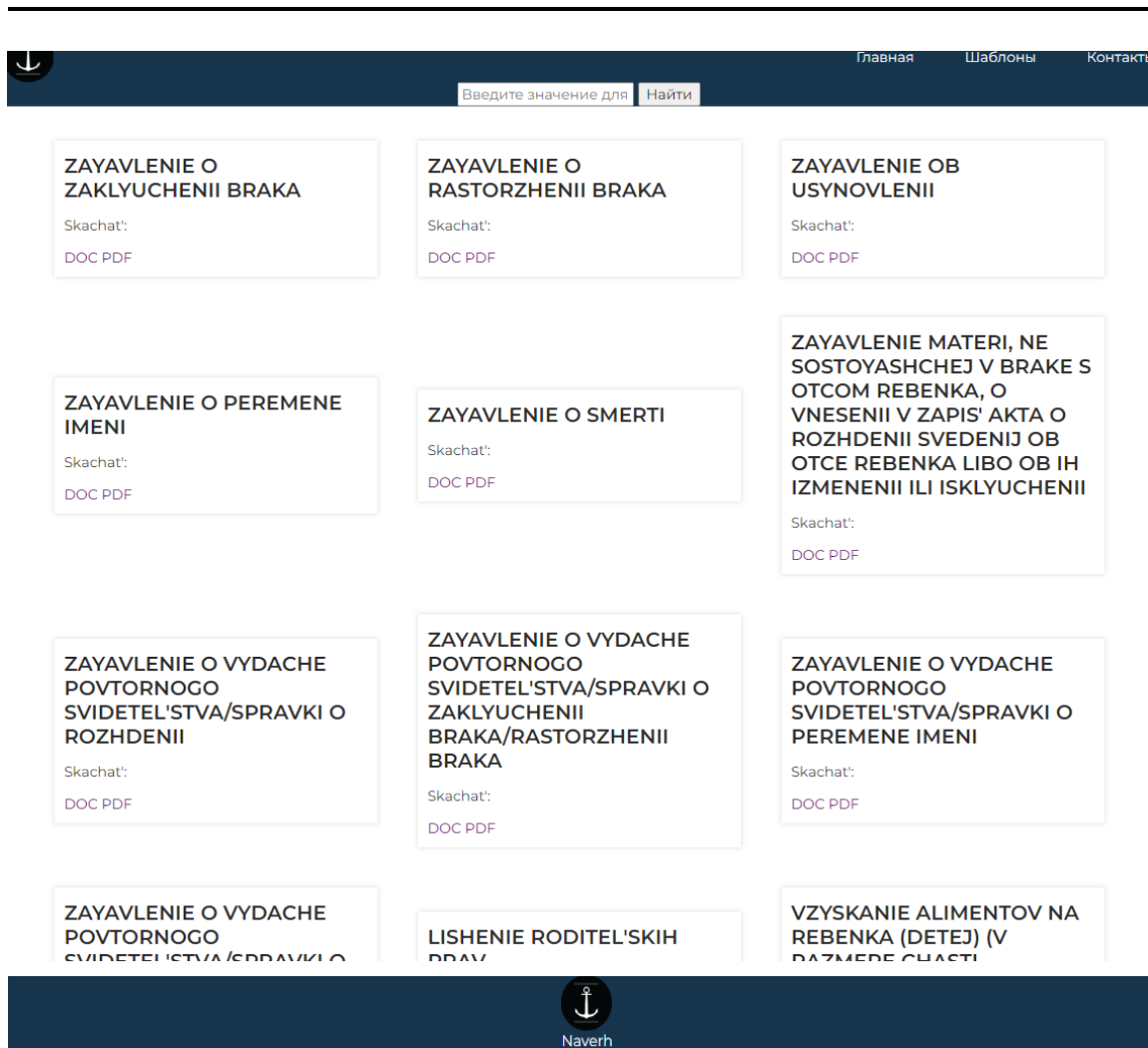


Рисунок 2. Страница "Шаблоны"

Мобильная версия данной страницы внешне выглядит практически так же, как и версия для настольных компьютеров, за исключением того, что вместо трех заявлений в ряд, на мобильном устройстве отображается только одно заявление на экране.

Разработка сайта-хранилища шаблонов для юридических документов имеет большую практическую значимость и потенциал для повышения эффективности работы юристов, поскольку помогает сократить время, затрачиваемое на составление документов, и обеспечивает их качество и соответствие актуальным юридическим требованиям. Работа сайта проверена в практической работе. Сайт показал свою полезность, и дальнейшая работа осуществляется в направлении наращивания информационной базы, расширения функционала, улучшения пользовательского интерфейса и поддержки дополнительных национальных языков и юрисдикций.

#### СПИСОК ЛИТЕРАТУРЫ

1. Дакетт Дж. HTML и CSS: разработка и дизайн веб-сайтов. — М.: Эксмо, 2020. - 480 с.
2. Фримен Э., Робсон Э. Изучаем программирование на JavaScript. — СПб: Издательство Питер, 2022. - 640 с.

## ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ АНАЛИЗА И ВИЗУАЛИЗАЦИИ ФИНАНСОВЫХ ДАННЫХ БИЗНЕСА

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: веб-разработка, анализ данных, визуализация данных.

В статье рассматривается метод реализации веб-приложения для анализа и визуализации финансовых данных бизнеса. Приложение позволяет формировать финансовый отчет и различные диаграммы на основе загруженных финансовых данных.

D.D. Kovaleva, A.N. Chikalov

## WEB-APPLICATION FOR ANALYSIS AND VISUALIZATION OF BUSINESS FINANCIAL DATA

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: web development, data analysis, data visualization.

This article discusses a method for implementing a web application for analyzing and visualizing business financial data. The application allows you to generate a financial report and various charts based on the downloaded financial data.

Современные предприятия в нашей динамичной экономической среде сталкиваются с огромными объемами финансовых данных, которые требуют анализа и обработки для принятия информированных решений. Вместе с этим, увеличиваются требования к точности, своевременности и доступности финансовой информации. В таком контексте возникает неотложная потребность в эффективных инструментах для анализа и визуализации этих данных, которые помогут предприятиям улучшить свою финансовую стратегию и принимать обоснованные решения.

Предлагаемое веб-приложение основано на языке программирования Python, который обладает мощными инструментами для работы с данными и разработки веб-приложений. У него интуитивно понятный и простой в использовании интерфейс, который позволит пользователям легко загружать данные, формировать отчет с финансовыми показателями, а также визуализировать результаты.

В статье предлагается разработка простого, но эффективного приложения для анализа и визуализации финансовых данных бизнеса.

Для реализации приложения использован фреймворк Dash. Это фреймворк для создания интерактивных веб-приложений на языке Python. Он базируется на библиотеке Flask и использует HTML, CSS и JavaScript для создания визуальных элементов интерфейса [1]. Dash предлагает мощные инструменты для создания графиков, таблиц и других элементов визуализации, а также предоставляет простой способ взаимодействия с базой данных и интеграции с другими библиотеками Python [2].

Приложение осуществляет загрузку данных о финансовых транзакциях в базу данных, а затем обработку и перемещение в хранилище данных, откуда их удобнее использовать в последующих расчетах.

Для работы с приложением используется база данных SQLite. Создается операционная база operation.db, которая заполняется после загрузки файлов пользователем. Далее из нее формируется хранилище данных data\_warehouse.db,

---

состоящее из таблиц нормализованных данных. Как правило это осуществляется из файлов электронных таблиц. Данные содержат типовой набор сведений, использующихся в коммерческих продающих структурах: данные о продуктах, их категориях, поставщиках, заказах, сотрудниках, клиентах и т.д. Этих сведений вполне достаточно для эффективного хранения и управления бизнес-данными. В последующем актуальные таблицы, отражающие финансовые транзакции, являются основой для формирования итогового набора данных `master_df`, который используется для формирования дашборда и визуализации.

Приведенные ниже операторы иллюстрируют этапы процедуры преобразования массивов исходных данных.

```
def main(folder_of_files):
    conn = sqlite3.connect('operation.db')
    files = glob.glob(os.path.join(folder_of_files,»**.xls«))
    if files == []:
        raise Exception('\nNo datasets found in DATASETS folder!')
    for file in files:
        xls_file = file
        xl = pd.ExcelFile(xls_file)
        for sheet in xl.sheet_names:
            table_name = sheet.replace(' ', '_').upper()
            df_tmp = xl.parse(sheet)
            df_tmp.to_sql(table_name, conn, if_exists='append', index = False)
            conn.commit()
            conn.close()
    if __name__ == '__main__':
        try:
            main('C:\Users\koval\Desktop\PocketProfit\datasets\sources')
        except Error as e:
            print(str(e) + ': Primary keys exists!')
            pass
    file_path = r'../datasets/sources'
    defcreate_operation_database(file_path):
        operation_database.main()
        try:
            extract_load.main(file_path)
        except Error as e:
            print(str(e) + ': Primary key exists!')
            pass
    defget_master_data_file():
        return elt.get_datawarehouse_dataframe()
    defcheck_operation_exists():
        folder_of_files = 'C:/Users/koval/Desktop/PocketProfit/datasets'
        files = glob.glob(os.path.join(folder_of_files, 'operation.db'))
        return bool(files)
    defcheck_dataawh_exists():
        folder_of_files = 'C:/Users/koval/Desktop/PocketProfit/datasets'
        files = glob.glob(os.path.join(folder_of_files, 'data_warehouse.db'))
        return bool(files)
    def main():
        checker_operation = check_operation_exists()
        checker_warehouse = check_dataawh_exists()
        if not checker_operation:
            print('\nCreating operation database!')
            create_operation_database(file_path)
            master_df = get_master_data_file()
            print('\nGeneratingdataframe for data warehouse!')
        else:
            print('\nOperation database exists, skipping to dataframe generation!')
            master_df = get_master_data_file()
```

---

```

        print('\nDataframe for data warehouse generated successfully')
    if not checker_warehouse:
        initialize_datawh.main()
        try:
            conn = sqlite3.connect('data_warehouse.db')
            master_df.to_sql('MASTER_FILE', conn, if_exists='append', index=False)
            print('\nData warehouse has been populated!')
            conn.commit()
        except Error as e:
            print(e)
    else:
        try:
            # insert master_df into data_warehouse
            conn = sqlite3.connect('data_warehouse.db')
            master_df.to_sql('MASTER_FILE', conn, if_exists='append', index=False)
            print('\nData warehouse has been updated!')
            conn.commit()
        except Error as e:
            print(e)

```

После расчета основных финансовых показателей на их основе формируются различные визуализации и отчет об экономических результатах. Перечень основных визуализаций отобран на основе практического опыта и потребностей активных предпринимателей. Среди них Продажи по категориям, Прибыль, Расходы по категориям, Последние операции, Поток наличности, Рейтинг продаж, Карта продаж, Изменение прибыли по годам, Диаграмма денежного потока.

Основные механизмы визуализации продемонстрированы совокупностью операторов и процедур.

```

app = dash.Dash(__name__, external_stylesheets=[dbc.themes.BOOTSTRAP],
suppress_callback_exceptions=True)
server = app.server
app.title = 'PocketProfit'
app.layout= html.Div(
    children=[
        dcc.Upload(
            id='upload-data',
            children=html.Div(['Перетащите или Выберите файлы']),
            style={
                'margin-top': '70px',
                'width': '350px',
                'height': '60px',
                'lineHeight': '60px',
                'borderWidth': '1px',
                'borderStyle': 'dashed',
                'borderColor': 'white',
                'borderRadius': '5px',
                'textAlign': 'center',
                'margin': '10px auto'
            },
            multiple=False
        ),
        html.Div(id='output-data-upload')
    ],
    style={'textAlign': 'center'}
),
    html.Div(
        children=[
            dcc.Tabs(
                id='tabs',

```

```

        value='tab-1',
        children=[
dcc.Tab(label='Продажи по категориям', value='tab-4'),
dcc.Tab(label='Прибыль', value='tab-5'),
        dcc.Tab(label='Экономические показатели', value='tab-
6'),
dcc.Tab(label='Расходы по категориям', value='tab-8'),
dcc.Tab(label='Последние операции', value='tab-3'),
dcc.Tab(label='Поток наличности', value='tab-9'),
dcc.Tab(label='Рейтинг продаж', value='tab-1'),
dcc.Tab(label='Карта продаж', value='tab-2'),
dcc.Tab(label='Выгрузить отчет', value='tab-10'),
],
        style={'color': '#6291C0'}
    )
],
className='row',
    style={'margin-top': '20px'}
),
html.Div(id='tab-content'),
],
className='container-fluid',
    style={'background-color': '#7CB0E4'}
)
fig.update_layout(
    title='Изменение прибыли (2023)',
    xaxis_title='Дата',
    yaxis_title='Прибыль',
    template='seaborn'
)

fig = go.Figure(data=[
go.Scatter(x=time_periods, y=cash_flow, mode='lines+markers', name='Кэш-
флоу'),
go.Bar(x=time_periods, y=cash_flow, name='Столбцы', opacity=0.5)
])
fig.update_layout(
    title='Диаграмма денежного потока',
    xaxis_title='Дни месяца',
    yaxis_title='Поток наличности',
    template='plotly_white'
)

@app.callback(
Output('tab-content', 'children'),
    [Input('tabs', 'value')]
)
dcc.Graph(id='bar_graph')
],
    style={'border-radius': '15px', 'backgroundColor': '#f8f9fa',
        'box-shadow': '4px 4px 2.5px #dddddd', 'padding': '20px',
        'margin-left': 'auto', 'margin-right': 'auto', 'margin-
top': '25px'}
)
elif tab == 'tab-2':
    return html.Div(
        children=[
dcc.Graph(id='graph-4', figure=map_data)
],
        style={'border-radius': '15px', 'backgroundColor': '#f8f9fa',
            'box-shadow': '4px 4px 2.5px #dddddd', 'padding': '20px',
            'margin-left': 'auto', 'margin-right': 'auto', 'margin-
top': '25px'}
)

```

```

    )
elif tab == 'tab-4':
    return html.Div(
        children=[
dcc.Graph(
            id='graph-1', figure=viz_scatter_iii2
        )
        ],
className='six columns',
        style={'border-radius': '15px', 'backgroundColor': '#f8f9fa',
            'box-shadow': '4px 4px 2.5px #dddddd', 'padding': '20px',
            'margin-left': 'auto', 'margin-right': 'auto', 'margin-
top': '25px'}
        )
elif tab == 'tab-9':
    return html.Div(
        children=[
dcc.Graph(id='graph-1', figure=fig)
        ],
className='six columns',
        style={
            'border-radius': '15px',
            'backgroundColor': '#f8f9fa',
            'box-shadow': '4px 4px 2.5px #dddddd',
            'padding': '20px',
            'margin-left': 'auto',
            'margin-right': 'auto',
            'width': '1400px',
            'height': '700px',
            'margin-top': '25px'
        }
    )
elif tab == 'tab-3':
    return html.Div(
        children=[
dash_table.DataTable(
            id='datatable-interactivity',
            data=data_table.to_dict('records'),
            columns=[{'name': i, 'id': i, 'deletable': True,
'selectable': True} for i in data_table.columns],
            editable=True,
            sort_action='native',
            sort_mode='multi',
            sort_by=[{'column_id': 'Date', 'direction': 'desc'}],
            column_selectable='single',
            row_selectable='multi',
            row_deletable=True,
            selected_columns=[],
            selected_rows=[],
            page_action='native',
            page_current=0,
            page_size=55,
            style_cell={
                'textOverflow': 'ellipsis',
                'overflow': 'hidden'
            },
            style_table={
                'width': '1400px',
                'height': '700px',
                'overflowY': 'auto',
                'overflowX': 'auto',
                'align': 'center'
            },
        ],
    )

```



```

style_header={
            'backgroundColor': 'rgb(230, 230, 230)',
            'fontWeight': 'bold'
        }
    )
],
style={'border-radius': '15px', 'backgroundColor': '#f8f9fa',
      'box-shadow': '4px 4px 2.5px #dddddd', 'padding': '20px',
      'margin-left': 'auto', 'margin-right': 'auto', 'margin-
top': '25px'}
)
elif tab == 'tab-8':
    return html.Div(
        children=[
            dcc.Graph(id='graph-1', figure=fig2)
        ],
        className='six columns',
        style={
            'border-radius': '15px',
            'backgroundColor': '#f8f9fa',
            'box-shadow': '4px 4px 2.5px #dddddd',
            'padding': '20px',
            'margin-left': 'auto',
            'margin-right': 'auto',
            'margin-top': '25px'
        }
    )
elif tab == 'tab-5':
    return html.Div(
        children=[
            dcc.Dropdown(
                id='months-dropdown',
                options=[{'label': month, 'value': month}],
            ),
            dcc.Graph(id='graph-2', figure=fig2)
        ],
        style={'border-radius': '15px', 'backgroundColor': '#f8f9fa',
              'box-shadow': '4px 4px 2.5px #dddddd', 'padding': '20px',
              'margin-left': 'auto', 'margin-right': 'auto', 'margin-
top': '25px'}
    )
elif tab == 'tab-10':
    return html.Div(
        children=[
            html.Div(
                children=[
                    html.H3('Отчет о финансовых результатах:'),
                    dcc.RadioItems(
                        value='financial',
                        labelStyle={'display': 'inline-block', 'margin-right': '10px'},
                        style={'textAlign': 'center'},
                    ),
                ],
                style={'textAlign': 'center', 'margin-top': '50px'},
            ),
            html.Div(
                children=[
                    html.Button(
                        'Скачать отчет',
                        id='download-report-button',
                        className='btn btn-primary',
                        style={'fontSize': '20px', 'margin-top': '20px'},
                    ),
                ],
            )
        ],
    )

```

```

        ],
        style={'textAlign': 'center', 'margin-bottom': '50px'},
    ),
],
className='container-fluid',
style={'backgroundColor': '#ffffff', 'padding': '20px', 'width':
'100%'}
)
elif tab == 'tab-6':
    return dbc.Row([
dbc.Col(html.Div(
dbc.Alert('Продажи ' + get_sales_quantity(master_df), color='light')),
width=2),
dbc.Col(html.Div(
dbc.Alert('Доход ' + get_revenue(master_df), color='light')), width=2),
dbc.Col(html.Div(
dbc.Alert('Расходы ' + get_expenses(master_df), color='light')), width=2),
dbc.Col(html.Div(
dbc.Alert('Скидка ' + get_discount(master_df), color='light')), width=2),
dbc.Col(html.Div(
dbc.Alert('Прибыль ' + get_profit(master_df), color='light')), width=2),
dbc.Col(html.Div(
dbc.Alert('Маржа ' + get_sales_margin(master_df), color='light')), width=2),
],
style={'border-radius': '15px', 'backgroundColor': '#f8f9fa',
'box-shadow': '4px 4px 2.5px #dddddd', 'padding': '20px',
'margin-left': 'auto', 'margin-right': 'auto', 'margin-top':
'50px'}
)
)

```

На главной странице приложения расположены кнопки «Регистрация», «Вход», «Скачать отчет», поле загрузки данных, а также вкладки с визуализациями, которые станут активными после загрузки данных.



Таким образом, удалось реализовать процедуры обработки и последующей визуализации больших объемов экономической информации для принятия обоснованных управленческих решений. Количество различных видов визуализаций значительно увеличено по сравнению с известными прототипами.

Дальнейшая работа над программой осуществляется в направлении расширения вариаций отчетов, оптимизации программы и обеспечении кроссплатформенности.

## СПИСОК ЛИТЕРАТУРЫ

1. <https://dash-gallery.plotly.host/Portal/> Dash Enterprise App Gallery
2. <https://dash.plotly.com/> Dash Python User Guide

---

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

### INFORMATION SECURITY

**В.И. Юхнов, А.В. Красников**

#### **ЗАЩИЩЕННОЕ КЛИЕНТ-СЕРВЕРНОЕ ХРАНИЛИЩЕ ДАННЫХ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: защита данных, симметричное шифрование, AES-шифрование, protobuf, GRPC, база данных, клиент-серверное приложение.

В статье проведен анализ проблемы утечки данных из крупных сервисов, рассмотрены существующие решения защищенных хранилищ данных, выявлены сильные и слабые стороны. Сформулированы задачи и цели для реализации программного средства.

**V.I. Yukhnov, A.V. Krasnikov**

#### **SECURED CLIENT-SERVER DATA STORAGE**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: data protection, symmetric encryption, AES encryption, protobuf, GRPC, database, client-server application.

The article analyzes the problem of data leakage from large services, reviews existing solutions for secure data storage, and identifies strengths and weaknesses. The tasks and goals for the implementation of the software are formulated.

#### **Введение.**

Согласно исследованию, проведенному компанией InfoWatch, контролирующей около 50% российского рынка систем защиты конфиденциальных данных, за первое полугодие 2022г. в мире зарегистрирована 2101 утечка информации ограниченного доступа, что почти в два раза (на 93,2%) больше, чем за аналогичный период прошлого года.

Количество утечек в России за первое полугодие 2022 г. составило 305 (+45,9% по сравнению с I полугодием 2021 г.).

Практически еженедельно в первой половине года публиковались сведения о крупных утечках из российских компаний и госорганов, в их числе: РЖД, авиакомпания «Победа», телекоммуникационные компании «Ростелеком» и «ВымпелКом», информационный портал Ykt.ru, сервисы «Мир Тесен», Fotostrana.ru и Text.ru, развлекательный ресурс Pikabu, сервисы доставки «Яндекс.Еда», Delivery Club и 2 Berega, школа управления «Сколково», образовательный портал GeekBrains.

Из опубликованных отчетов видно, что даже крупные компании не всегда могут предотвратить утечку конфиденциальных и/или любой другой информации. Исходя из полученных аналитических данных приходим к выводу – информацию необходимо зашифровать так, чтоб расшифровать ее было невыгодно.

---

### **Постановка задачи.**

Целью данной работы является разработка защищенного клиент-серверного хранилища данных, обладающего следующими требованиями:

Сервер должен реализовывать следующую бизнес-логику:

- регистрация, аутентификация и авторизация пользователей;
- хранение приватных данных;
- обеспечение безопасности передачи и хранения данных;
- передача приватных данных владельцу по запросу.

Клиент должен реализовывать следующую бизнес-логику:

- аутентификация и авторизация пользователей на удалённом сервере;
- доступ к приватным данным по запросу.

Типы хранимой информации:

- произвольные текстовые данные;
- произвольные бинарные данные;
- данные банковских карт.

Для любых данных должна быть возможность хранения произвольной текстовой метainформации (принадлежность данных к веб-сайту, личности или банку, списки одноразовых кодов активации и прочее).

### **Анализ существующих защищенных хранилищ данных.**

Tresorit – облачное хранилище данных. Применяется сквозное шифрование и полный набор функциональных возможностей для бизнеса, команд и отдельных пользователей, отвечает требованиям HIPAA, GDPR, FedRAMP и множеству других правил защиты данных. Сервис ориентирован на B2B сектор, позволяя сотрудникам синхронизировать данные с другими филиалами компании.

Sync.com – облачное хранилище с нулевым разглашением. Инфраструктура с нулевым разглашением выглядит максимально надёжной, но результаты сторонних тестов и аудитов не публикуются. Данное решение может располагаться на компьютере пользователя, предоставляя в пользование 5ГБ дискового пространства. Если доступного дискового пространства недостаточно необходимо установить клиент синхронизации, который может вызывать конфликты в версиях файлов.

Internxt – облачное хранилище с открытым кодом и нулевым разглашением. Наряду с Internxt Drive, компания предлагает использовать Internxt Photos и Send, позволяющие хранить фото и безопасно ими делиться с другими пользователями. Internxt бесплатно предоставляет до 10 ГБ хранилища, также есть тарифные планы на 20 ГБ, 200 ГБ и 2 ТБ. Оплата возможна ежемесячно, ежегодно, а также пожизненные планы, с оплатой один раз и получением аккаунта на постоянной основе.

Все вышеперечисленные решения являются зарубежными продуктами, не соблюдающие закон № 242-ФЗ «О персональных данных». Могут собирать статистику использования без уведомления пользователя. Данные хранятся на серверах решений и попадают под законы страны, в которой они расположены. Нет возможности произвести интеграцию решения с другим программным продуктом.

### **Выбор программных средств и технологий разработки.**

Для серверной части приложения выбран язык Go. Главная особенность Go — в его минимализме. В то время как другие языки меняются, обрастая новыми функциями, Go изначально был создан, чтобы идеально решать поставленную перед ним задачу, поэтому чаще меняется только в сторону улучшения уже существующих инструментов, а не добавления новых.

Преимущества:

- простой синтаксис. В Go нет наследования, классов, объектов и сложных функций;

- много готовых инструментов для разработчиков. С языком поставляются уже готовые инструменты для форматирования и тестирования кода, создания документации, анализатор исходного кода и другие полезные утилиты;
- большое количество библиотек. Практически для каждой задачи есть готовые стандартные библиотеки внутри языка. Сторонние тоже есть, их список постоянно растёт. К коду на Go можно подключать библиотеки C (хотя для этого и потребуется некоторый опыт), которых очень много из-за популярности этого языка;
- высокая производительность. Если переписать код с другого языка на Go, можно даже без специальной оптимизации повысить производительность в 5–10 раз. Также в Go присутствует собственный макроассемблер, который позволяет добиваться максимальной производительности там, где это действительно нужно;
- надёжность. Программы на Go грамотно используют память и вычислительные ресурсы, поэтому работают стабильно;
- развитое и отзывчивое сообщество. Go — проект с открытым исходным кодом. Участники сообщества постоянно разрабатывают новые инструменты, продвигают его в IT-индустрии и с радостью отвечают на вопросы новичков.

В качестве базы данных используется PostgreSQL. PostgreSQL — это свободно распространяемая объектно-реляционная система управления базами данных (СУБД) с открытым исходным кодом, написанном на языке C.

Преимущества:

- расширяемость и богатый набор типов данных. Помимо стандартных, в PostgreSQL есть типы для геометрических расчётов, сетевых адресов и полнотекстового поиска. Мощная система расширений позволяет добавлять новые возможности и типы данных;
- масштабируемость. Для повышения производительности и масштабируемости в PostgreSQL используются разные виды блокировок на уровне таблиц и строк; шесть видов индексов, среди которых B-дерево и обобщённое дерево поиска (GiST) для полнотекстового поиска; наследование таблиц — для быстрого создания таблиц на основе имеющейся структуры;
- кросс-платформенность. PostgreSQL поддерживается всеми популярными операционными системами, среди которых различные дистрибутивы Linux и BSD, macOS, Windows, Solaris и другие;
- безопасность. В PostgreSQL есть множество инструментов для защиты данных от злоумышленников: пароль, Kerberos, LDAP, GSSAPI, SSPI, PAM и другие. Она позволяет управлять доступом к объектам БД на нескольких уровнях — от базы данных до отдельных столбцов, а также шифровать данные на аппаратном уровне;
- возможности NoSQL. Помимо стандартных форматов, PostgreSQL поддерживает XML, а с девятой версии — JSON и JSONB. Последний позволяет не разбирать JSON-документ перед записью в базу данных, что существенно ускоряет его сохранение в БД.

Protocol Buffers (Protobuf) — это формат сериализации данных, разработанный компанией Google. Он эффективно и компактно хранит структурированные данные в двоичной форме, что позволяет быстрее передавать их по сети. Protobuf поддерживает широкий спектр выбранных языков программирования и является платформонезависимым, что означает, что программы, написанные с его использованием, могут быть легко перенесены на другие платформы.

Формат Protobuf имеет ряд преимуществ перед другими форматами, такими как XML или JSON. Поскольку структурированные данные хранятся в двоичном формате, они гораздо меньше текстовых форматов, таких как XML или JSON, что позволяет быстрее

---

передавать их по сети. Protobuf разработан так, чтобы его было легко расширять, что делает его идеальным для работы с быстро меняющимися структурами данных и новыми возможностями. Наконец, специально сгенерированный исходный код Protobuf может быть оптимизирован для повышения скорости работы, что позволяет создавать более быстрые приложения, использующие меньше памяти.

GRPC (Google Remote Procedure Calling) — система удаленного вызова процедур, разработанная компанией Google.

Основное назначение — реализация взаимодействия между микросервисными архитектурами при разработке приложений.

Фреймворк GRPC включает в себя три основных составляющих:

- стандарт сериализации данных Protocol Buffers (Protobuf). Сериализация подразумевает преобразование текстовых данных в бинарные (двоичные), оптимизированные под быстрый обмен короткими сообщениями;
- протокол передачи данных HTTP/2. Протокол является дальнейшим развитием гипертекстового протокола HTTP и оптимизирован для работы с бинарными данными. Он позволяет разбивать передачи на отдельные небольшие пакеты и обеспечивает одновременную поддержку нескольких запросов, включая двунаправленную передачу информации;
- язык описания интерфейса IDL. Предназначен для упрощенного описания сервисов удаленного вызова процедур с возможностью автоматической генерации кода для выбранной программной среды.
- GRPC, как и большинство распределенных сервисов, организован по принципу клиент-серверной архитектуры. Клиенты посылают на сервер информационные запросы, сервер предоставляет ответы и методы их обработки. При этом программная реализация клиента и сервера не имеет особого значения благодаря кроссплатформенности протокола GRPC.

AES (Advanced Encryption Standard) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES.

Режим GCM. Режим гаммирования с аутентификацией Галуа (Galois/Counter mode – GCM) порождает шифртекст так же, как в режиме CTR. Блоки счетчика шифруются блочным шифром, в результате чего порождается гамма. Затем к гамме и открытому тексту применяется операция XOR, и получается шифртекст.

Отличие от режима CTR заключается в том, что GCM не только шифрует открытый текст, но также аутентифицирует шифртекст. Это означает, что знание ключа шифрования позволяет проверить целостность шифртекста, иными словами, обнаружить несанкционированные изменения шифртекста, если проверка не проходит. Такое обнаружение полезно, потому что в основе многих атак лежит изменение шифртекста: измененный шифртекст подается оракулу, и анализируется его ответ.

### **Создание структуры PROTO.**

Proto-файлы – это файлы описания протоколов, которые используются в системе RPC (Remote Procedure Call) для определения сообщений, передаваемых между клиентом и сервером. Они содержат инструкции на языке ProtoBuf (Protocol Buffers) для определения структуры данных, используемых в конкретном протоколе.

На листинге 1 описана структура RPC-сервиса.

```
service GrpcService {
  rpc CreateUser(UserRegisterRequest) returns
  (AuthorizedResponse);
  rpc LoginUser(UserAuthorizedRequest) returns
  (AuthorizedResponse);

  rpc SaveRawData(SaveRawDataRequest) returns (ErrorResponse);
  rpc SaveLoginWithPassword(SaveLoginWithPasswordRequest)
returns (ErrorResponse);
  rpc SaveBinaryData(SaveBinaryDataRequest) returns
(ErrorResponse);
  rpc SaveCardData(SaveCardDataRequest) returns (ErrorResponse);

  rpc GetRawData(GetRawDataRequest) returns
(GetRawDataResponse);
  rpc GetLoginWithPassword(GetLoginWithPasswordRequest) returns
(GetLoginWithPasswordResponse);
  rpc GetBinaryData(GetBinaryDataRequest) returns
(GetBinaryDataResponse);
  rpc GetCardData(GetCardDataRequest) returns
(GetCardDataResponse);

  rpc GetAllSavedDataNames(GetAllSavedDataNamesRequest) returns
(GetAllSavedDataNamesResponse);
}
```

### Даталогическая модель таблицы хранения данных.

В таблице 1 представлена даталогическая модель таблицы «raw\_data».

Таблица 1 - даталогическая модель таблицы «raw\_data».

Наименование поля	Тип данных	Длина	Допустимое значение	Первичный ключ	Внешний ключ	Описание
name	varchar	45	NOT NULL, UNIQUE	+		Ключ хранимых данных
data_type	int	2	NOT NULL			Тип хранимых данных
data	bytea				+	Хранимая информация в бинарном формате
user_id	varchar	45	References to user by ID		+	Ссылка на пользователя

### Использование мета информации для аутентификации.

Для аутентификации пользователя и авторизации выполняемых запросов используется JWT-токен. JSON Web Token (JWT) — это открытый стандарт (RFC 7519) для создания токенов доступа, основанный на формате JSON. Так как данные потоковые используется Интерсептор авторизации — это некоторый класс, перехватывающий вызовы методов целевого класса и "оборачивающий" их в некоторую дополнительную функциональность.

На листинге 2 описан интерсептор авторизации.

```
func (interceptor *AuthInterceptor) authorize(ctx
context.Context) error {
    accessToken, err :=
interceptor.jwtManager.ExtractJWTFromContext(ctx)
    if err != nil {
        return status.Errorf(codes.Unauthenticated, err.Error())
    }

    token, err := interceptor.jwtManager.ParseToken(accessToken)
    if err != nil || !token.Valid {
        return status.Errorf(codes.Unauthenticated, "access token
is invalid: %v", err)
    }

    return nil
}
```

### Шифрование данных.

Алгоритмом шифрования выбран симметричный алгоритм AES с режимом счетчика Галуа — это режим работы блочного шифра, который использует универсальное хеширование над двоичным полем Галуа для обеспечения аутентифицированного шифрования.

Режим счетчика Галуа — это режим работы криптографических блочных шифров с симметричным ключом, получивший широкое распространение благодаря своей эффективности и быстрдействию. Пропускная способность в режиме счетчика Галуа для современных высокоскоростных каналов связи может быть достигнута при разумных аппаратных ресурсах.

На листинге 3 описан метод блочного шифрования данных.

```
func (cm *CipherManager) Encrypt(plaintext []byte) ([]byte,
error) {
    c, err := aes.NewCipher(cm.secretKey)
    if err != nil {
        return nil, err
    }

    gcm, err := cipher.NewGCM(c)
    if err != nil {
        return nil, err
    }

    nonce := make([]byte, gcm.NonceSize())
    if _, err = io.ReadFull(rand.Reader, nonce); err != nil {
        return nil, err
    }

    return gcm.Seal(nonce, nonce, plaintext, nil), nil
}
```

### Тестирование.

Создадим пользователя с данными: Login = admin, Password = P@ssw0rd.  
Выполним вызов RPC метода «CreateUser», передав данные пользователя.



При успешном выполнении вызова получим статус-код «0 OK» и ответ с JWT-токеном пользователя, который необходимо использовать при дальнейших вызовах к серверу.

На рисунке 1 представлен RPC запрос создания пользователя.

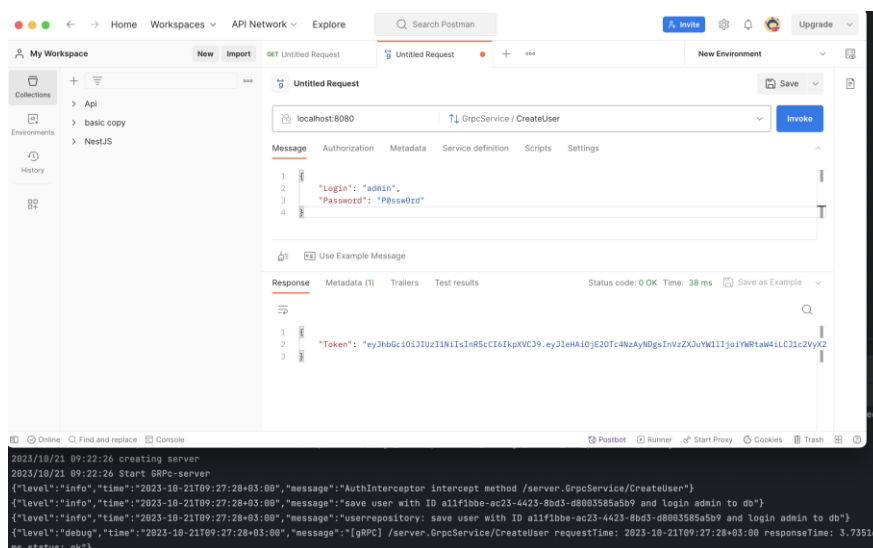


Рисунок 1. RPC запрос создания пользователя

После успешной авторизации и получении JWT-токена создадим запись с данными банковской карты.

На рисунке 2 представлен RPC запрос сохранения данных банковской карты.

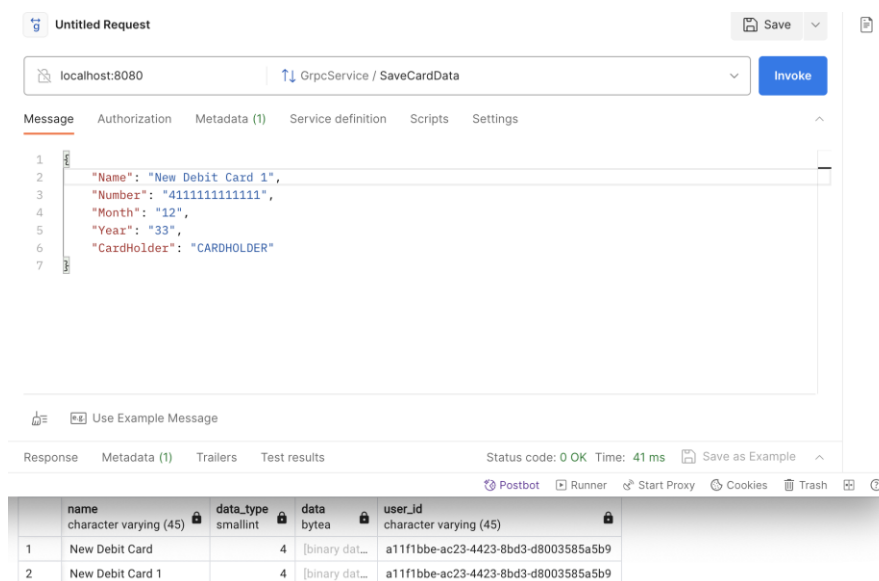


Рисунок 2. RPC запрос сохранения данных банковской карты

### Выводы.

Разработанное хранилище соответствует такими требованиям, как:

- расширяемость. Благодаря использованию PROTOBUF имеется возможность сгенерировать интерфейс доступа для любого из поддерживаемых языков программирования;
- защищенность. Доступ к хранилищу происходит по токenu авторизации, а данные хранятся в зашифрованном виде;
- мультиформатность. Приложение позволяет сохранять информацию различных типов данных;

- 
- быстродействие. Благодаря работе по RPC достигается высокое быстродействие, аналогичное работе на локальной машине.

#### СПИСОК ЛИТЕРАТУРЫ

1. gRPC framework, официальный сайт. [Электронный ресурс] URL: <https://grpc.io/>, 2023
2. AES. Описание и принцип работы алгоритма шифрования [Электронный ресурс] URL: <https://cryptographyacademy.com/aes/>, 2023
3. PostgreSQL. Официальный сайт базы данных [Электронный ресурс] URL: <https://www.postgresql.org> , 2023
4. Go. Официальный сайт языка программирования Go [Электронный ресурс] URL: <https://go.dev/> , 2023

Д.А. Пикуль

#### АНАЛИЗ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КИБЕРБЕЗОПАСНОСТИ

Донской государственной технической университет,  
Ростов-на-Дону, Россия

Ключевые слова: информационная безопасность, искусственный интеллект, данные, защита информации, нейронная сеть, угрозы, методы защиты информации.

В данной научной статье представлены основные методы использования искусственного интеллекта в области кибербезопасности. В ходе исследования освещены как преимущества, так и ограничения применения этой технологии. Рассмотрены как положительные, так и негативные аспекты использования методов искусственного интеллекта в контексте обеспечения кибербезопасности.

D.A. Pikul

#### ANALYSIS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Don State Technical University,  
Rostov-on-Don, Russia

Keywords: information security, artificial intelligence, data, information protection, neural network, threats, information security methods.

This scientific article presents the fundamental methods of utilizing artificial intelligence in the realm of cybersecurity. Throughout the research, both the advantages and limitations of applying this technology are elucidated. Both the positive and negative aspects of employing artificial intelligence methods in the context of cybersecurity are examined.

#### Введение.

В современном информационном веке, сопровождаемом внушительным ростом цифровых технологий и интернет-связанной активностью, кибербезопасность стала одним из самых важных и актуальных вопросов. С каждым днем киберугрозы становятся все более сложными, организованными и разрушительными, поставляя перед нашими информационными системами и данными угрозы без прецедента. В ответ на эту

---

эволюцию киберугроз, технологии и методы обнаружения и предотвращения кибератак также продолжают развиваться, и в этом контексте искусственный интеллект (ИИ) занял выдающееся место.

ИИ предоставляет мощный инструмент для анализа больших объемов данных и выявления сложных угроз в реальном времени. Он способен адаптироваться к изменяющейся угрозной среде и автоматизировать процессы обнаружения, что позволяет снижать время реакции на инциденты и улучшать общую эффективность систем кибербезопасности. Роль ИИ в обеспечении безопасности информационных систем стала критической, исследования в этой области продолжают расширять горизонты наших знаний и возможностей.

**Цель данной** научной статьи заключается в исследовании и анализе роли и применения ИИ в контексте обнаружения и предотвращения кибератак. Основными задачами работы являются:

- рассмотрение способов, которыми ИИ может быть применён для обнаружения и предотвращения киберугроз в информационных системах;
- рассмотрение достоинств и недостатков ИИ в защите информации;
- обзор текущих тенденций и перспектив развития ИИ в области кибербезопасности;
- приведение примеров использования ИИ для защиты информации.

Рассмотрим следующие способы, которыми ИИ может быть применён для обнаружения и предотвращения киберугроз в информационных системах:

- анализ событий и трафика: ИИ способен анализировать огромные объемы событий и сетевого трафика в реальном времени. Это позволяет выявлять аномалии, подозрительное поведение и атаки, основываясь на шаблонах и предыдущих инцидентах;
- идентификация угроз и аномалий. Системы на основе ИИ могут автоматически выявлять угрозы, такие как вирусы, вредоносные программы и фишинговые попытки. Они также способны обнаруживать аномалии в поведении пользователей и устройств, что может свидетельствовать о несанкционированном доступе;
- прогнозирование угроз. Используя аналитику данных и обучение на больших данных, ИИ может предсказывать вероятные угрозы и атаки на основе анализа текущей ситуации и исторических данных;
- автоматизация реакции. ИИ может автоматически реагировать на обнаруженные угрозы, включая блокирование атак и изоляцию уязвимых частей сети. Это снижает время реакции на инцидент и минимизирует потенциальные убытки;
- обучение на размеченных данных. Модели машинного обучения могут обучаться на размеченных данных, что позволяет им выявлять новые угрозы и атаки на основе известных шаблонов [2];
- мониторинг и анализ уязвимостей. ИИ может сканировать информационные системы для выявления уязвимостей, которые могли бы быть использованы злоумышленниками, и предлагать рекомендации по их устранению;
- интеллектуальные средства защиты. Используя ИИ, можно создавать более интеллектуальные средства защиты, способные адаптироваться к новым атакам и угрозам;
- обучение с подкреплением. Этот метод позволяет системам ИИ «учиться» на основе награды и наказания, что делает их более способными к адаптации и улучшению в реальном времени [4].

Эти методы представляют собой несколько примеров того, как ИИ может применяться для обнаружения и предотвращения киберугроз. Исследования в этой

---

области продолжают развиваться, и их роль в обеспечении кибербезопасности становится все более важной.

#### **Достоинства и недостатки.**

Для начала можно рассмотреть его положительные стороны. К достоинствам можно отнести следующее [1]:

- обработка большого количества параметров. Одной из ключевых характеристик ИИ является его способность обрабатывать огромное количество данных и учитывать множество параметров, которые человеку физически сложно или невозможно учесть;
- скорость и автоматизация. Технологии ИИ способствуют повышению скорости и уровня автоматизации обработки больших объемов информации, при этом повышая качество и эффективность этого процесса;
- возможность быстрого обучения. В отличие от статистических методов, ИИ способен обучаться, что делает его более адаптивным к новым условиям и угрозам;
- обнаружение новых угроз. ИИ способен не только выявлять известные угрозы, но и обнаруживать аномалии и таргетированные атаки, что делает его более эффективным в предотвращении разнообразных угроз.

Несмотря на все достоинства ИИ, он также имеет ряд недостатков:

- технические разработки. ИИ действует на основе логических выводов, но его ответы могут не всегда соответствовать стереотипным ответам, что может вызвать недопонимание и несоответствие ожиданиям [5];
- отсутствие защиты от столкновений. Несмотря на присутствие наблюдателей, системы ИИ иногда могут работать неправильно, и выявление этих ошибок может быть сложным, что представляет риск для целостности данных и работоспособности системы;
- узкая направленность. ИИ часто разрабатывается для конкретных задач и может быть неспособен к универсальному применению, что приводит к созданию нескольких отдельных сетей вместо единой универсальной;
- сложность принципов работы нейросетей. Сложная организация сетей ИИ может затруднять понимание точных принципов, по которым нейросеть принимает решения, что может усложнить анализ ее выводов.

#### **Обзор основных текущих тенденций и перспектив развития.**

Текущие тенденции представляют собой текущее состояние сферы деятельности, ее характеристики и особенности, которые могут включать в себя изменения, новшества, модные практики или сдвиги в важных аспектах данной области. Текущие тенденции могут быть результатом социокультурных, технологических, экономических или политических изменений. К тенденциям ИИ, на данный момент, относятся [3]:

- расширение применения ИИ в кибербезопасности. Современные системы кибербезопасности все больше используют ИИ для обнаружения и предотвращения атак. Это охватывает области, такие как обнаружение аномалий, идентификация угроз, анализ событий и реагирование на инциденты;
- облако и кибербезопасность. Расширение облачных вычислений приводит к необходимости усовершенствования кибербезопасности в облаке. ИИ используется для защиты облачных ресурсов, а также для обеспечения безопасности облачных приложений и данных;
- угрозы ИИ. С развитием ИИ возникают новые угрозы, связанные с их злоупотреблением. Злоумышленники могут использовать ИИ для создания

---

более утонченных и эффективных атак. Таким образом, разработчики кибербезопасности должны уделять внимание защите от таких угроз.

К перспективам развития ИИ в области кибербезопасности относятся:

- усиление анализа с большими данными. ИИ будут все более интегрироваться в кибербезопасность для анализа огромных объемов данных из различных источников. Это позволит более точно идентифицировать аномалии и атаки;
- автоматизация и оркестрация. Перспективы развития включают в себя создание автоматизированных систем, способных реагировать на атаки без вмешательства человека. Оркестрация инцидентов станет более эффективной;
- интеграция с квантовыми вычислениями. Квантовые вычисления предоставляют новые возможности для шифрования и дешифрования данных. ИИ будут интегрированы с квантовыми вычислениями для более надежной кибербезопасности;
- развитие технологий предсказания. Предсказательная аналитика, поддерживаемая ИИ, будет использоваться для выявления потенциальных угроз и атак до их возникновения, что позволит предупредить инциденты;
- многоуровневая защита. Системы кибербезопасности будут использовать комбинацию методов и технологий, включая ИИ, для обеспечения многоуровневой защиты и уменьшения рисков [3].

#### **Вывод.**

В настоящей статье были рассмотрены основные аспекты использования ИИ в области кибербезопасности. Анализ применения ИИ в этой сфере позволяет выявить как положительные, так и негативные стороны его использования.

Существует множество примеров использования ИИ в сфере кибербезопасности таких как: системы обнаружения аномалий (IDS/IPS), анализ угроз, антивирусное сканирование, анализ электронной почты и другие.

Одним из значительных достоинств использования ИИ в кибербезопасности является его способность обрабатывать огромные объемы данных в реальном времени. Это позволяет выявлять аномалии, подозрительные события и атаки, которые могли бы остаться незамеченными при ручном анализе. ИИ также способен предсказывать потенциальные угрозы на основе анализа текущих данных и исторических трендов, что позволяет предотвращать атаки до их возникновения.

Кроме того, ИИ способен дообучаться, что делает его более адаптивным к изменяющимся угрозам и сценариям атак. Это позволяет быстро реагировать на новые виды угроз, даже без необходимости вручную перенастраивать системы.

Однако, следует признать, что использование ИИ также сопряжено с некоторыми недостатками. В частности, ИИ может выносить решения, которые не всегда соответствуют ожиданиям или стандартным ответам. Это может усложнять понимание принципов работы ИИ и оказывать влияние на доверие к его выводам.

Кроме того, с увеличением использования ИИ в кибербезопасности возникает риск злоупотребления этой технологией злоумышленниками. Они могут использовать ИИ для создания более утонченных и эффективных атак, что требует разработки более сложных методов защиты.

В заключение, можно утверждать, что ИИ представляет собой мощный инструмент для обеспечения кибербезопасности, который обладает значительными преимуществами в обнаружении и предотвращении атак. Однако важно учитывать его недостатки и постоянно развивать методы защиты, чтобы минимизировать возможные риски и обеспечить безопасность информационных систем в долгосрочной перспективе.

---

## СПИСОК ЛИТЕРАТУРЫ

1. Abu-Nimeh S, Nappa D, Wang X. Learning and Classification of Malware Behavior. // In Proceedings of the 2007 European Symposium on Research in Computer Security (ESORICS). — 2007. — С. 20.
2. Thomas K, Verma D, Sorrell S, Lee W, Srinivasan A. Machine Learning at Microsoft with Security in Mind. // arXiv preprint arXiv. — 2019. — № 1902.07047.
3. Roesch M. Snort - Lightweight Intrusion Detection for Networks. // USENIX LISA, 1999. — С. 11.
4. Kaur M, Gupta S, Singla V. Artificial Intelligence in Cyber Security: A Review. // Procedia Computer Science. — 2021. — № 179. — С. 358-365.
5. Thomas K, Verma D, Sorrell S, Lee W, Srinivasan A. Machine Learning at Microsoft with Security in Mind. // arXiv preprint. — 2019. — № 1902.07047.

**Н.А. Байтяков, С.В. Мухачев**

### **АНАЛИЗ КИБЕРАТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И МЕР ПО ИХ ПРЕДОТВРАЩЕНИЮ**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения», Екатеринбург, Россия

Ключевые слова: информация, информационная безопасность, угроза информационной безопасности, критическая информационная инфраструктура, кибератака, защита информации, неправомерный доступ к информации.

Статья посвящена анализу кибератак на объекты критической информационной инфраструктуры. Рассматриваются также организационные и правовые меры по их предотвращению. Приводятся примеры кибератак, анализируются используемые приемы нападения. Показана масштабность и опасность кибератак, и катастрофичность их последствий. Проведен анализ организационно-правовой системы обеспечения информационной безопасности и предотвращения кибератак на объектах критической информационной инфраструктуры.

**N.A. Baytyakov, S.V. Mukhachev**

### **ANALYSIS OF CYBER ATTACKS ON CRITICAL INFORMATION INFRASTRUCTURE FACILITIES AND MEASURES TO PREVENT THEM**

Ural State University of Railway Transport, Ekaterinburg, Russia

Keywords: information, information security, threat to information security, critical information infrastructure, cyberattack, information protection, unauthorized access to information.

The article is devoted to the analysis of cyber attacks on objects of critical information infrastructure. Organizational and legal measures to prevent them are also being considered. Examples of cyberattacks are given, the methods of attack used are analyzed. The scale and danger of cyberattacks and the catastrophism of their consequences are shown. The analysis of

---

the organizational and legal system for ensuring information security and preventing cyber attacks on critical information infrastructure facilities has been carried out.

Проблема обеспечения информационной безопасности на объектах критической информационной инфраструктуры (КИИ) приобрела особую актуальность в связи с тем, что информационные технологии играют определяющую роль в организации процессов управления в различных сферах деятельности. В текущем десятилетии государство, частные компании, исследователи вынуждены уделять много внимания защите от многочисленных угроз, связанных с информационной безопасностью. Одна из наиболее серьезных и получившая широкое распространение угроз – кибератаки. В современном мире, насыщенном информационными технологиями, риск существенного ущерба часто связан с реализацией кибератак на объекты КИИ. Количество таких кибератак велико. Поэтому предотвращение данной угрозы в отношении КИИ приобрело особую значимость.

Понятие КИИ закреплено в Федеральном законе от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Критическая информационная инфраструктура – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, а также сети электросвязи, используемые для организации их взаимодействия.

Еще одно важное понятие, которое определено в Федеральном законе № 187-ФЗ – компьютерная атака. Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации. Следует отметить, что в средствах массовой информации и специальной литературе часто вместо термина «компьютерная атака» не совсем точно используют термин «хакерская атака». Однако это неверно. Термин «хакерская атака» имеет более широкое смысловое значение: атака с целью нанесения ущерба в сфере информационной безопасности, реализуемая злоумышленником, обладающим специальными познаниями.

Важно различать объекты и субъекты КИИ. Субъект КИИ – государственные органы, государственные учреждения, российские юридические лица, индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, Российские юридические лица, индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей. Объект КИИ – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ. Объекты КИИ могут содержать как общедоступную информацию, так и конфиденциальные данные, защищенные тем или иным способом.

Статистика кибератак на объекты КИИ широко представлена и описана в публикациях [1-4]. Наиболее значимые и показательные случаи кибератак за последнее десятилетие в странах Европы и Америки представлены на рисунке 1.

Рисунок наглядно демонстрирует разнообразие объектов атаки: от промышленных предприятий до криптовалютной биржи. Показательно и то, что кибератаки угрожают любой стране, независимо от географического положения и общественного уклада. Цели

таких кибератак также различны: получение «выкупа» за расшифровку данных, хищение криптовалюты, незаконное копирование персональных данных, получение доступа к финансовой отчетности, выведение из строя промышленных мощностей, нанесение ущерба здоровью людей, реализация политических устремлений и так далее. Причем, с течением времени, объекты и цели атак расширяются. Также расширяется масштаб явления в целом.

Все перечисленные тенденции справедливы и для России [5].

В целом, динамика количества успешных кибератак на промышленные объекты в мире наглядно приведена на рисунке 2 [6].

В России ситуация обострилась после начала специальной военной операции на Украине, т.к. сегодня кибератаки – один из видов оружия.

Особый интерес для атак, связанных с политическими мотивами, представляют нефтяная и ядерная отрасли. Это обстоятельство отчетливо прослеживается в примерах таких кибератак.

						Атаки хакерской группировки Darkside на различные компании (США)	Атака на энергетическую компанию Marquard & Bahls (Германия)
						Атака на компанию JBS (Бразилия)	Атака на Международный Комитет Красного Креста (Швейцария)
					Атака на IT-компанию SolarWinds (США)	Атака на компанию Sol Oriens, связанную с производством ядерного оружия (США)	Атака на новостную организацию News Corp (США)
				Атака на сеть дата-центров CygusOne (США)	Утечка данных пользователей Zoom	Атака на Национальную службу здравоохранения Ирландии (HSE)	Атака на криптовалютную биржу Crypto.com
		Атака NotPetya на систему финансовой отчетности (Украина)		Атака на органы государственного управления в Луизиане (США)	Атака на Energias de Portugal (Португалия)	Атака на предприятия трубопроводной системы Colonial Pipeline (США)	Утечка данных в сети отелей Marriott (США)
		Атака вируса Egebus на веб-хостинговую компанию Nayana (Южная Корея)		Атака на производителя авиазапчастей ASCO (Бельгия)	Атака на Garmin (США)	Взлом Microsoft Exchange Server	Атака на блокчейн Ethereum
Атака вредоносной программы Stuxnet на промышленные предприятия Ирана	Атаки вредоносной программы Petya по всему миру	Атаки вредоносной программы WannaCry по всему миру	Атака вируса SamSam на клинику Hancock Health (США)	Атака на металлургическую компанию Norsk Hydro (Норвегия)	Атака вируса Snake на предприятия General Electric, Honda и др.	Атака на предприятие водоснабжения в Олдмар (США)	Атака программы-вымогателя Conti на финансовую систему Коста-Рика
2010-212	2016	2017	2018	2019	2020	2021	2022

Рисунок 1. Наиболее значимые и показательные случаи кибератак.



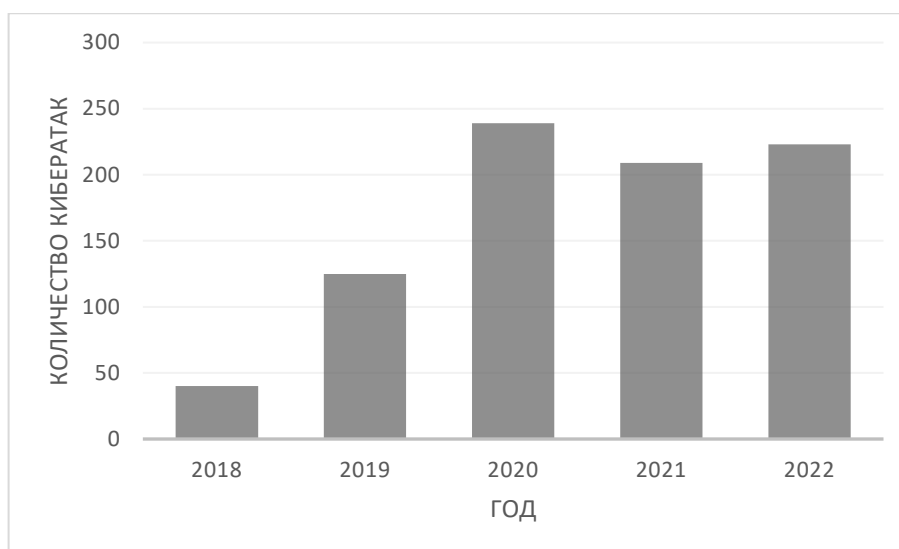


Рисунок 2. Динамика успешных кибератак.

В 2010 г. совершена достаточно успешная попытка выведения ядерной программы Ирана из строя путем внедрения вируса Stuxnet в систему управления оборудованием промышленного предприятия по обогащению урана [7]. В 2012 г. нефтедобывающая компания Saudi Aramco на протяжении месяца восстанавливала свою сеть после ряда кибератак. Известны кибератаки на такие важные и опасные объекты, как АЭС: Susquehanna, США, 2012 г.; Моңжу, Япония, 2014 г.; КННР, Южная Корея, 2014 г.

Российские компании не стали исключением, и также попали в список жертв кибератак. Самыми узнаваемыми и важными среди них стали компании «Сбербанк» [8], «Роснефть» [9], «Башнефть» [10].

Приведенные примеры представляют собой лишь малую часть кибератак, реализованных в последнем десятилетии. Приведенные примеры демонстрируют меру опасности и потому стали предметом обсуждения среди широкой общественности.

Работа объектов КИИ должна быть организована таким образом, чтобы обеспечить их безопасную эксплуатацию. Информационная безопасность КИИ связана с обеспечением эффективного и безопасного использования информации на КИИ, предотвращением утечки и хищения информации, обеспечением совместной работы множества пользователей и подразделений без нарушения целостности и конфиденциальности данных, гарантией эффективного функционирования системы в целом, ее отказоустойчивости и устойчивости к внешним угрозам.

Для обеспечения информационной безопасности разрабатывается система различных мер, которая защищает объект от внутренних и внешних угроз, обеспечивает криптографическую защиту данных, возможность проведения оперативного анализа и контроля информации на КИИ.

Немаловажную роль в реализации и укреплении информационной безопасности на объектах КИИ играют специальные исследования. Они призваны заложить научную базу как для программно-технических мероприятий, так и для совершенствования организационно-правового регулирования. Используются различные математические модели, позволяющие выявить иерархическую структуру подлежащего защите объекта КИИ, понять функционирование каждого уровня, увидеть опасные уязвимости и предложить механизмы предотвращения ущерба [11]. Разрабатываются принципы работы систем раннего обнаружения кибератак, развиваются методики, позволяющая получать численную оценку эффективности мониторинга параметров технологических процессов [12].

С целью обеспечения информационной безопасности запущена Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак

---

(ГосСОПКА). Корпоративный центр ГосСОПКА автоматизирует выявление инцидентов, реагирование на них и взаимодействие с Национальным координационным центром по компьютерным инцидентам (НКЦКИ).

В связи с необходимостью укрепления информационной безопасности и предотвращения кибератак в России разработана комплексная организационно-правовая система регулирования отношений в сфере информационной безопасности на объектах КИИ.

Разработаны соответствующие нормативно-правовые акты.

Важный элемент обеспечения информационной безопасности – категорирование объектов КИИ. Объект КИИ, вне зависимости от того, в какой сфере работает организация, может быть отнесен к значимым или незначимым. Значимость объектов и правила категорирования определено в Постановлении Правительства РФ от 08.02.2018 №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». Документ содержит требования, которые позволяют организациям провести инвентаризацию и категорирование эксплуатируемых систем. Всего предусмотрено три категории значимости, первая – самая высокая.

Основными критериями категорирования являются: социальная значимость, что включает в себя причинение ущерба людям, прекращение или нарушение функционирования, отсутствие доступа к государственной услуге, политическая, экономическая, экологическая значимость. Исходными данными для определения категории служат сведения об объекте КИИ (назначение, архитектура объекта, применяемые программные и аппаратные средства, взаимодействие с другими объектами КИИ, наличие и характеристики доступа к сетям связи); выполняемые процессы (управленческие, технологические, производственные, финансово-экономические, иные) и состав обрабатываемой информации; декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект КИИ; сведения о взаимодействии и/или зависимости от других объектов КИИ; угрозы безопасности информации в отношении объекта КИИ, а также имеющиеся данные о компьютерных инцидентах, произошедших ранее на объектах КИИ соответствующего типа.

Требования по защите объекта КИИ напрямую зависят от субъекта КИИ в соответствии с его критерием значимости. Регулирование безопасности объектов КИИ регламентируется Приказом ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования». Деятельность по защите информации подлежит обязательной аккредитации уполномоченными организациями в соответствии с Постановлением Правительства РФ от 30 сентября 2022 г. N 1729 «Об утверждении Положения о государственной аккредитации российских организаций, осуществляющих деятельность в области информационных технологий». ФСТЭК России проводит тщательную проверку компаний на наличие необходимых ресурсов, обучения и опыта в области защиты информации. При этом основной целью является определение степени готовности организации к защите своей информации, а также соблюдение установленных законодательством критериев.

В обеспечении информационной безопасности и противодействия кибератакам задействованы и уголовно-правовые меры. УК РФ содержит главу 28 «Преступления в сфере компьютерной информации». Она содержит следующие статьи: 272 «Неправомерный доступ к компьютерной информации», 273 «Создание, распространение и использование вредоносных программ», 274 «Нарушение правил эксплуатации средств

---

хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» и 274.2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования». Последние две непосредственно связаны с КИИ. Наиболее жесткая санкция – лишение свободы на срок до 7 лет – предусмотрена за деяния, которые повлекли тяжкие последствия или создали угрозу их наступления.

Таким образом, проблема обеспечение информационной безопасности и предотвращения кибератак крайне актуальна. Приведенные примеры говорят об опасности кибератак, последствия которых могут быть катастрофическими.

Для обеспечения информационной безопасности на объектах КИИ необходимо реализовать комплексный подход, который включает следующие компоненты:

1. Выполнение мероприятий по категорированию. Сбор первичных данных о субъекте и объектах КИИ. Идентификация организации в качестве субъекта КИИ. Выявление и категорирование значимых объектов. От уровня защищенности значимого объекта КИИ, которому он должен соответствовать зависит набор организационных и технических мер, обеспечивающих блокирование угроз безопасности информации, последствиями которых может быть прекращение или нарушение его функционирования.
2. Создание системы информационной безопасности значимых объектов КИИ. Цель – обеспечение их устойчивого функционирования и готовность к предотвращению угроз завтрашнего дня. Как раз здесь необходимо использовать результаты научных исследований в области информационной безопасности.
3. Совершенствование. Дело в том, что система информационной безопасности, запущенная однажды, должна не только непрерывно функционировать, но и развиваться, адаптироваться к вновь возникающим условиям и угрозам. Как раз здесь необходимо использовать результаты научных исследований в области информационной безопасности.
4. Мониторинг и контроль. Цель – определить, как обстоят дела в области обеспечения информационной безопасности, и спланировать, какие меры необходимо предпринять для улучшения системы защиты информации.

#### СПИСОК ЛИТЕРАТУРЫ

1. Статистика атак на промышленные организации [Электронный ресурс]. – Режим доступа: URL: [https://rdc.grfc.ru/2021/07/kiberataki\\_na\\_kii/](https://rdc.grfc.ru/2021/07/kiberataki_na_kii/) (дата обращения 29.09.2023).
2. Кибератаки на критическую информационную инфраструктуру [Электронный ресурс]. – Режим доступа: URL: <https://www.ptsecurity.com/ru-ru/research/analytics/industrial-cybersecurity-threatscape-2022/> (дата обращения 29.09.2023).
3. Крупнейшие утечки данных и кибератаки 2022 года [Электронный ресурс]. – Режим доступа: URL: [https://translated.turbopages.org/proxy\\_u/en-ru.ru.1539ba98-64562afa-420833f0-74722d776562/https://www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022](https://translated.turbopages.org/proxy_u/en-ru.ru.1539ba98-64562afa-420833f0-74722d776562/https://www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022) (дата обращения 29.09.2023).
4. Крупнейшие кибератаки 2022 год [Электронный ресурс]. – Режим доступа: URL: <https://vc.ru/finance/515029-krupneyshie-kiberataki-2022-god> (дата обращения 29.09.2023).

5. Число кибератак в России и в мире [Электронный ресурс]. – Режим доступа: URL: [https://www.tadviser.ru/index.php/index.php/Статья: Число\\_кибератак\\_в\\_России\\_и\\_в\\_мире](https://www.tadviser.ru/index.php/index.php/Статья:Число_кибератак_в_России_и_в_мире) (дата обращения 29.09.2023).
6. Актуальные киберугрозы для промышленных организаций: итоги 2022 года [Электронный ресурс]. – Режим доступа: URL: <https://www.ptsecurity.com/ru-ru/research/analytics/industrial-cybersecurity-threatscape-2022/> (дата обращения 29.09.2023).
7. Первые пять жертв Stuxnet были тщательно отобраны атакующими и в итоге позволяли осуществить атаку на завод по обогащению урана в городе Нетенз [Электронный ресурс]. – Режим доступа: URL: <https://www.kaspersky.ru/blog/stuxnet-victims-zero/6119/> (дата обращения 29.09.2023).
8. Сбербанк отразил около 500 кибератак с начала 2022 года [Электронный ресурс]. – Режим доступа: URL: <https://securitymedia.org/news/sberbank-otrazil-okolo-500-kiberatak-s-nachala-2022-goda.html> (дата обращения 29.09.2023).
9. «Роснефть» сообщила о мощной хакерской атаке на свои серверы [Электронный ресурс]. – Режим доступа: URL: [https://www.rbc.ru/technology\\_and\\_media/27/06/2017/595241.7629a7947dc9d430d2c](https://www.rbc.ru/technology_and_media/27/06/2017/595241.7629a7947dc9d430d2c) (дата обращения 29.09.2023).
10. Клон Вируса WannaCry атакует крупные компании – пострадала «Башнефть» [Электронный ресурс]. – Режим доступа: URL: <https://promdevelop.com/news/virus-wannacry-atakuet-krupnye-kompanii-postradala-bashneft/> (дата обращения 29.09.2023).
11. Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия / А. А. Захаров, А. С. Римша, А. М. Харченко, И. Р. Зилькарнеев // Вестник УрФО. Безопасность в информационной сфере. – 2017. – № 3(25). – С. 24-33.
12. Разработка моделей и методов раннего обнаружения кибератак на объекты энергетики металлургического предприятия / А. Н. Соколов, А. Н. Рагозин, А. Е. Баринов [и др.] // Вестник УрФО. Безопасность в информационной сфере. – 2021. – № 3(41). – С. 65-87.

**И.В. Грибанов<sup>1</sup>, Б.П. Борисов<sup>2</sup>**

## **АНАЛИЗ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ОТ DDOS-АТАК В КОРПОРАТИВНЫХ СЕТЯХ**

Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Ростов-на-Дону, Россия<sup>1</sup>  
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: локальная сеть, DDOS-атака, система защиты сети StormWall, Usergate, Континент 4 NGFW, Diamond VPN/FW, VipNet xFirewall 5, Ideco NGFW, DDoS-Guard, Qrator, Rostelecom DDoS Protection, Kaspersky DDoS Prevention.

В данной статье проведен разбор возможных DDoS-атак, а также анализ эффективности использования различных решений для предотвращения воздействия DDoS-атак на сетевую инфраструктуру компании.

## ANALYSIS OF THE EFFECTIVENESS OF DDOS PROTECTION SYSTEMS IN CORPORATE NETWORKS

Federal State Autonomous Educational Institution of Higher Education "Southern Federal University", Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

**Keywords:** local area network, DDOS attack, network protection system, StormWall, Usergate, Континент 4 NGFW, Diamond VPN/FW, VipNet xFirewall 5, Ideco NGFW, DDoS-Guard, Qrator, Rostelecom DDoS Protection, Kaspersky DDoS Prevention.

This article analyzes possible DDoS attacks, as well as analyzes the effectiveness of using various solutions to prevent the impact of DDoS attacks on the network infrastructure of the campaign.

### **Введение.**

В настоящее время внедрение системы защиты от DDoS-атак стало неотъемлемой составляющей информационной безопасности компаний. С развитием информационных технологий и увеличением объемов передаваемой по сети информации, DDoS-атаки стали все более частыми и мощными. Они причиняют значительные проблемы, приводя к простоям в работе сетей, потере данных и финансов.

По проведенному кампанией StormWall исследованию, выяснилось, что количество DDoS-атак на отечественные компании во 2 квартале 2023 года возросло на 28% относительно 2 квартала 2022 года. Наиболее всего пострадали: государственный сектор, телекоммуникационная и финансовая сферы. Самым часто используемым для атаки протоколом являлись протоколы прикладного уровня HTTP/HTTPS, а следующими по популярности протоколами были TCP/UDP.

Поэтому важно найти эффективно работающее средство для защиты от данного типа атак.

### **Принцип воздействия на сеть DDoS.**

В целом DDoS атаки принято делить на 3 типа, а именно:

- атаки по модели OSI;
- атаки по используемым протоколам;
- атаки по механизму воздействия.

Первый тип подразделяется на низкоуровневые и высокоуровневые атаки. Под низкоуровневыми атаками подразумевают атаки, происходящие на 2, 3 и 4 уровнях модели OSI (канальный, сетевой и транспортный). Высокоуровневые атаки осуществляются на 5, 6 и 7 уровнях (сеансовом, представительском и прикладном).

Рассмотрим примеры низкоуровневых атак. На канальном уровне считается самой распространенной атакой – MAC-Flood, которая нагружает коммутаторы пакетами данных и выводит из строя порта соединения. На сетевом довольно частый ICMP-Flood, который снижает пропускную способность сети и ограничивает число обрабатываемых запросов.

Высокоуровневые атаки обладают куда больше разрушительным потенциалом, в отличие от низкоуровневых. На сеансовом становится возможным использовать уязвимости протокола удаленного доступа Telnet. На уровне представления для злоумышленника открывается возможность устроить SSL-Flood, путем генерации искаженных SSL-запросов. На прикладном уровне возможен HTTP(-S)-Flood. HTTP(-S)-Flood возникает путем формирования множества запросов по данному протоколу, которые

---

могут включать в себя различных данных, таких как: текст, фото, видео, форм отправки логина и пароля, файлов и других.

Во втором типе атак по частоте использования выделяют следующие протоколы: UDP, TCP, ICMP и другие. Рассмотрим примеры атак. IP NULL атака заключается в присвоении полю «Protocol» значение равное нулю, что позволяет пересылать пакеты в большом количестве. SYN-Flood атака использует тройное рукопожатие TCP, позволяя отправить множество запросов на соединение с сервером с поддельным IP-адресом источника и тем самым забивает память таблицы соединений. Атака UDP-Flood заключается в отправке «жертве» множества фальсифицированных UDP-запросов. Ping of Death использует протокол ICMP для отправки множества неправильно сформированных пакетов к узлам, тем самым перегружая их. Атака Slowloris устанавливает TCP-соединение между 2 узлами («жертвой» и атакующим ботом) и удерживают сессию открытой, путем отсутствия ответа ACK-пакетом до срабатывания Session Time Out.

Третий тип условно подразделяется на:

- Flood-Атаки (DNS Amplification, UDP-Flood, ICMP-Flood, UDP-Flood и др.);
- атака с использованием уязвимостей сетевых протоколов (ACK, RST, FIN-Flood, атака поддельными сессиями и др.);
- атака на уровень приложений (HTTP(-S)-Flood, SQL-Injection и др.).

Как можно заметить, варианты атаки «отказ в обслуживании» разнообразны, что подтверждает важность изучения способов защиты от них.

#### **Анализ решений для защиты от DDoS.**

Существует 3 пути решения проблем, связанных с атакой «отказ в обслуживании», это: составление договора об оказании услуг сервисом по защите от DDoS-атак (облачное решение), внедрение в локальную корпоративную сеть программных и программно-аппаратных средств защиты и гибридный. Стоит упомянуть, что решения рассматриваются исключительно ориентируясь на рынок отечественных производителей товаров и услуг. Проанализируем решения по порядку.

Далеко не в каждой локальных сетях используются программные и (или) программно-аппаратные средства по защите от атаки «отказ в обслуживании». Это может быть связано с неосознанностью или недостатком информации о возможных угрозах, недостаточными ресурсами или просто отсутствием приоритета на обеспечение безопасности. Однако, без использования средств защиты от DDoS-атак, локальные сети могут стать легкой мишенью для злоумышленников. С этой целью, опираясь на бюджет и вероятность возможных угроз, разворачивают решения, позволяющие обнаруживать и предотвращать атаки.

Защитить локальную сеть от воздействия атаки можно следующим образом: фильтровать трафик с помощью Firewall, установить ограничения на количество одновременных соединений с сервером, мониторить сеть административными инструментами и подключить услугу CDN. Не лишним будет интегрирование в функционал сети облачного сервиса, но об этом далее.

В случае разворачивания сервера, необходимо отказаться от ОС Windows Server 2008, 2016 из-за особенностей сетевого стека, а также, в случае если сервер разворачивается на ОС Linux, то нужно отказаться от Apache и отдать предпочтение Nginx, ввиду ряда уязвимостей Apache.

Таблица 1. Программно-аппаратные средства защиты. Firewall NGFW.

Наименование	Usergate	Континент 4 NGFW	Diamond VPN/FW	VipNet xFirewall 5	Ideco NGFW
Целевой сегмент	Гос. сектор, малый и средний бизнес	Гос. сектор, средний и крупный бизнес	Малый и средний бизнес	Гос. сектор, средний и крупный бизнес	Средний и крупный бизнес
Сертификация	ФСТЭК	ФСТЭК, Минцифры, ЕАЭС	ФСТЭК	ФСТЭК	ФСТЭК
VPN / SSL VPN Client	+ / +	+ / +	+ / +	+ / +	+ / +
Поддержка алгоритмов ГОСТов	Не поддерживает	ГОСТ 28147-89	ГОСТ 28147-89, 34.13-2015 34.10-2012 34.11-2012	ГОСТ 28147-89 только в VipNet Coordinator	Не поддерживает
Антивирусная проверка трафика	+	-	-	+	-
Защита зон от DDoS-атак / настройка исключений	Для протоколов TCP, UDP, ICMP / +	+ / +	Защита работает через IPS / +	+ / +	+ / +
Инспект. SSL-трафика	+	+	-	+	+
Обновление сигнатур	Автоматическое обновление	+	+	+	+
Переключение режимов IPS/IDS	+	+	+	+	-

В таблице 1 приведен перечень программно-аппаратных средств защиты, а именно Firewall нового поколения, сочетающий в себе IPS/IDS – NGFW (Next Gen FireWall). Внедрение в локальную сеть Firewall перед граничным маршрутизатором позволит эффективно фильтровать входящий трафик, а также проверять на наличие подозрительных сигнатур (чем занимается модуль IPS) не нагружая маршрутизатор. Установка стандартного Firewall после граничного маршрутизатора позволит защититься от атак внутри сети и, при использовании DMZ (демилитаризованной зоны), стать барьером между DMZ и внутренней сетью (см. рис. 1).

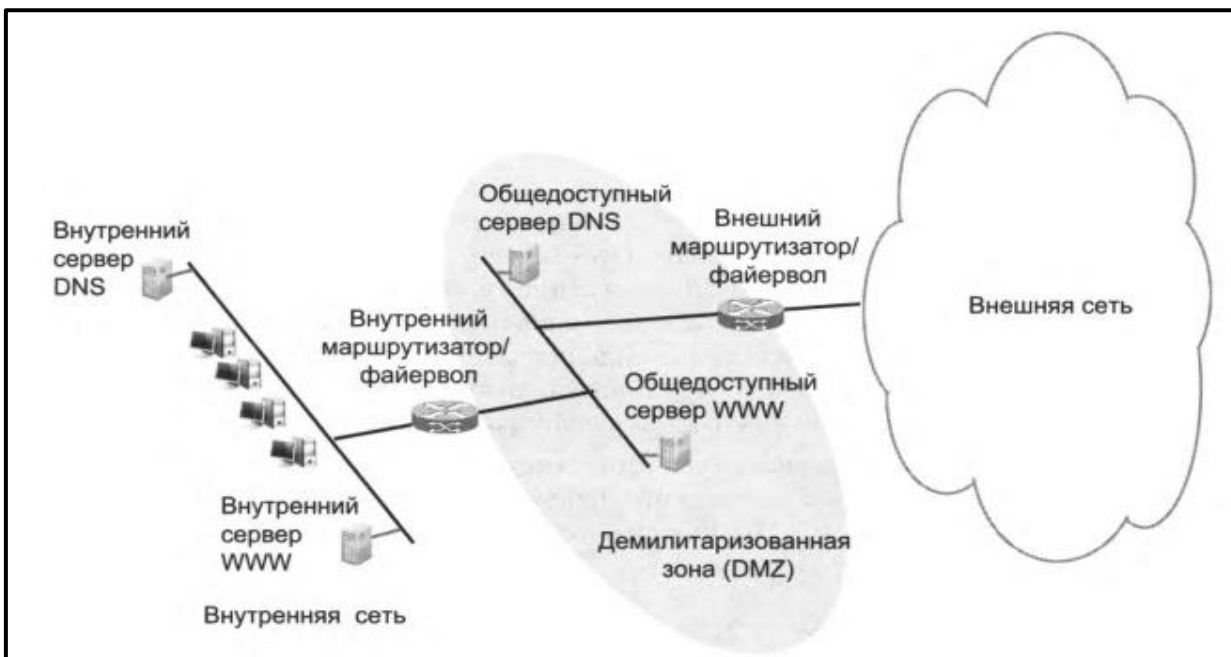


Рисунок 1. DMZ

В зависимости от потребностей заказчика составляется ТЗ и по нему подбирается оборудование с необходимыми модернизациями и (или) дополнениями. Так для государственного сектора предпочитают продукты компаний «Код Безопасности» и «Инфотекс», а для коммерческих организаций – в зависимости от масштаба локальной корпоративной сети (один офис или множество офисов, разнесенных по различным локациям).

Скорость обработки данных и максимальная пропускная способность зависят от комплектации выбранного устройства.

Сервисы по защите от DDoS-атак предназначены для гибкой интеграции в функционал корпоративной сети компании. В среднем, время подключения услуг обходится до 30 минут без учета обновления DNS-списка. Данный тип борьбы с DDoS является полноценным решением для малого и среднего бизнеса, но бывает недостаточен для больших инфраструктур. Принцип работы сервисов заключается в том, чтобы перенести DNS-запись вашего сайта на выданный компанией-исполнителем услуг защищенный адрес. Связь клиента с исполнителем реализуется путем создания GRE/IPIP (функционал как у GRE, но работает только с IPv4)/MPLS -туннелирования и для обеспечения защищенности используется протокол IPsec, работающий поверх GRE/IPIP/MPLS.

В таблице 2 продемонстрированы основные параметры, исходя из которых стоит предпочесть тот или иной облачный сервис. Стоит упомянуть, что недавно на рынке услуг зарегистрировалась компания Servicepipe, однако ввиду отсутствия информации, она не попала в данную таблицу, но в будущем, возможно, стоит обратить внимание в ее сторону. Бывают ситуации, когда использования сервисов недостаточно и необходимо построить гибридную защиту.



Таблица 2. Сравнение облачных сервисов по защите от DDoS-атаки.

Наименование сервиса	DDoS-Guard	StormWall	Qrator	Rostelecom DDoS Protection	Kaspersky DDoS Prevention
Целевой сегмент	Любой сегмент, гос. сектор	Любой сегмент	Средний и крупный бизнес	Любой сегмент	Средний и крупный бизнес, гос. сектор
Лицензии ФСБ / ФСТЭК / РКН	+ / + / +	+ / + / +	+ / - / +	+ / + / +	+ / + / -
Сроки подключения защиты сайта / сети	15 минут / 60 минут	10 минут / 60-120 минут	15 минут / 60 минут	30 минут / 30 минут	1 сутки
Время реакции на DDoS-атаку	До 5 минут	1-2 секунды для L4, 1 минута для L5-7, в ручном – до 15 минут.	До 4 секунд для атак L2-4, 180 секунд для L5-7	До 1 минуты в автомат. режиме, до 15 минут в ручном режиме	Немедленно для Always on, до 15 минут на Demand.
Защита от ботов	-	+	+	+	+
Выбор режимов постановки на защиту	On demand, Always on.	Disabled, Sensor, Always on.	On demand, Always on.	On demand	On Demand, Always on.
Максимальная мощность отражения атак	1500 Гбит/с	3500 Гбит/с	5000 Гбит/с	5000 Гбит/с	500 Гбит/с
Фильтрация HTTPS без раскрытия ключа / с раскрытием ключа	+ / +	Только на сетевом уровне / +	+ / +	+ / +	+ / +
Коридор гарантируемой доступности	95-99,99%	98-99,9%	97-99,99%	99,5%	98-99,5%
Фильтрация без внесения изменений в работу страниц сайта	+	+	+	+	+

Большинство коммерческих компаний, таких как: ООО «АВИТО», ООО «Tilda Publishing», АО «Raiffeisen», АО «Тинькофф», «Хакер» предпочитают использовать сервис Qrator, который доказал наибольшую эффективность по сравнению с аналогами, однако это не означает, что другие сервисы плохи. По соотношению цена/качество следующими выступают StormWall и DDoS-Guard. В отличие от Qrator они не такие дорогие в оказании услуг по фильтрации трафика. Ими пользуются «РАНХиГС», ООО «Ozon», ПАО «Банк Уралсиб» и другие. Выбор того или иного сервиса зависит от важности организации мероприятий по защите от DDoS.

Под гибридной защитой подразумевается комплекс мер, состоящей из программно-аппаратных средств компании и облачных средств защиты (фильтрации) траффика. Таким образом, сюда входят всевозможные комбинации вышеперечисленных средств фильтрации траффика, совокупность которых определяется спецификой компании (организации). Гибридный способ защиты позволяет производить фильтрацию на всевозможных уровнях модели OSI (L2-L7). Данный подход используют крупные компании, деятельность которых связана с финансовым оборотом (банки, страховые), телекоммуникациями (интернет-провайдер) и др.

---

### **Заключение.**

Кибератаки происходят ежедневно, поэтому спрос на оборудование и оказание услуг по защите корпоративных сетей растут прогрессивно. И даже после ухода иностранных производителей товаров и услуг в IT-сфере, отечественный рынок оказался более чем готов к подобным переменам. Российские компании постоянно совершенствуют свои решения, тем самым составляя конкуренцию иностранным компаниям.

Внедрение программно-аппаратных изделий не всегда будет работать эффективно, потому как в ЦОД облачных сервисов приходит больше информации для анализа на вредоносный трафик и, соответственно, они будут знать о новой возникшей угрозе раньше. Однако с точки зрения безопасности корпоративных сетей и обрабатываемых данных в государственных структурах, подключение к такому ЦОД может означать потенциального «прослушивателя» каналов связи, что не является хорошим решением.

Стоит отметить, что идеального и единственно правильного решения касемо защиты не существует и все следует выбирать в соответствии со спецификой инфраструктуры сети и деятельности в ее пределах.

### **СПИСОК ЛИТЕРАТУРЫ**

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – Спб.: Питер, 2020. – 672с.
2. Государственный реестр сертифицированных средств защиты информации. [Электронный ресурс]: URL: <https://reestr.fstec.ru/reg3> (Дата обращения: 7.10.2023 г.)
3. DDoS HANDBOOK. [Электронный ресурс]: URL: [http://cstor.com/wp-content/uploads/2016/10/Radware\\_DDoS-Handbook\\_eBook.pdf](http://cstor.com/wp-content/uploads/2016/10/Radware_DDoS-Handbook_eBook.pdf) (Дата обращения 6.10.2023 г.)
4. Сравнительный анализ эффективности существующих методов защиты сетей связи от DDoS-атак. [Электронный ресурс]: URL: [https://www.researchgate.net/publication/344735525\\_Comparative\\_analysis\\_of\\_the\\_effectiveness\\_of\\_existing\\_methods\\_of\\_networks\\_security\\_from\\_DDoS\\_attacks](https://www.researchgate.net/publication/344735525_Comparative_analysis_of_the_effectiveness_of_existing_methods_of_networks_security_from_DDoS_attacks) (Дата обращения: 7.10.2023 г.)
5. Effective DDoS Mitigation in Distributed Peering Environments. [Электронный ресурс]: URL: <https://www.netscout.com/sites/default/files/2019-01/Effective-DDoS-Mitigation-in-Distributed.pdf> (Дата обращения 9.10.2023 г.)
6. Отчеты от DDoS-атаках. [Электронный ресурс]: URL: <https://stormwall.pro/blog/analytics> (Дата обращения: 5.10.2023 г.)
7. Классификация DDoS: полное руководство по типам атак. [Электронный ресурс]: URL: <https://ddos-guard.net/ru/blog/classification-of-ddos-attacks> (Дата обращения: 5.10.2023 г.)

## МЕТОДЫ ЗАЩИТЫ ОТ КЛИКДЖЕКИНГА

Донской государственной технической университет (ДГТУ), г. Ростов-на-Дону

Ключевые слова: информационные технологии, информационная безопасность, социальная инженерия.

В данной статье рассмотрены разновидности кликджекинга, его механизм действия, а также предлагаются методы защиты от данного вида атак. Также, представлены существующие средства и технологии, которые помогают выявить кликджекинг и предотвратить его негативное воздействие на пользователей. Статья представляет практическую и теоретическую ценность для исследователей в области кибербезопасности и веб-разработки, а также для специалистов, ответственных за защиту интернет-ресурсов от вредоносных атак.

D.I. Lyan, A.V. Kornilova, O.V. Kulikova

## METHODS OF PROTECTION AGAINST CLICKJACKING

Don State Technical University (DSTU), Rostov-on-Don.

Keywords: information technology, information security, social engineering.

This article discusses the types of clickjacking, its mechanism of action, and also offers methods of protection against this type of attacks. Also, the existing tools and technologies that help to identify clickjacking and prevent its negative impact on users are presented. The article is of practical and theoretical value for researchers in the field of cybersecurity and web development, as well as for specialists responsible for protecting Internet resources from malicious attacks.

Кликджекинг (clickjacking) — это вид атаки в компьютерной безопасности, при которой злоумышленник посредством фальшивого интерфейса заманивает пользователя совершить определенные действия, которые могут привести к опасным последствиям. Например, злоумышленник может скрыть невидимую кнопку под смещенной или прозрачной областью другой страницы, чтобы заставить пользователя случайно щелкнуть на нее, что может привести к выполнению нежелательных действий, таких как совершение покупок, подтверждение подписки или разрешение на доступ к конфиденциальной информации. Помимо классической подмены iframe существует и другие виды атак с использованием кликджекинга:

- лайкджекинг – это атака на основе кликджекинга, которая обманом заставляет своих жертв ставить лайки в социальных сетях;
- куккиджекинг – это атака, с помощью которой злоумышленник изменяет UI для взлома, то есть кражи, файла cookie пользователя в браузере. Для обмана используется метод перетаскивания. Как только посетитель совершает нужное мошеннику действие, тот в дальнейшем может выдавать посещения ботов за человека, используя похищенные куки-файлы;
- курсорджекинг – атака с изменением местоположения курсора. В этом случае, когда посетитель наводит курсор на один элемент сайта и нажимает на него, то на самом деле клик происходит по элементу, расположенному в другом месте;
- файлджекинг – данный метод атаки использует сайты с возможностью доступа к файловой системе устройства пользователя. Вредоносный код внедряется в

---

кнопку загрузки файлов, после нажатия пользователем, злоумышленник получает доступ к файлам.

Для предотвращения манипуляций злоумышленника над пользователем, разработаны методы защиты от рассмотренных ранее веб-атак.

Использование заголовка X-Frame-Options поможет контролировать отображение страницы внутри фрейма. На рисунке 1 показано практическое использование данного метода защиты со значением sameorigin, данный атрибут сообщает браузеру, что никто кроме страниц одного и того же веб – сайта не могут включать эту страницу в iframe.

```
app.use(function(req, res, next) {  
  res.setHeader('X-Frame-Options', 'sameorigin');  
  next();  
});
```

Рисунок 1. Использование заголовка X-Frame-Options

Помимо sameorigin у X-Frame-Options имеется альтернативное значение – deny, что предотвращает любую попытку поместить страницу во фрейм.

Использование заголовка X-Frame-Options никогда не был стандартизирован, из – за чего существуют браузеры, которые не поддерживают его. Однако есть метод, который является его альтернативой, а именно CSP (Content Security Police). Это механизм, обеспечивающий безопасность, с помощью которого имеется возможность описать безопасные источники загрузки ресурсов, установить определенные правила использования для CSS (встроенных стилей), скриптов, а также динамической оценки JS (JavaScript).

На рисунке 2 представлено практическое применение CSP, где задано значение frame-ancestors 'self' – она предназначена для каждого исходящего ответа. Возможности и результат этой директивы аналогичны заголовку X-Frame-Options со значением sameorigin.

```
app.use(function(req, res, next) {  
  res.setHeader("Content-Security-Policy", "frame-ancestors 'self'");  
  next();  
});
```

Рисунок 2. Использование CSP

Помимо значения self, frame-ancestors имеет:

frame-ancestors 'none'; : предотвращение любой попытки включить страницу во фрейм;

frame-ancestors 'https://www.aaa.ru'; : директива позволяющая указать определенный веб – сайт, которому разрешено встраивать страницу во фрейм.

Использование cookie sameSite origin. Установление атрибута на Strict. Samesite – атрибут cookie, который может помочь избежать кликджекинг-атаки. Если samesite = Strict, то cookie-файл будет отправлен на сайт только в том случае, если он открыт напрямую, не через фрейм или каким-либо другим способом. На рисунке 3 представлено использование данного метода. Этот метод защиты эффективен только в том случае, если вы используете cookie для авторизации пользователей.

```
cookie: {  
  httpOnly: true,  
  sameSite: 'strict'  
}
```

Рисунок 3. Использование cookie sameSite

---

Методы защиты от рассмотренного вида атак являются актуальными и по сей день, т.к. кликджекинг один из самых распространенных видов мошенничества в интернете. В целом, продолжающиеся угрозы кликджекинга заставляют организации и пользователей принимать меры по защите от него. Комбинация разных методов защиты поможет снизить возможность попадания в ловушку кликджекинга и повысить общую безопасность в Интернете.

#### СПИСОК ЛИТЕРАТУРЫ

1. Бирн Деннис Безопасность веб-приложений на Python / Бирн Деннис — 1-е изд. — Москва: ДМК-Пресс, 2023 — 334 с.
2. Гладкий А.В., Горбунова И.Я. Признаки и методы обнаружения кликджекинга веб-ресурсов. Современные информационные технологии и ИТ-образование, 2018, т. 14, № 2, с. 348-352.
3. Тарасов А.С., Каримов М.А., Шалагинова Е.В. Анализ методов кликджекинга и способы их предотвращения. Вестник Кемеровского государственного университета, 2017, № 4(65), с. 194-200.
4. Тихомиров Н.В., Капустина О.М. Проблемы кликджекинга и методы их предотвращения. Вестник Московского городского психолого-социального института, 2020, т. 23, № 1, с. 126-133.
5. Шишкова С.В. Методы обнаружения и предотвращения кликджекинга на веб-ресурсах. Технологии информационного общества, 2019, № 1(29), с. 48-55.
6. Осокин К.А., Олейников Д.А. Методы построения систем защиты от кликджекинга в интернет-рекламе. Системы управления и информационные технологии, 2018, т. 62, № 1, с. 63-71.

**А.С. Никитин<sup>1</sup>, И.А. Трухлов<sup>2</sup>, Т.А. Наговицын<sup>3</sup>**

#### **МОДЕЛИРОВАНИЕ КИБЕРАТАК НА БАЗЕ ВИРТУАЛЬНОЙ ПЛАТФОРМЫ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Институт математики, механики и компьютерных наук им. И.И. Воровича ЮФУ,  
Ростов-на-Дону, Россия<sup>2</sup>  
АО Альфа Банк, Москва, Россия<sup>3</sup>

**Ключевые слова:** информационная безопасность, моделирование атак, информационное общество, киберполигон.

Статья посвящена актуальной теме моделирования атак в области информационной безопасности. Рассмотрены основные преимущества киберполигонов и простейший пример их использования. Моделирование кибератак становится ключевым инструментом для обучения, тренировок и тестирования систем безопасности, а также для разработки инновационных решений в области информационной безопасности.

## SIMULATION OF CYBER ATTACKS BASED ON A VIRTUAL PLATFORM

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Institute of Mathematics, Mechanics and Computer Sciences named after I.I. Vorovich Southern  
Federal University, Rostov-on-Don, Russia<sup>2</sup>  
JSC Alfa Bank, Moscow, Russia<sup>3</sup>

Keywords: information security, attack modeling, information society, cyber testing ground.

The article is devoted to the current topic of modeling attacks in the field of information security. The main advantages of cyber ranges and the simplest example of their use are considered. Cyber attack simulation is becoming a key tool for teaching, training and testing security systems, as well as for developing innovative information security solutions.

В связи с приобретением киберугроз все более сложного характера, определяемого динамичностью и трудностью предсказания и предотвращения, актуальность моделирования кибератак непрерывно растет [1]. Данное направление ставит перед собой задачу создания абстрактных представлений о сценариях проведения атак и о том, какие уязвимости они могут эксплуатировать.

Среди некоторых ключевых аспектов, подчеркивающих необходимость моделирования кибератак можно выделить следующие:

- возможность анализа и классификации различных видов атак и их потенциальных последствий;
- оценка рисков и их влияния на организацию, что позволяет принимать меры предосторожности и разрабатывать стратегии предупреждения атак;
- проведение тестирования и проверки системы безопасности, помогающей в выявлении уязвимостей и модернизации мер защиты;
- возможность анализировать различные сценарии и разрабатывать навыки реагирования на киберугрозы;
- стимуляция разработки новых технологий и инновационных решений в области кибербезопасности, ведущая к созданию более эффективных и устойчивых систем защиты.

Кибератаки могут варьироваться от простых до чрезвычайно сложных. Они могут использовать множество методов, включая вирусы, фишинг, DDoS-атаки, атаки на приложения и многое другое.

Приведем наиболее популярные типы кибератак и их модификации.

### **1. DDoS-атаки и их вариации.**

Сетевые атаки: классические DDoS-атаки, где злоумышленники перегружают цель трафиком. Также могут применяться атаки на уровне протоколов, такие как SYN-флуды или амплификацию DNS-запросов, чтобы усилить свой эффект.

DNS-атаки: злоумышленники могут атаковать DNS-серверы, подвергая риску доступ к веб-сайтам и услугам, и таким образом нарушая работу сети.

### **2. Фишинг и социальная инженерия.**

Спиро-фишинг: модификация фишинга, ориентированная на жертвы с высоким статусом. Злоумышленники используют персональные данные и создают поддельные письма, чтобы убедить жертву в своей достоверности.

---

Бизнес-фишинг: злоумышленники маскируются под высокоорганизованные бизнес-сущности, чтобы украсть корпоративные данные или финансовую информацию.

### **3. Вредоносные программы и эксплойты.**

Шифровальщики: современные шифровальщики часто используют шифрование, чтобы заблокировать доступ к данным, и требуют выкуп для их разблокировки.

Уязвимости приложений: эксплойты уязвимостей в популярных приложениях, таких как браузеры или операционные системы, продолжают быть важным инструментом для злоумышленников.

### **4. Сетевые атаки и внедрение в системы.**

Внедрение в системы интернета вещей (IoT): злоумышленники могут использовать уязвимости в устройствах IoT для создания ботнетов или атак на корпоративные сети.

Атаки на облачные ресурсы: проникновение в облачные среды, используя украденные учетные данные или уязвимости, чтобы получить доступ к данным и инфраструктуре.

### **5. Социальные атаки и кибершпионаж.**

Атаки на социальные медиа: использование фейковых профилей и манипуляции с информацией на платформах социальных медиа для распространения дезинформации и манипуляции общественным мнением.

Кибершпионаж и атаки на правительства: государственные акторы могут совершать сложные кибератаки для сбора разведывательной информации или даже дестабилизации других стран.

Все эти типы атак, а также многие другие могут моделироваться на киберполигонах. Сейчас почти у каждой крупной ИБ-компании есть свой киберполигон, на котором происходят как тренировки сотрудников, так и научные изыскания в сфере информационной безопасности. Известные киберполигоны так или иначе отличаются друг от друга и имеют свои преимущества и недостатки. Однако каждый из них приносит свою пользу в общее дело информационной безопасности, с каждым днём улучшая безопасность в сети.

Понятие «киберполигон» в контексте кибербезопасности относится к специально созданной инфраструктуре или площадке, предназначенной для проведения учений, тренировок и тестирования в области киберзащиты и кибератак. Киберполигоны создаются с целью симуляции реальных ситуаций и атак, позволяя специалистам и организациям тренироваться и развивать навыки в сфере кибербезопасности.

Функциональность киберполигона включает:

- тестирование защиты;
- обучение и тренировки;
- моделирование атак;
- сотрудничество и обмен знаниями;
- инновации и исследования.

Разные платформы имеют разную структуру и используют различные конфигурации устройств. В данной работе предлагается проект виртуальной платформы, реализующей самую простую структуру – два устройства (первое – это устройство злоумышленника, а второе – жертвы) подключённые к общей точке доступа (рис. 1). Данная структура дает возможность максимально просто реализовать главные функции платформы – моделирование и обучение.

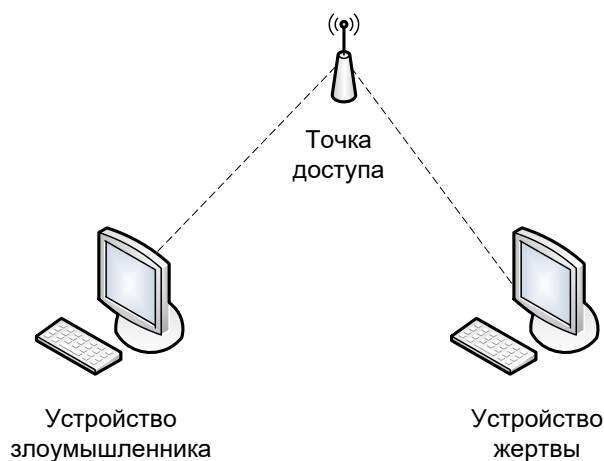


Рисунок 1. Структура экспериментальной платформы.

Конфигурации виртуальных машин представляют собой две возможные схемы:

1. Одно устройство, используемое злоумышленником, с дистрибутивом Kali Linux и средой для проведения атак. Второе устройство, используемое жертвой, с операционной системой Windows и средствами защиты и обнаружения.
2. Одно устройство, используемое злоумышленником, с дистрибутивом Kali Linux и средой для проведения атак. Второе устройство (жертва) имитирует работу сервера.

Экспериментальную проверку предложенного решения проведем на примере моделирования MITM-атаки (атаки «человек посередине») с использованием ARP-спуфинга [2]. Для наглядности будем использовать самодельные скрипты.

Суть моделируемой MITM-атаки состоит в том, чтобы подменить посылаемые пакеты данных так, чтобы точка доступа передавала машине злоумышленника данные запрашиваемые жертвой из сети. В то время как жертва будет отправлять данные злоумышленнику, полагая, что его машина – это точка доступа.

По сути все, что нужно сделать злоумышленнику – это отправлять точке доступа ARP-пакеты с адреса жертвы, а жертве ARP-пакеты с адреса точки доступа, что и называется ARP-спуфингом. После данных действий разрешить использование своего устройства, в виде пропускного пункта, а дальше просто читать и/или изменять проходящие через него пакеты.

Перед проведением атаки злоумышленник выполняет сканирование сети и поиск целевых устройств – точки доступа и машины на Windows (рис. 2).

```

└─# python3 net_scan.py -i 10.0.2.1/24
IP      |          MAC address
-----|-----
10.0.2.1      52:54:00:12:35:00
10.0.2.2      52:54:00:12:35:00
10.0.2.3      08:00:27:8f:37:52
10.0.2.15     08:00:27:42:5b:54
  
```

Рисунок 2. Сканирование сети.



В данном случае целью является машина с адресом 10.0.2.15, а так же точка доступа с адресом 10.0.2.1. На примере этого скрипта можно видеть, что злоумышленник осуществляет сканирование с помощью широковещательного запроса по маске сети 10.0.2.1/24. В данном случае посылаются запросы на все устройства с адресом, начинающимся на 10.0.2.X, где вместо X подставляются значения от 1 до 255. Ответом на запрос является возвращённый IP- и MAC-адрес устройства, которые выводятся в таблицу.

При помощи полученных сведений проводится сама атака. Для этого запускается скрипт, который будет создавать и автоматически отправлять пакеты с нужными данными. В данном случае, в атрибутах запуска скрипта указываются адреса жертвы и точки доступа. После этого скрипт автоматически составит ARP-пакет и отправит его, буквально поместив устройство между двумя другими (рис. 3).

```
python3 arp_spoof.py -t 10.0.2.15 -g 10.0.2.1
total packet send 50.
```

Рисунок 3. ARP-спуфинг.

В данном случае атрибуты -t и -g означают target\_ip и gateway\_ip, соответственно. Выполнение скрипта можно отследить по количеству отсылаемых пакетов. Если пакеты отсылаются и скрипт не выдаёт никаких ошибок, то вывод в терминале будет такой же, как и на рис. 3. После того, как успешно использован ARP-спуфер, то начинается дальнейшая эксплуатация этой уязвимости. Если сейчас на машине жертвы посмотреть настройки сети, то можно заметить, что MAC-адрес точки доступа будет отличаться от изначального, т.к. он изменен на MAC-адрес устройства злоумышленника. Последующие действия по эксплуатации уязвимости выходят за рамки статьи ввиду их огромного разнообразия, поэтому не будут реализованы.

Целью данной работы было показать возможность построения платформы для моделирования различных атак в виртуальном пространстве по типу киберполигона, не подвергая опасности системы, используемые для отличных от тестирования целей. Промоделированная простейшая атака представляет собой лишь малую долю того, что представляют киберполигоны и иные платформы для моделирования инцидентов информационной безопасности. Последующее развитие этой идеи может помочь выявлять слабые места моделируемых систем, а также заинтересовать тех, кто хочет развиваться в информационной безопасности.

## СПИСОК ЛИТЕРАТУРЫ

1. Лаврова Д.С., Зегжда Д.П., Зайцева Е.А. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. – 2019. – № 2(30). – С. 13-20.
2. Бирюков А.А. Информационная безопасность: защита и нападение: практическое руководство. – Москва: ДМК Пресс, 2017. – 434 с.

## НЕКОТОРЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЛУЧАЕ ИСПОЛЬЗОВАНИЯ ОНЛАЙН-БАНКА

Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения», Екатеринбург, Россия

Ключевые слова: информационная безопасность, угроза информационной безопасности, компьютерный вирус, онлайн-банкинг, интернет-мошенничество

В статье рассматриваются угрозы информационной безопасности при несанкционированном доступе к онлайн-банку. Анализируются возможные источники угроз и негативные последствия при несанкционированном доступе к онлайн-банку. Приводятся меры информационной безопасности при использовании онлайн-банкинга.

K.N. Gural'sky, S.V. Mukhachev

## SOME THREATS TO INFORMATION SECURITY IN THE CASE OF USING AN ONLINE BANK

Ural State University of Railway Transport, Ekaterinburg, Russia

Keywords: information security, threat to information security, computer virus, online banking, Internet fraud

The article discusses threats to information security in case of unauthorized access to online banking. Possible sources of threats and negative consequences of unauthorized access to online banking are analyzed. Information security measures are provided when using online banking.

Онлайн-банкинг – сервис любого современного банка [1,2]. Он представляет собой один из видов дистанционного обслуживания клиентов. Посредством онлайн-банкинга клиент получает возможность управлять своими счетами, пользоваться услугами кредитного учреждения без необходимости личного посещения офиса банка.

Данный вид обслуживания появился относительно недавно, около двадцати лет назад. За это время технология онлайн-банкинга, вместе с техническим и программным развитием, усовершенствовалась и получила широкое распространение.

Распространению этой технологии способствовало широкое применение для онлайн-банкинга смартфонов. Смартфон является неотъемлемым инструментом для любого современного человека. Сегодня это не просто средство связи. Он используется как хранилище важной информации, а также позволяет работать с большим набором полезных сервисов.

Однако, наряду с несомненными удобствами и распространенностью, с онлайн-банкингом связаны многочисленные и серьезные угрозы информационной безопасности в случае получения незаконного доступа к сервису злоумышленником. Для этого используются различные способы [3,4].

Статистика инцидентов информационной безопасности, связанных с незаконным доступом к онлайн-банку, неутешительна [5]. Количество операций с электронными счетами без согласия клиентов исчисляется цифрой около 13 тыс. с общим объемом более миллиарда рублей за квартал. Только в первом квартале 2023 г. регулятор инициировал блокировку почти 97 тыс. телефонных номеров, которые использовались

---

злоумышленниками для звонков гражданам с целью незаконного получения доступа к денежным средствам.

Активность преступников с использованием сети Интернет в 2003 г. по сравнению с аналогичным периодом 2022 г. возросла более чем в 2,5 раза.

Доступ к онлайн-банку злоумышленник может получить различными способами. Остановимся подробнее на наиболее распространенных.

### **1. Фишинг.**

Фишинг представляет собой вид кибермошенничества, когда злоумышленник использует ложные или поддельные сайты, письма, страницы для обмана пользователей с целью получения личных данных, финансовых сведений и паролей.

Часто фишинговые атаки организуются злоумышленниками в социальных сетях и мессенджерах: Одноклассники, ВКонтакте, Telegram или WhatsApp. Пользователей под тем или иным предлогом просят перейти по ссылке на фишинговый сайт и ввести свои данные.

Масштаб этого явления таков, что только в первом квартале 2023 г. Центробанк России инициировал блокировку более 8 тыс. фишинговых сайтов. Они были замаскированы под официальные сайты финансовых организаций: кредитных, страховых, участников рынка ценных бумаг, а также организаций, предлагающих сверхдоходные инвестиционные продукты.

### **2. Вредоносные программы.**

Использование вредоносных программ – еще один распространенный способ кражи учетных данных и получения доступа к онлайн-банку жертвы.

По статистике, существенную часть активных вредоносных программ составляют трояны-стиллеры. Они предназначены для кражи сохраненных в браузерах логинов и паролей, файлов cookie, реквизитов банковских карт и криптовалютных кошельков.

Для выполнения вредоносных функций такие программы исследуют файлы, записывают действия пользователя, снимают скриншоты с рабочего стола зараженного устройства. Попав на устройство жертвы, троянская программа ждет, когда пользователь зайдет на какой-нибудь сайт или сервис и копирует введенные для аутентификации данные. Полученную информацию стиллер отправляет своему «хозяину». Такие программы могут долгое время скрываться в устройстве.

Наиболее опасны специализированные банковские троянцы – вредоносные программы, которые используются для кражи банковских учетных данных путем удаленной установки вредоносного программного обеспечения в компьютерную систему жертвы. Они адаптированы к определенным типам устройств.

Во втором квартале 2023 г. количество установочных пакетов банковских троянцев оценивалось цифрой, превышающей 59 тыс. [6].

### **3. Утечка данных из сервисов.**

За 2022 г. в России количество утекших записей персональных данных и платежной информации выросло в 2,67 раза по сравнению с предыдущим годом и составило более 667 млн единиц [6].

В 2022 г. произошли крупные утечки личных данных.

Произошла утечка сведений о пользователях «Яндекс.Еды». Они были представлены в виде карты, на которой указаны адреса доставки, телефоны, электронная почта, сумма заказа. Сведения приводились за полгода.

Об утечке данных также сообщал сервис доставки еды Delivery Club. Личные данные включали: фамилию, имя, отчество, адреса и информацию о заказах.

Стало известно об утечках СДЭК.

---

Сервис проката электросамокатов Whoosh также не избежал утечки: в доступе оказалось около 7,3 млн записей, в том числе имена пользователей, номера телефонов, адреса электронной почты и часть данных банковских карт.

#### **4. Утрата смартфона.**

Пожалуй, наиболее опасен именно этот случай, т.к. в руках злоумышленника оказывается устройство, обычно используемое для работы с сервисами онлайн-банкинга.

Получив доступ к приложению банка, злоумышленнику открывается возможность управления счетами. Также, с получением доступа к телефону, злоумышленник получает доступ к сим-карте. Даже если он не сможет разблокировать телефон, имея данные банковской карты и сим-карту клиента банка, злоумышленник сможет получить доступ к онлайн-банку.

#### **5. Использование двойника sim-карты.**

Сим-карта широко используется для аутентификации пользователя и подтверждения операций при использовании онлайн-банка. Поэтому, имея ее дубликат, злоумышленник получает возможность распоряжения финансами жертвы.

Используются различные схемы получения двойников.

Наиболее просто изготовить сим-карту-двойник, если преступник сам работает в салоне связи. Однако это не единственная возможность. Злоумышленник может использовать утерянный паспорт: в салоне сообщить, что старая сим-карта утеряна и потребовать выдать новую с тем же номером. Мошенник может использовать поддельный паспорт, либо фальшивую доверенность. Также имеется техническая возможность клонирования сим-карт, правда, для этого злоумышленнику необходима настоящая сим-карта.

#### **6. Социальная инженерия.**

Представляет собой совокупность методик психологического воздействия на человека с целью получения определенной конфиденциальной информации или принуждения совершить определенные действия [8].

Используются различные приемы, связанные с рассылкой писем, использованием интернет-ресурсов.

Сегодня наиболее распространены звонки на средства мобильной связи и «давление» на жертву с целью получить, например код подтверждения банковской операции или заставить жертву перевести средства на счет злоумышленника.

Таким образом, за удобством использования онлайн-банкинга скрываются и существенные риски. Поэтому необходимо предусмотреть некоторые меры обеспечения информационной безопасности при использовании онлайн-банка. Это позволит уменьшить вероятность стать жертвой мошенничества.

Самые элементарные состоят в следующем.

Не следует переходить по ссылкам, полученным в письмах от неизвестных отправителей. Аккуратно и бдительно, с осторожностью относиться к ресурсам, на которых требуется ввести какие-либо данные, касающиеся доступа к финансовым средствам, либо идентифицирующие личность. В случае использования сервисов, которые подверглись компрометации, необходимо изменить пароль для доступа к ним. В случае утраты смартфона следует как можно быстрее заблокировать сим-карту. Обязательно использовать двухфакторную аутентификацию там, где она доступна, что обеспечит дополнительный уровень защиты и не позволит получить доступ к учетным записям посторонних, даже если они будут иметь логи и пароль.

Таким образом, небрежное отношение к информационной безопасности может привести к тому, что злоумышленник получит доступ к многим сервисам, в том числе к онлайн-банкингу. Такая ситуация может создать большое количество проблем,

---

порожденных угрозами, связанными с информационной безопасностью. Денежные средства, хранящиеся на банковских счетах, могут оказаться под угрозой. Злоумышленник может от имени жертвы выполнить финансово значимые операции, например взять кредит, перечислить денежные средства на подставной счет, совершить покупки за счет жертвы. Поэтому необходимо с особым вниманием относиться к безопасности использования онлайн-банкинга, соблюдать определенные правила безопасности и не пренебрегать мерами обеспечения информационной безопасности.

#### СПИСОК ЛИТЕРАТУРЫ

1. Онлайн банкинг [Электронный ресурс]. - Режим доступа: URL: <https://mytopfinance.ru/chto-takoe-internet-banking/> (дата обращения 29.09.2023).
2. Кориченков Д. А. Интернет - банкинг в России. Новые горизонты развития / Д. А. Кориченков // Плехановский барометр. – 2022. – № 1(29). – С. 93-97.
3. Безопасность при использовании онлайн-банкинга [Электронный ресурс]. - Режим доступа: URL: <https://bankstoday.net/last-articles/bezopasnost-pri-ispolzovanii-onlajn-bankinga#i> (дата обращения 29.09.2023).
4. Сидорина, Т. Н. Безопасность онлайн-банкинга / Т. Н. Сидорина // Таможенное администрирование и экономическая безопасность в цифровой экономике : материалы всероссийской научно-практической конференции, Брянск, 14–15 ноября 2019 года. – Брянск: Брянский государственный университет имени академика И.Г. Петровского, 2019. – С. 523-527.
5. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств [Электронный ресурс]. - Режим доступа: URL: [https://cbr.ru/statistics/ib/review\\_2q\\_2023/](https://cbr.ru/statistics/ib/review_2q_2023/) (дата обращения 29.09.2023).
6. Развитие информационных угроз во втором квартале 2023 года. Мобильная статистика [Электронный ресурс]. - Режим доступа: URL: <https://securelist.ru/it-threat-evolution-q2-2023-mobile-statistics/107872/> (дата обращения 29.09.2023).
7. В России за год утекло более 660 млн записей с персональными данными [Электронный ресурс]. - Режим доступа: URL:[https://www.rbc.ru/technology\\_and\\_media/17/04/2023/643936229a7947134f0ce21c?ysclid=Indevy3lvh885916600](https://www.rbc.ru/technology_and_media/17/04/2023/643936229a7947134f0ce21c?ysclid=Indevy3lvh885916600)
8. Сазонов А. И. Социальная инженерия как угроза информационной безопасности / А. И. Сазонов, И. А. Воробьева // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2020. – № 1. – С. 111-114.

**Д.В. Маршаков, Ю.Д. Кокоулина, А.А. Аболмасов, А.В. Панасюк**

#### **ОБ ИНТЕРПРЕТИРУЕМОСТИ НЕЙРОСЕТЕВЫХ ПЛАТФОРМ ИНТЕРНЕТА ВЕЩЕЙ В УСЛОВИЯХ РЕАЛИЗАЦИИ УГРОЗ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: информационная безопасность, интернет вещей, искусственные нейронные сети, достоверность, интерпретация, интерпретируемость.

В статье рассмотрены свойства интерпретации и интерпретируемости нейросетевых моделей обработки информации, лежащих в основе интеллектуальных

---

платформ интернета вещей. Обоснована значимость данных свойств в аспекте обеспечения безопасности технологии интернета вещей в условиях угроз качественного искажения информации граничных узлов в результате реализации уязвимостей протоколов связи и обмена сообщениями прикладного уровня интернета вещей. Даны рекомендации по решению задачи интерпретируемости нейросетевых платформ интернета вещей.

**D.V. Marshakov, Yu.D. Kokoulina, A.A. Abolmasov, A.V. Panasyuk**

## **ABOUT THE INTERPRETABILITY OF NEURAL NETWORK PLATFORMS OF THE INTERNET OF THINGS IN THE CONTEXT OF THREATS**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: information security, Internet of things, artificial neural networks, reliability, interpretation, interpretability.

The paper deals with the interpretation and interpretability properties of neural network models of information processing that underlie artificial intelligent platforms of the Internet of Things (IoT). The significance of these properties is substantiated in terms of ensuring the security of the IoT-technology in the context of the implementation of threats of qualitative distortion of information of border nodes as a result of the implementation of vulnerabilities in communication protocols and messaging at the application level of the IoT. Recommendations for solving the problem of interpretability of neural network platforms of the IoT are given.

Одной из ключевых технологических тенденций современных киберфизических систем является развитие экосистемы интернета вещей, концептуально представляющей собой сеть передачи данных между физическими объектами, оснащенными встроенными средствами и технологиями для взаимодействия друг с другом и внешней средой.

Экспоненциальный рост устройств интернета вещей привел к расширению первоначальной идеи пограничных (периферийных) вычислений и переносу потока генерируемых ими данных из граничных узлов в платформу интернета вещей и облачные сервисы для аналитического анализа, как правило, с применением высокотехнологичных моделей машинного обучения, в частности искусственных нейронных сетей (ИНС).

Большинство существующих на сегодняшний день пограничных вычислительных устройств не могут использовать технологии аппаратного ускорения для выполнения сложных операций линейной алгебры и вычислений с плавающей запятой, свойственных для ИНС, а больше подходят для выполнения уже обученных моделей в режиме вывода, оставляя обучение за облачными платформами, располагающими необходимыми вычислительными ресурсами.

Гибкие и открытые характеристики устройств интернета вещей и общедоступность данной технологии повышает вероятность реализации угроз и атак на их сеть как со стороны внешних, так и внутренних злоумышленников [1], в связи с чем в аспекте моделирования угроз граничных узлов также рассматривают безопасность непосредственно данных, поступающих в платформу и центры обработки информации.

Для обеспечения безопасного информационного обмена между узлами интернета вещей применяются различные протоколы связи и обмена сообщениями прикладного уровня, такие как CoAP, AMQP, MQTT и XMPP [2]. Вместе с тем, анализ их безопасности [3] показал, что ландшафт угроз продуктам и услугам интернета вещей, использующим эти протоколы, остается весьма разнообразным. Реализация уязвимостей протоколов приводит к нарушению конфиденциальности и целостности сообщений, передаваемых в

платформу интернета вещей из граничных узлов, что ведет к качественному искажению информации.

Все это влечет за собой необходимость анализа безопасности и оценки уязвимостей такого рода систем в аспекте надежности их практического применения в условиях вредоносных воздействий, представляющих собой целенаправленные воздействия на нейронные сети для организации ошибок в их поведении [4]. В частности, имеются в виду угрозы нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта и угрозы модификации модели машинного обучения путем искажения («отравления») обучающих данных (УБИ.220, УБИ.221 [5]).

В связи с этим, значимым представляется рассмотрение механизмов обработки данных в платформе интернета вещей, а именно возможностей интерпретации частично неполной или недостоверной информации, которая представляет собой существенную уязвимость для данной технологии.

Принципиальной особенностью нейросетевой модели обработки информации является трудность её интерпретации вследствие чрезмерной параметризации, что приводит к проблеме доверия к её результатам, в особенности в условиях реализации обозначенных выше угроз.

Проблемы интерпретации и интерпретируемости [6,7] моделей машинного обучения являются важной составляющей направления исследований в области объяснимого искусственного интеллекта (ХАИ). При этом сами эти понятия применительно к моделям машинного обучения являются многозначными в зависимости от мотивов интерпретации и технического описания моделей [8]. В общем, под задачей интерпретации понимается раскрытие способов формирования конечного результата на основе входных данных, например, выявление отличительных входных признаков или оценки степени их влияния на вывод. В то же время интерпретируемость модели характеризуется внутренними механизмами формирования решений и возможностью логического объяснения произведенных выводов.

Степень доверия к алгоритмам интерпретации нейросетевых моделей обработки информации, определяющая достоверность нейросетевого алгоритма, может быть оценена с помощью разнообразных подходов, например, оценки возмущений или показателей достоверности/чувствительности [7], а интерпретируемость – посредством экспертных знаний. Связь между данными понятиями приведена на рис. 1.

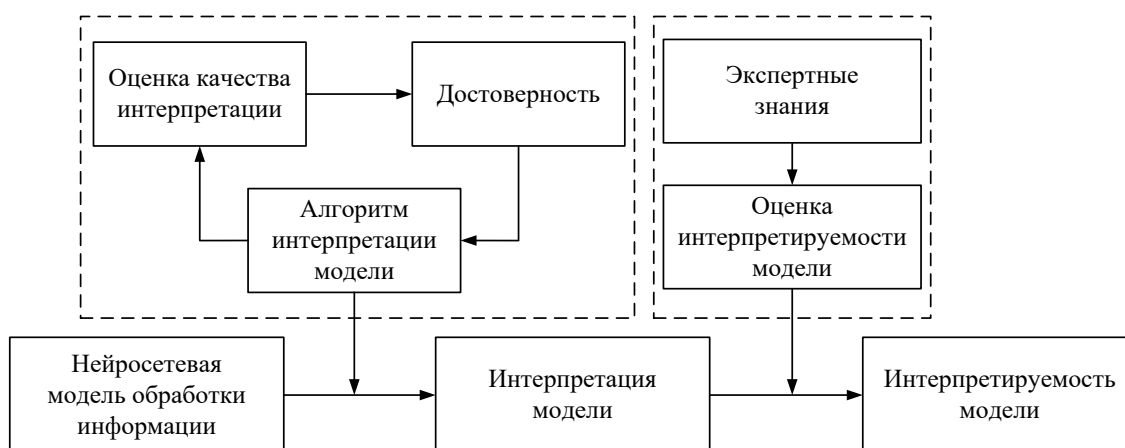


Рисунок 1. Схема интерпретации и интерпретируемости нейросетевой модели обработки информации.

Существуют разнообразные методы интерпретации различных моделей машинного обучения, в том числе нейронных сетей. Наиболее популярными на практике способами интерпретации являются LIME и SHAP – модельно-независимые библиотеки,

---

применимые к любой модели машинного обучения. Однако их общим недостатком является апостериорный характер интерпретации модели, определяемый отсутствием информации о её внутренней механике, что не обеспечивает построения причинно-следственной структуры процессов обработки информации, формируемых во время обучения или принятия решений.

Выявление скрытых закономерностей в нейросетевых алгоритмах, их формализация и сведение к системе логически объяснимых правил является одним из путей повышения «прозрачности» обработки информации нейронной сетью, определяющей их объяснимость, а значит и интерпретируемость нейросетевой модели.

Для решения данной задачи известны методы приведения нейросетевых алгоритмов к виду продукционных правил вида ЕСЛИ-ТО [9,10], на основе которых строятся нейро-нечёткие модели, а также гибридные модели, использующие ИНС и технологии экспертных систем (нейро-экспертные системы). При построении нейро-нечётких моделей, в том числе нечётких когнитивных карт [11], система становится более «прозрачной» для анализа структуры связей, однако это требует уточнения правил нечётких продукций и функций принадлежности, используя специальные алгоритмы обучения. Кроме того, такой подход ведет к сокращению избыточности информационного поля нейросетевой системы. Для нейро-экспертных систем активация нейросетевой базы знаний аналогична извлечению правил из информационного поля нейронной сети, что, как правило, требует высокой вычислительной сложности.

Перспективным представляется подход, предложенный в работе [12], основанный на гранулярных вычислениях, позволяющий вербально описать правила функционирования ИНС. Данный подход является развитием гибридной нейронной сети с самоорганизацией, представляющей собой каскадное соединение самоорганизующегося слоя и персептронной сети, с тем отличием, что самоорганизующиеся слои, осуществляющие грануляцию информационного пространства ИНС, располагаются не только во входном, но и между последующими слоями ИНС. Такая структурная особенность обеспечивает функцию кластеризации информации внутри межнейронных соединений с возможностью последующего анализа обрабатываемых нейросетью данных и представления результатов работы нейросетевого алгоритма в виде наглядных лингвистических правил. Структуризация промежуточных и выходных процессов функционирования нейронной сети и последующее их интерпретирование производится на основе нечёткого моделирования, приводящего к построению правил функционирования ИНС и обоснования их заключений. Данный подход вписывается в общую концепцию когнитивного моделирования и не требует уточнения правил нечётких продукций или прореживания ИНС с целью приведения её к логически прозрачному виду с ущербом структурной избыточности.

Оценить применимость данного подхода к построению интерпретируемой нейросетевой модели платформы интернета вещей и степень доверия к ней представляется возможным посредством следующих действий:

1. Сформировать из потока данных пограничных устройств интернета вещей обучающий набор данных для ИНС.
2. Провести генерацию аномального трафика устройств интернета вещей на основе модели потенциального злоумышленника, применимой под конкретную область интернета вещей.
3. Сформировать пару нейросетевых моделей обработки информации: модель на обучающем наборе без вредоносных воздействий, априори нечувствительную к недостоверным решениям, и модель, обученную с учетом аномального трафика данных и минимизацией тем самым недостоверных решений.
4. На основе описанного выше метода провести реструктуризацию разработанных нейросетевых моделей с целью формирования систем



---

логических правил, описывающих процедуру формирования заключений каждой из них.

5. Выполнить сравнительный анализ результатов моделирования построенных нейросетевых платформ интернета вещей на предмет интерпретации и интерпретируемости.

С целью объективности оценки полученных результатов разумным также представляется проведение интерпретации выполненных нейросетевых моделей с применением популярных библиотек SHAP, ELI5 и LIME.

Нейросетевые платформы интернета вещей используются для анализа большого количества данных, собранных с пограничных устройств, и принятия автоматических решений на основе этих данных. Они могут обрабатывать большие объемы информации, находить скрытые связи и использовать их для предсказаний и оптимизации различных процессов. Это позволяет повысить эффективность, безопасность и удобство использования устройств интернета вещей в различных, в том числе критических, областях: промышленности, здравоохранении, транспорте и пр.

Анализ механизмов обработки данных в интеллектуальной платформе интернета вещей, подразумевающий оценку интерпретации и интерпретируемость применяемой в ней модели обработки информации в условиях реализации угроз, определяет безопасность данной технологии. В данной работе были рассмотрены актуальные вопросы интерпретируемости нейросетевых платформ интернета вещей, с прицелом на последующую алгоритмическую реализацию механизма объяснения формируемых в ней решений.

#### СПИСОК ЛИТЕРАТУРЫ

1. Butt S.A., Diaz-Martinez J.L., Jamal T., Ali A., De-La-Hoz-Franco E., Shoaib M. IoT smart health security threats // Proceedings of the 2019 19th International Conference on Computational Science and Its Applications (ICCSA), (St. Petersburg, Russia, 1-4 July 2019). – pp. 26-31.
2. Al-Masri E., Kalyanam K.R., Batts J., Kim J., Singh S., Vo T., Yan C. Investigating messaging protocols for the Internet of Things (IoT) // IEEE Access 2020. – Vol. 8. – pp. 94880-94911.
3. Маршаков Д.В., Кокоулина Ю.Д., Аболмасов А.А., Панасюк А.В. Проблемы обеспечения безопасности протоколов обмена сообщениями интернета вещей // Информационно-вычислительные технологии и их приложения: сборник статей XXVII Международной научно-технической конференции (г. Пенза, 24-25 августа 2023 г.). – Пенза: Пензен. гос. аграр. ун-т, 2023. – С. 228-232.
4. Уорр К. Надежность нейронных сетей: укрепляем устойчивость ИИ к обману. – СПб.: Питер, 2021. – 272 с.
5. Банк данных угроз безопасности информации ФСТЭК России. – URL: <https://bdu.fstec.ru/threat> (дата посещения: 18.10.2023 г.)
6. Linardatos P., Papastefanopoulos V., Kotsiantis S.B. Explainable AI: A Review of Machine Learning Interpretability Methods // Entropy. – 2021. – Vol. 23. – pp. 1-45.
7. Li X., Xiong H., Li X., Wu X., Zhang X., Liu J., Bian J., Dou D. Interpretable deep learning: interpretation, interpretability, trustworthiness, and beyond // Knowledge and Information Systems. – Vol. 64. – 2022. – pp. 3197-3234.
8. Lipton Z.C. The mythos of model interpretability // Communications of the ACM. – 2016. – Vol. 61. – pp. 36-43.
9. Гридин В.Н., Солодовников В.И. Совместное использование нейросетевых технологий и деревьев решений для поиска логических закономерностей в данных // Информационные технологии и нанотехнологии: сб. тр. III Междунар. конф. и мол. шк. (Самара, 25–27 апреля 2017 г.). – Самара, 2017. – С. 1763–1769.

- 
10. Chopade H.A., Narvekar M. Hybrid Auto Text Summarization Using Deep Neural Network And Fuzzy Logic System // Proceedings of the International Conference on Inventive Computing and Informatics (Coimbatore, India, 23–24 November 2017). – IEEE, 2017. – P. 52–56.
  11. Аверкин А.Н., Ярушев С.А., Павлов В.Ю. Когнитивные гибридные системы поддержки принятия решений и прогнозирования // Программные продукты и системы. – №4. – 2017. – С. 632-642.
  12. Marshakov D.V. Rule extraction from the Artificial Neural Network // IOP Conference Series: Materials Science and Engineering: 16 (Rostov-on-Don, 11–13 September 2020). – Rostov-on-Don, 2021. P. 012127.

**А.В. Наливайко<sup>1</sup>, О.А. Решетникова<sup>2</sup>**

**ПРАКТИКА СОЗДАНИЯ СИСТЕМ  
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ  
ИНФРАСТРУКТУРЫ В ЭЛЕКТРОЭНЕРГЕТИКЕ**

ООО «Рубикон», Ростов-на-Дону, Россия<sup>1</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: информационные технологии, информационная безопасность, система обеспечения информационной безопасности, критическая информационная инфраструктура в электроэнергетике, категорирование объектов критической информационной инфраструктуры, выбор средств защиты информации.

В статье рассмотрена практика формирования перечня значимых объектов критической информационной инфраструктуры и создания системы обеспечения информационной безопасности в соответствии с требованиями законодательства Российской Федерации на примере отрасли электроэнергетики.

**A.V. Nalivaiko<sup>1</sup>, O.A. Reshetnikova<sup>2</sup>**

**THE PRACTICE OF CREATING INFORMATION SECURITY SYSTEMS  
OF CRITICAL INFORMATION INFRASTRUCTURE  
IN THE ELECTRIC POWER INDUSTRY**

LLC «Rubicon», Rostov-on-Don, Russia<sup>1</sup>

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>

Keywords: information technologies, information security, information security system, critical information infrastructure in the electric power industry, categorization of CII objects, selection of information security tools

The article considers the practice of forming a list of significant objects of critical information infrastructure and creating an information security system in accordance with the requirements of the legislation of the Russian Federation on the example of the electric power industry.

## Основные термины и определения

Критическая информационная инфраструктура (КИИ)	—	объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов (187-ФЗ, ст. 2, п. 6)
Субъекты критической информационной инфраструктуры	—	государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей (187-ФЗ, ст. 2, п. 8)
Объекты критической информационной инфраструктуры	—	информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ (187-ФЗ, ст. 2, п. 7)
Значимый объект критической информационной инфраструктуры	—	объект КИИ, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов КИИ (187-ФЗ, ст. 2, п. 3)
Компьютерная атака	—	целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации (187-ФЗ, ст. 2, п. 4)
Компьютерный инцидент	—	целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации (187-ФЗ, ст. 2, п. 4) факт нарушения и (или) прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки (187-ФЗ, ст. 2, п. 5)

### Введение.

Защита объектов критической информационной инфраструктуры (далее — КИИ) — важнейшая задача для поддержания суверенитета и безопасности государства, экономики и в целом общественной стабильности. Во всем мире фиксируются попытки осуществления целенаправленных и все более изощренных кибератак на объекты КИИ. Как сказал В.В. Путин на заседании Совета Безопасности 20 мая 2022 года: «Нам нужно самым серьезным образом и в режиме реального времени совершенствовать механизмы обеспечения информационной безопасности отраслевых критически важных объектов, от которых напрямую зависит обороноспособность нашей страны, стабильное развитие экономики и социальной сферы».

Основным документом в части защиты критически важных объектов является Федеральный Закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В нем даны основные определения КИИ и вопросов обеспечения ее безопасности.

Цель статьи — показать процесс подготовки и создания системы обеспечения информационной безопасности (далее — СОИБ) значимого объекта критической

---

информационно инфраструктуры (далее — ЗО КИИ) на примере одной из стратегически важной для государства отрасли — электроэнергетики. В статье использованы следующие методы исследования: анализ и обобщение литературы, опыта ООО «Рубикон».

Со ссылками на законодательство и примерами рассмотрим следующие процессы:

- Подтверждение, что компания — субъект КИИ.
- Определение объектов КИИ.
- Выявление ЗО КИИ (категорирование объектов КИИ).
- Создание СОИБ.

## **1. Структура электроэнергетики в России.**

В энергоснабжении Российской Федерации участвуют различные виды энергокомпаний. Под энергокомпанией понимается самостоятельный хозяйственный субъект, созданный в порядке, установленном законом РФ, для производства продукции, выполнения работ и оказания услуг в целях удовлетворения определенных общественных потребностей.

Компании сферы электроэнергетики в зависимости от их деятельности можно классифицировать по следующим функциям:

- Генерирующие компании. Крупные компании, активами которых являются электростанции разных типов.  
Например: группа «Интер РАО» и Группа «РусГидро».
- Электросетевые компании. Владеют электрическими сетями и осуществляют передачу и распределению электрической энергии с использованием объектов электросетевого хозяйства.  
Например: ПАО «Россети» и АО «Донэнерго».
- Энергосбытовые компании. Осуществляют поставку электрической энергии и мощности, крупным потребителям непосредственно с оптового рынка электрической энергии.  
Например: ПАО ГК «ТНС энерго» и АО «АтомЭнергоСбыт».

В структуре электроэнергетики присутствуют и другие неотъемлемые элементы (потребители, регуляторы, контролирующие органы и др.), но они не участвуют непосредственно в процессе энергоснабжения.

## **2. Определение значимых объектов КИИ.**

Для того, чтобы понять какие объекты информатизации (ИС, ИТКС, АСУ) необходимо защитить и являются ли они объектам КИИ, выполним ряд шагов.

### **2.1. Подтверждение, что компания — субъект КИИ.**

В соответствии с Методическими рекомендациями по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса компания относится к субъекту КИИ в случае, если для нее справедливы первые два условия или третье.

- Государственное учреждение, российское юр. лицо и/или ИП осуществляет один или несколько из основных видов своей деятельности в одной или нескольких сферах (областях) деятельности, предусмотренных п. 8 ст. 2 № 187-ФЗ.
- Государственному учреждению, российскому юр. лицу и/или ИП принадлежат на праве собственности, аренды или на ином законном основании любые ИС, ИТКС и АСУ ТП.
- Российское юр. лицо и/или ИП обеспечивает взаимодействие ИС, ИТКС и АСУ ТП, принадлежащих государственному учреждению, российскому юр. лицу и/или ИП, осуществляющему свою деятельность в одной или нескольких сферах (областях) деятельности, предусмотренных п. 8 ст. 2 187-ФЗ.

---

Если мы рассматриваем одну из описанных выше типов энергокомпаний, то они относятся к субъектам КИИ. Однако, важно понимать, что окончательное решение об отнесении к субъектам КИИ принимает компания, проанализировав свою деятельность на соответствие требованиям законодательства.

## **2.2. Определение объектов, обеспечивающих (автоматизирующих) работу критических процессов.**

Основываясь на информации из Устава, выписки из ЕГРЮЛ, внутренних документов, а также в процессе обследования информационной инфраструктуры субъекта КИИ формируем перечень процессов основных видов деятельности.

В соответствии с Методическими рекомендациями по определению и категорированию объектов КИИ топливно-энергетического комплекса субъект КИИ комиссионно определяет для каждого определенного процесса, способен ли его нарушение повлечь последствия, определенные в перечне показателей критериев значимости объектов КИИ Российской Федерации и их значений, утвержденных Постановлением Правительства Российской Федерации от 08.02.2018 № 127. Важно, что нужно рассматривать только последствия компьютерных инцидентов при наихудшем варианте развития событий.

*Примеры процессов:*

- *Оперативно-технологическое управление;*
- *Организация введения режима ограничения (возобновления) потребления электроэнергии;*
- *Управление энергосбережением и повышением энергоэффективности;*
- *Метрологическое обеспечение.*

Полученный перечень критических процессов сопоставляется с теми объектами информатизации субъекта КИИ, которые обеспечивают их автоматизацию.

Из полученного перечня ИС, АСУ, ИТКС, принадлежащих субъекту КИИ на праве собственности, обеспечивающих функционирование (автоматизацию) критических процессов, формируется перечень объектов КИИ.

*Примеры объектов:*

- *Общего характера, которые можно встретить в любой организации, вроде электронной почты, ЛВС, системы видеонаблюдения, ИСПДн на базе ИС и др.*
- *Специализированные учетные системы, в том числе с возможностью контроля подачи электроэнергии конечному потребителю.*
- *Специализированные информационные системы, которые связаны с телемеханикой и позволяют управлять и контролировать на расстоянии технологические процессы на электрических станциях и подстанциях электросетевого комплекса различного класса напряжения.*

## **2.3. Выявление значимых объектов (категорирование).**

На данном этапе определяем значимость выявленных объектов КИИ. Для этого комиссия субъекта КИИ проводит оценку масштаба возможных последствий в случае возникновения компьютерных инцидентов и присваивает каждому объекту КИИ категорию значимости либо присваивает статус «без категории».

В процессе оценки требуется провести анализ потенциальных нарушителей и угроз безопасности. Для этих целей разрабатывается модель угроз безопасности информации ЗО КИИ.

Также определяем и рассматриваем типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации.

В процессе категорирования формируется ряд документов, в том числе «Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий» (акт категорирования). Важно, что каждая графа акта категорирования должна быть заполнена. Если какой-то из пунктов неактуален, то необходимо указать с

---

обоснованием о его неприменимости. Это касается и указания нарушителей, угроз и типов инцидентов.

Всего выделяется 3 категории значимости. Чем ниже категория, тем ниже значимость. Если же объекту КИИ комиссия не присвоила категорию, то он не является значимым. В этом случае система защиты объекта не регулируется 187-ФЗ, но субъект КИИ имеет право его применить по своему решению.

В Постановлении Правительства Российской Федерации от 08.02.2018 № 127 детально расписаны показатели критериев значимости. Они делятся на следующие категории:

- Социальная;
- Политическая;
- Экономическая;
- Экологическая;
- Значимость для обеспечения обороны страны, безопасности государства и правопорядка.

Рассмотрим процесс категорирования на примерах.

### **2.3.1. Пример № 1. SCADA-система в составе системы телемеханики.**

Объект представляет собой автоматизированную систему управления технологическим процессом, а также совокупность функционально объединенных компонентов и устройств. Предназначен для обеспечения функционирования системы сбора и передачи технологической информации и автоматизации следующих процессов:

- сбор дискретных телесигналов (ТС) состояния и режима работы оборудования;
- сбор аналоговых сигналов – телеизмерений (ТИ) режима работы сети электроснабжения;
- контроль устройств РЗА - срабатывание устройств сигнализации, защиты и автоматики;
- прием и выполнение команд управления (ТУ).

#### **Субъекты доступа.**

Субъектами доступа в Системе являются пользователи (пользователи Системы, администраторы Системы, администраторы безопасности Системы), а также процессы, инициируемые программным обеспечением.

#### **Прикладные программы, обеспечивающих выполнение функций объекта.**

Программный комплекс «Корсар 2» — ООО «НПО «НовоТестСистемы».

#### **Архитектура объекта.**

Программное обеспечение имеет клиент-серверную архитектуру. Серверное ПО выполняет обработку данных, передаваемых от контроллеров телемеханики на конечных объектах — подстанциях, реклоузерах и др. Клиентское ПО предназначено для рабочих станций, обеспечивающих отображение данных и человеко-машинный интерфейс. Аппаратная часть системы представляет собой совокупность серверов и рабочих станций, объединённых в локальную вычислительную сеть.

#### **Значимость объекта.**

Для объекта актуален критерий социальной значимости, в частности «Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения».

Оценка производится с учетом наличия возможности несанкционированного воздействия на компоненты объекта КИИ. Рассматривается количество населения в тыс. человек, у которого могут возникнуть перебои в поставках электроэнергии, при нарушении штатного режима функционирования объекта КИИ в результате проведения компьютерной атаки, а также масштаб территории: в одном или более субъектов РФ.

Таблица 1. Показатели значимости SCADA-системы в составе системы телемеханики

Показатель ПП 127	Значение показателя		
	III категория	II категория	I категория
I. Социальная значимость			
2. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, оцениваемые:			
а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения	в пределах территории одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	более или равно 2, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000

В зависимости от этих показателей комиссия по категорированию субъекта принимает решение о присвоении категории значимости объекту. Рассмотрим вариант, когда масштаб объекта находится в пределах одного муниципального региона и количество людей, которых может коснуться последствия компьютерного инцидента, менее 1 000 тыс. человек — выбираем третью категорию. По остальным критериям, хоть они и не актуальны, необходимо указать расчет показателя или основание, по которому тот или иной критерий в данном случае не применим.

### 2.3.2. Пример № 2. Интеллектуальная система учета электроэнергии.

Объект представляет собой автоматизированную систему управления технологическим процессом, а также совокупность функционально объединенных компонентов и устройств. ИСУЭ предназначена для удаленного сбора, обработки, передачи показаний приборов учета электрической энергии, обеспечивающая информационный обмен, хранение показаний приборов учета электрической энергии, удаленное управление ее компонентами, устройствами и приборами учета электрической энергии, не влияющее на результаты измерений, выполняемых приборами учета электрической энергии, а также предоставление информации о результатах измерений, данных о количестве и иных параметрах электрической энергии.

#### Субъекты доступа.

Субъектами доступа в Системе являются пользователи (пользователи Системы, администраторы Системы, администраторы безопасности Системы, пользователи публичного портала Системы), а также процессы, инициируемые программным обеспечением.

#### Прикладные программы, обеспечивающие выполнение функций объекта.

Программное обеспечение «Пирамида 2.0» — АО ГК «Системы и Технологии».

#### Архитектура.

Программное обеспечение имеет клиент-серверную архитектуру. Серверное ПО выполняет обработку данных, передаваемых от приборов учета и устройств сбора и передачи данных (далее – УСПД). Клиентское ПО предназначено для рабочих станций, обеспечивающих отображение данных и человеко-машинный интерфейс. Аппаратная

---

часть системы представляет собой совокупность серверов и рабочих станций, объединённых в локальную вычислительную сеть.

#### **Значимость объекта.**

При условии, что используется функция контроля подачи электроэнергии, для объектов данного типа актуален критерий социальной значимости, в частности «Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения».

Оценка производится комиссией субъекта КИИ аналогично прошлому примеру. Теперь рассмотрим вариант, что объект затрагивает два субъекта РФ, поэтому автоматически выходим на первую категорию. По остальным критериям, хоть они и не актуальны, необходимо указать расчет показателя и основание, по которому они в данном случае не применимы.

Чтобы избежать первой категории, разумно рассмотреть варианты сегментирования. Так один объект масштаба двух регионов может быть разбит на несколько. Например, по регионам или муниципальным образованиям. Иногда, конечно, такое сегментирование экономически нецелесообразно в связи с необходимостью приобретения программного обеспечения для управления, а также серверов для каждого отдельного объекта, выделения отдельных ответственных специалистов на местах.

### **3. Создание системы обеспечения информационной безопасности.**

Теперь на основе полученной информации формируем требования к СОИБ.

#### **3.1. Формирование требований.**

Требования определяем в соответствии со следующими нормативными актами:

- Приказом ФСТЭК от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказом ФСТЭК от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказом ФСТЭК от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (только в части определения мер защиты среды виртуализации, по причине отсутствия данных мер в Приказе ФСТЭК от 25.12.2017 № 239).

Также могут быть актуальны и другие документы в зависимости от данных, которые обрабатываются в информационных системах. Например, Приказ ФСТЭК № 21 для ИСПДн или Приказ ФСТЭК № 17 для ГИС.

СОИБ должна реализовывать технические и организационные меры защиты и соответствовать требованиям нормативно-распорядительных документов, установленными для определенной категории значимости.

Меры вытекают из актуальных угроз безопасности, которые определяем в модели угроз. Для каждой угрозы (имеет код формата «УБИ.ХХХ») выбираем в приказах ФСТЭК соответствующие меры (имеют буквенно-численный код типа «ИАФ.0»: первая часть — категория, вторая — номер по порядку). Далее для каждой меры необходимо описать требования по реализации.

*Например, для угрозы с кодом «УБИ.026» (Угроза искажения XML-схемы) выбираем меру с кодом «ЗИС.19» (Защита информации при ее передаче по каналам связи) из Приказа ФСТЭК № 239. А для угрозы с кодом «УБИ.085» (Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации) выбираем меру с кодом «ЗСВ.8» (Резервное копирование данных,*



резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры) из Приказа ФСТЭК № 21, кроме ряда мер из 239 Приказа.

В соответствии с Приказом ФСТЭК № 239 при проектировании СОИБ:

- определяются субъекты доступа (пользователи, процессы и иные) и объекты доступа;
- определяются политики управления доступом (дискреционная, мандатная, ролевая, комбинированная);
- определяются и обосновываются организационные и технические меры, подлежащие реализации в рамках СОИБ;
- определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности Системы;
- осуществляется выбор средств защиты информации и (или) их разработка с учетом категории значимости Системы, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;
- разрабатывается архитектура СОИБ, включающая состав, места установки, взаимосвязи средств защиты информации;
- определяются требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта;
- определяются меры по обеспечению безопасности при взаимодействии Системы с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями

В случае если в ходе проектирования СОИБ значимого объекта предусмотрена разработка программного обеспечения, в том числе программного обеспечения средств защиты информации, такая разработка проводится в соответствии со стандартами безопасной разработки программного обеспечения.

Технические меры по обеспечению безопасности реализуются посредством использования программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов – средств защиты информации. При этом в приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов.

### 3.2. Этапы создания.

Содержание и порядок работ по созданию СОИБ выполняются в соответствии с Национальным стандартом Российской Федерации «ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». Создание СОИБ обеспечивается работами согласно Таблице 2.

Таблица 2. Этапы создания СОИБ

№	Этап
1	Разработка технико-рабочей документации проекта СОИБ
2	Формирование эксплуатационной документации СОИБ
3	Разработка нормативно-организационной документации, обеспечивающей реализацию организационных мер защиты
4	Создание СОИБ, в том числе Строительно-монтажные и пусконаладочные работы
5	Предварительные испытания СОИБ
6	Опытная эксплуатация СОИБ
7	Приемочные испытания СОИБ

### 3.3. Пример. СОИБ интеллектуальной системы учета электроэнергии.

Рассмотрим создание СОИБ на примере ИСУЭ, которой присвоили 1 категорию.

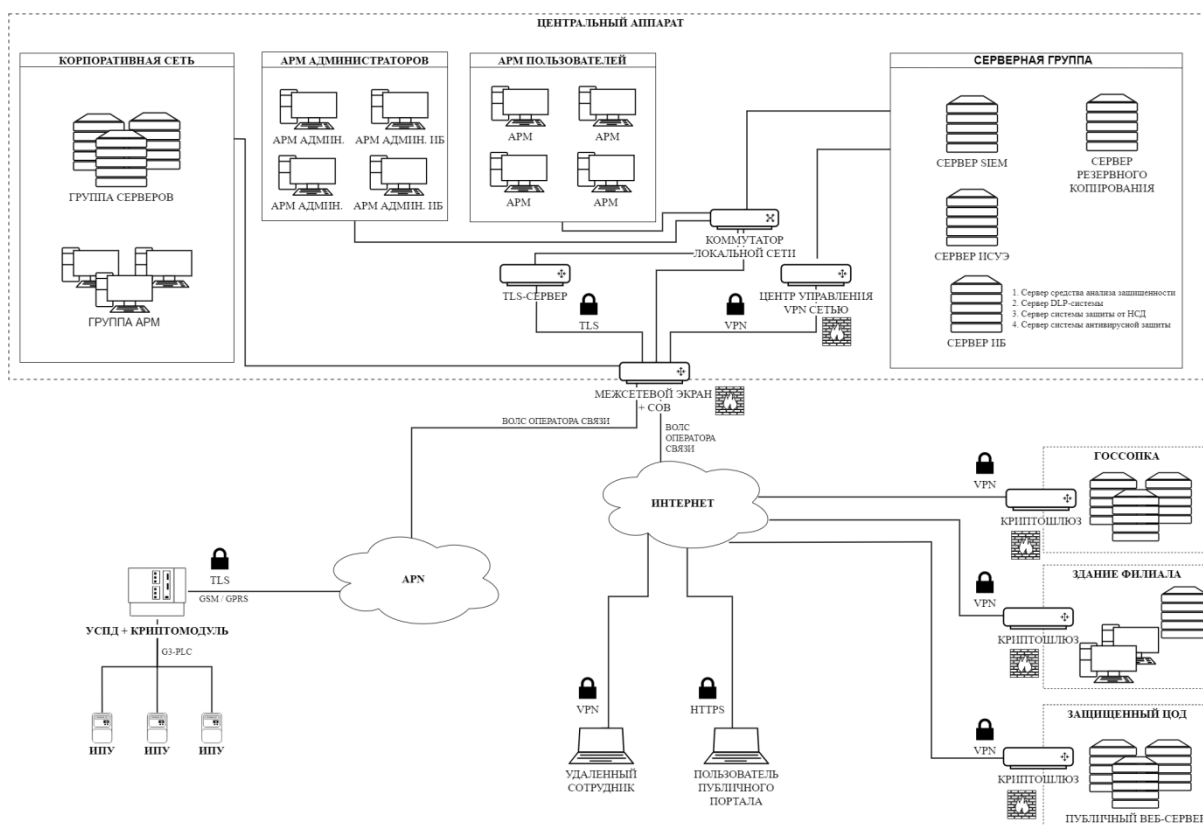


Рисунок 1. Архитектура СОИБ ИСУЭ

В данном случае СОИБ состоит из следующих подсистем:

1. Подсистема идентификации, аутентификации и управления доступом:  
Примеры СЗИ: SecretNet LSP, сертифицированная ОС и др.
2. Подсистема контроля целостности данных и защиты от НСД.  
Примеры СЗИ: SecretNet LSP, сертифицированная ОС и др.
3. Подсистема антивирусной защиты (обязательно использовать 2 разных):  
Примеры СЗИ: Kaspersky Endpoint Security, DrWEB и др.
4. Подсистема резервного копирования и восстановления информации.  
Примеры ПО: RuBackup, Кибер Бэкап и др.
5. Подсистема сбора, анализа и корреляции событий информационной безопасности.  
Примеры СЗИ: RuSIEM, MaxPatrol SIEM и др.
6. Подсистема межсетевого экранирования, обнаружения предотвращения вторжений.  
Примеры СЗИ: Континент 4, PT NGFW, UserGate NGFW и др.
7. Подсистема криптографической защиты.  
Примеры СЗИ: IT SM + NGate, АПКШ «Континент» и др.
8. Подсистема анализа защищённости.  
Примеры СЗИ: Сканер-ВС, PT XSpider и др.
9. Подсистема выявления утечек данных.  
Примеры СЗИ: SearchInform, Staffcop и др.
10. Подсистема защиты среды виртуализации.  
Примеры СЗИ: Горизонт-ВС, Средства виртуализации ОС «Astra Linux Special Edition» и др.

### **Заключение.**

В статье рассмотрен процесс подготовки и создания СОИБ ЗО КИИ на примере электроэнергетических компаний.

В соответствии с федеральным законом 187-ФЗ, подзаконными актами и отраслевыми документами разобрано понятие субъекта КИИ, процесс формирования перечня объектов и выявления среди них значимых. На основе полученной информации рассмотрен порядок формирования требований к системе обеспечения информационной безопасности значимого объекта КИИ и примеры технических решений для использования в системе безопасности интеллектуальной системы учета электроэнергии.

Можно сделать вывод, что важность данного процесса не вызывает сомнения. Это также подтверждают нововведения, которые вводят регуляторы. Например, в качестве подготовки к применению СКЗИ в ИСУЭ в августе 2023 года внесены изменения, которые позволяют работать с СКЗИ в приборах учета, УСПД и иных промежуточных элементах ИСУЭ без лицензии ФСБ России. Также вступило в силу требование ФСТЭК России к производителям программного обеспечения значимых объектов КИИ — для новых и модернизируемых объектов с начала 2023 года необходимо предоставлять информацию о соответствии разрабатываемого программного продукта требованиям по безопасности.

### **СПИСОК ЛИТЕРАТУРЫ**

1. Об информации, информационных технологиях и о защите информации : Федер. закон от 27.07.2006 № 149-ФЗ // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/12148555/> (дата обращения: 20.10.2023). — Текст : электронный.
2. О безопасности критической информационной инфраструктуры Российской Федерации : Федер. закон от 26.07.2017 № 187-ФЗ // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/71730198/> (дата обращения: 20.10.2023). — Текст : электронный.
3. О безопасности объектов топливно-энергетического комплекса : Федер. закон от 21.07.2011 № 256-ФЗ // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/12188188/> (дата обращения: 20.10.2023). — Текст : электронный.
4. Об электроэнергетике : Федер. закон от 26.03.2003 № 35-ФЗ // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/185656/> (дата обращения: 20.10.2023). — Текст : электронный.
5. Об утверждении показателей критериев значимости объектов КИИ РФ и их значений, а также порядка и сроков осуществления их категорирования : Пост. Правительства РФ от 08.02.2018 № 127-П // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/71876120/> (дата обращения: 20.10.2023). — Текст : электронный.
6. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования : Приказ ФСТЭК России от 21.12.2017 № 235 // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/71886248/> (дата обращения: 20.10.2023). — Текст : электронный.
7. Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий : Приказ ФСТЭК России от 22.12.2017 № 236 // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/71924214/> (дата обращения: 20.10.2023). — Текст : электронный.
8. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : Приказ

- 
- ФСТЭК России от 25.12.2017 № 239 // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/71901880/> (дата обращения: 20.10.2023). — Текст : электронный.
9. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России от 18.02.2013 № 21 // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/70380924/> (дата обращения: 20.10.2023). — Текст : электронный.
  10. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : Приказ ФСТЭК России от 14.03.2014 № 31 // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/70690918/> (дата обращения: 20.10.2023). — Текст : электронный.
  11. Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну : Приказ ФАПСИ от 13.06.2001 № 152 // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/183628/> (дата обращения: 20.10.2023). — Текст : электронный.
  12. Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005) : Приказ ФСБ России от 09.02.2005 № 66 // Гарант: офиц. сайт. — URL: <http://ivo.garant.ru/#/document/187947/> (дата обращения: 20.10.2023). — Текст : электронный.
  13. Методика оценки угроз безопасности информации : Метод. документ ФСТЭК России от 05.02.2021 // ФСТЭК России: офиц. сайт. — URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g> (дата обращения: 20.10.2023). — Текст : электронный.
  14. Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса : Метод. документ Минэнерго России от 31.07.2019 № ЧА-8630/15 // Минэнерго России: офиц. сайт. — URL: <https://minenergo.gov.ru/view-pdf/11357/102517> (дата обращения: 20.10.2023). — Текст : электронный.
  15. Базовая модель угроз безопасности информации в ИСУ : Метод. документ Минэнерго России от 29.06.2021 № НШ-7491/07 // Минэнерго России: офиц. сайт. — URL: <https://minenergo.gov.ru/node/20966> (дата обращения: 20.10.2023). — Текст : электронный.
  16. Заседание Совета Безопасности 20 мая 2022 года // Администрация Президента России : офиц. сайт. — URL: <http://www.kremlin.ru/events/president/news/68451/> (дата обращения: 20.10.2023).
  17. Защита объектов КИИ // ООО «Рубикон» : офиц. сайт. — URL: <https://rcngroup.ru/blog/zashhita-obektov-kii/> (дата обращения: 20.10.2023).

## **НАСТРОЙКА ВИРТУАЛЬНОГО ЧАСТНОГО СЕТЕВОГО КАНАЛА МЕЖДУ ДВУМЯ ОТДЕЛАМИ**

Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Ростов-на-Дону, Россия

Ключевые слова: VPN, IP-адрес, локальная сеть, трафик, Интернет.

В статье рассмотрены вопросы реализации VPN-туннеля для связи между филиалами. Виртуальная частная сеть представляет собой связь между двумя разными точками, такими как VPN-маршрутизаторы, находящимися в различных сетях. Она обеспечивает безопасную передачу личных данных через публичную сеть, такую как Интернет, и создает частную сеть, способную безопасно передавать информацию между указанными точками или сетями через зашифрованный туннель. VPN-туннель устанавливает связь между двумя компьютерами или сетями, позволяя передавать данные через Интернет так, словно они находятся внутри этих сетей.

**I.A. Kazachansky**

## **SETTING UP A VIRTUAL PRIVATE NETWORK CHANNEL BETWEEN THE TWO DEPARTMENTS**

Federal State Autonomous Educational Institution of Higher Education "Southern Federal University", Rostov-on-Don, Russia

Keywords: VPN, IP address, local, network, traffic, Internet.

The article discusses the implementation of the VPN tunnel for communication between branches. The virtual private network is a connection between two different points, such as VPN routers located in various networks. It provides a safe transfer of personal data through a public network, such as the Internet, and creates a private network capable of safely transmitting information between the specified points or networks through an encrypted tunnel. The VPN tunnel establishes a connection between two computers or networks, allowing you to transmit data via the Internet as if they are inside these networks.

Виртуальная частная сеть представляет собой связь между двумя разными точками, такими как VPN-маршрутизаторы, находящимися в различных сетях. Она обеспечивает безопасную передачу личных данных через публичную сеть, такую как Интернет, и создает частную сеть, способную безопасно передавать информацию между указанными точками или сетями через зашифрованный туннель. VPN-туннель устанавливает связь между двумя компьютерами или сетями, позволяя передавать данные через Интернет так, словно они находятся внутри этих сетей. Важно отметить, что это соединение обеспечено шифрованием данных, передаваемых между двумя сетями.

Если компания имеет структурные подразделения и филиалы, расположенные на разных территориях, или если требуется обеспечить безопасный доступ, то настройка VPN в данном случае является идеальным решением. Очень часто установка структурированной кабельной системы не полностью удовлетворяет потребности предприятия, для сотрудников необходимо соорудить доступ к важным данным с мобильных устройств, вне офиса, во время командировок и других случаев. Кроме того, существует надобность в обеспечении надежной связи между филиалами, что особенно актуально для компаний, занимающихся логистикой, торговыми сетями, банками и другими сферами. VPN-технология широко используется в корпоративной среде и не

только. VPN — это создание виртуальной частной сети, которая позволяет успешно решать все эти задачи. VPN-соединение создает безопасный канал связи между двумя физическими сетями путем их объединения в единую виртуальную сеть. Оно также обеспечивает безопасный доступ к корпоративным ресурсам с удаленных устройств.

Виртуальные частные сети защищают передачу данных в интернете, обеспечивая шифрование, при этом зашифрованные соединения способствуют обеспечению конфиденциальности при передаче данных и могут предотвратить несанкционированный доступ, а также позволяют пользователям работать удаленно.

Часто можно провести аналогию с платными шоссе, где пакеты данных проходят через пункты контроля и регистрации. В публичной сети любой может наблюдать за передачей данных и даже попытаться их перехватить для несанкционированного доступа к ресурсам. VPN-соединение создает безопасный "туннель", который защищает передачу данных (трафика) от посторонних глаз. Этот процесс часто описывается как "туннелирование".

Однако, создание виртуальной сети поверх физической локальной сети требует решения важных вопросов, таких как оплата трафика и выбор правильной схемы маршрутизации.

При настройке VPN-соединения основной DNS-шлюз на компьютере, подключающемся к корпоративному серверу, по умолчанию устанавливается для VPN-сети, это означает, что доступ к локальной сети и Интернету будет осуществляться через VPN-соединение, и клиент будет оплачивать внутрисетевой трафик, как если бы он передавался через Интернет.

Важным моментом при создании VPN-сети является правильный выбор схемы маршрутизации для VPN-сервера, это гарантирует, что доступ к важным данным и ресурсам будет доступен только тем, кто имеет на это право, и что информация, передаваемая через VPN-сеть, достигнет только своего адресата. Существует несколько вариантов схем маршрутизации VPN-сервера:

- VPN-клиенты используют IP-адреса, которые присваиваются из локального сетевого диапазона, который изображён на Рисунке 1;

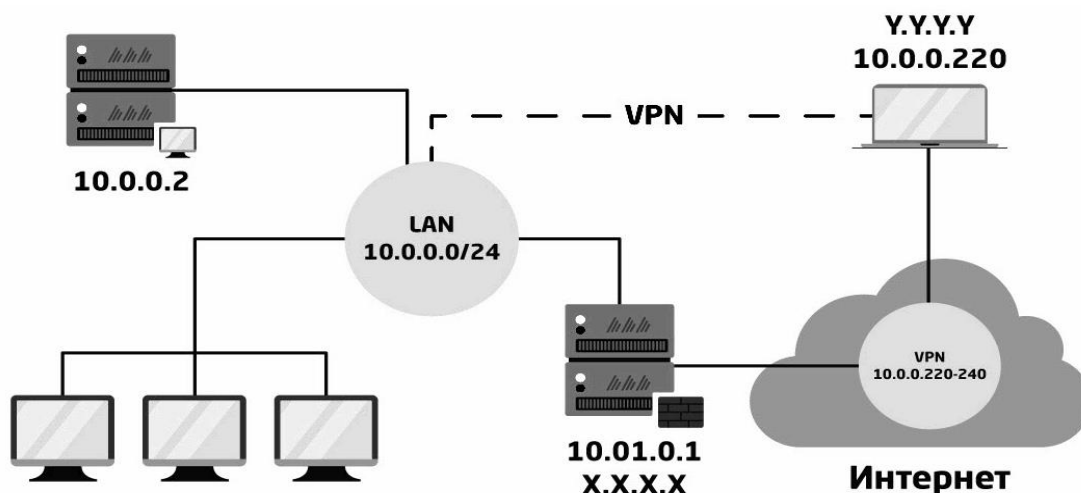


Рисунок 1. Присвоение IP-адреса, принадлежащего локальной сети

- VPN-клиенты получают IP-адреса из диапазона, который находится вне локальной сети, но управляется ею, как показано на Рисунке 2;

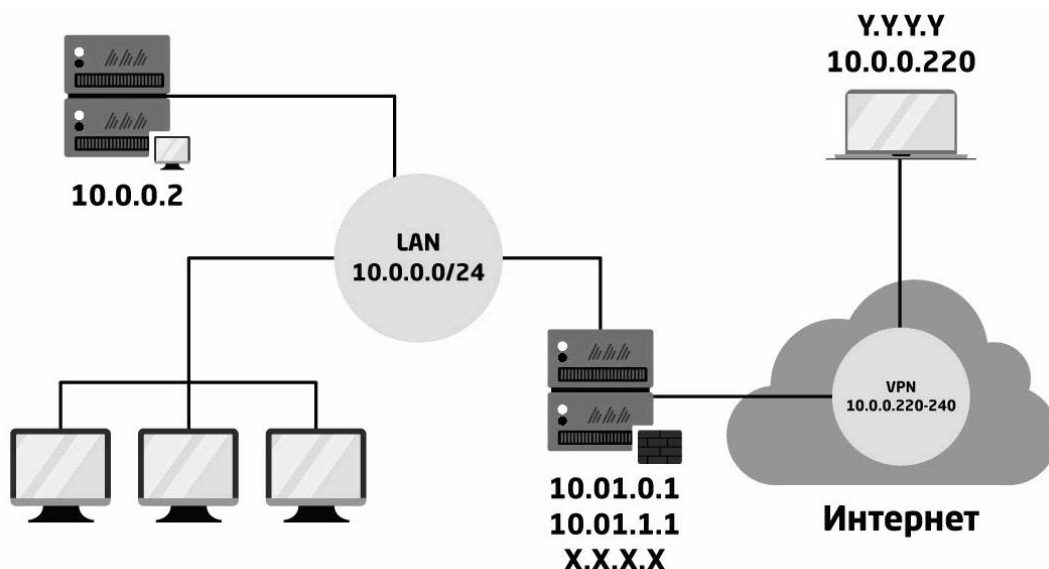


Рисунок 2. Присвоение IP-адреса из диапазона, не являющегося частью локальной сети, но управляемого из нее

- VPN-клиентам назначаются IP-адреса из диапазона вне сети, который не маршрутизируется из нее, показано на Рисунке 3.

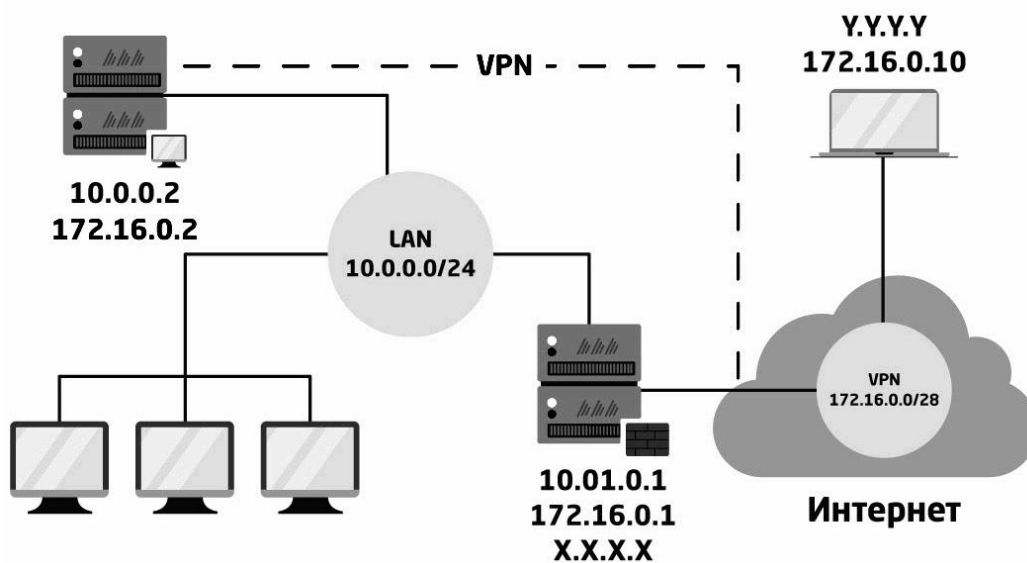


Рисунок 3. Присвоение IP-адреса из диапазона, не являющегося частью локальной сети, но находящегося под ее контролем

Этот план пригоден для осуществления доступа внутри корпоративной сети для пользователей, у которых низкое доверие, в данном случае пользователи могут получить доступ к информации расположенная на VPN сервере, но только с определённого IP-адреса. К примеру, на приведённом рисунке сервер с IP-адресом 10.0.0.2 будет открыт доступ пользователям через VPN соединение используя IP-адрес 172.16.0.2. Объединение подсетей филиалов с центральным офисом показана на Рисунке 4.

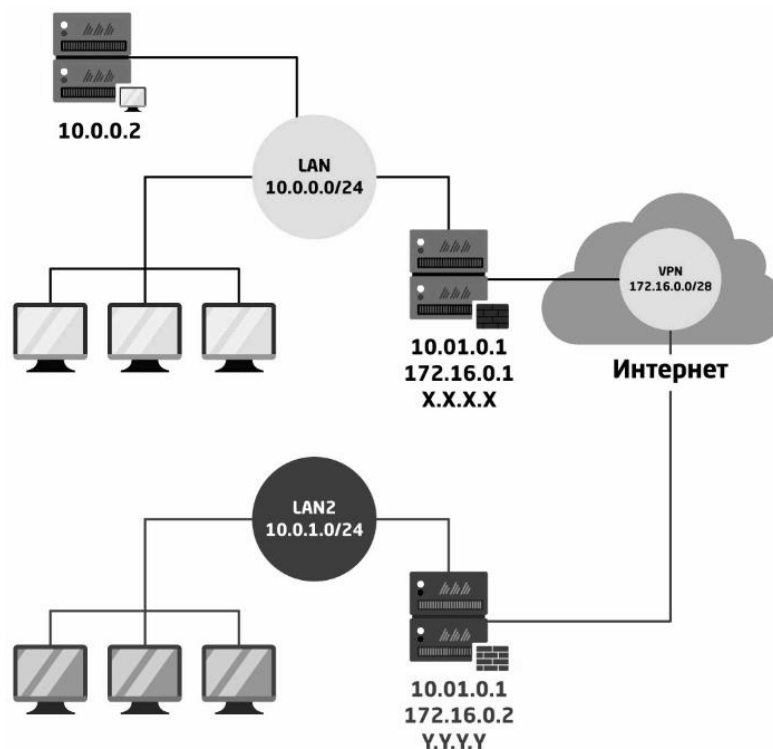


Рисунок 4. Объединение подсетей филиалов с центральным офисом

Следящая схема являться достаточно сложная, однако она идеально подходит для обеспечения надёжного соединения между филиалами. В этой схеме VPN сервер, расположенный в головном офисе, и управляет трафиком в то время маршрутизаторы действуют как VPN-клиенты. В данной схеме для обеспечения работы используется статическая маршрутизация для каждого клиента которые устанавливаются один раз и затем остаются неизменными.

#### СПИСОК ЛИТЕРАТУРЫ

1. VPN между локальными сетями. URL: <https://www.osp.ru/lan/1998/10/133760> (дата обращения 03.10.23).
2. Раздельное туннелирование VPN: как использовать его для обеспечения максимальной безопасности и производительности. URL: <https://clickfraud.ru/razdelnoe-tunnelirovanie-vpn-kak-ispolzovat-ego-dlya-obespecheniya-maksimalnoj-bezopasnosti-i-proizvoditelnosti/> (дата обращения 03.10.23).
3. Организация VPN каналов между офисами. Маршрутизация. URL: [https://interface31.ru/tech\\_it/2015/08/organizaciya-vpn-kanalov-mezhdu-ofisami-marshrutizaciya.html](https://interface31.ru/tech_it/2015/08/organizaciya-vpn-kanalov-mezhdu-ofisami-marshrutizaciya.html) (дата обращения 04.10.23).
4. Мезенцев А.В. Технологии защищенной обработки информации: учеб. пособие. / А.В. Мезенцев, Н. И. Синадский, Д. А. Хорьков; Федер. гос. бюджет. учреждение высш. проф. образования "Иркут. гос. ун-т", Ин-т математики, экономики и информатики. – Иркутск: Издво ИГУ, 2013. – 120 с.
5. VPN соединение между двумя офисами. Создание новой сети и удаление созданной сети. Настраиваем OpenVPN сервер. URL: <https://qzoreteam.ru/vpn-soedinenie-mezhdu-dvumya-ofisami-sozdanie-novoi-seti-i-udalenie/> (дата обращения 04.10.23).
6. Столлингс В. «Основы защиты сетей. Приложения и стандарты - М.: «Вильямс», 2012. – 432 с.



## ЭФФЕКТИВНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ СЕТИ

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: локальная сеть, обеспечение безопасности, антивирусное программное обеспечение, средство защиты информации от несанкционированного доступа, средство анализа защищённости, защита службы системы доменных имен, списки контроля доступа, туннелирование, шифрование данных, фильтрация на межсетевом экране.

В статье рассмотрены вопросы безопасности инфраструктуры локальной сети и необходимость проведения анализа угроз безопасности информации в целях определения способов возникновения угроз и устранения их последствий.

**A.A. Borisenko, B.P. Borisov, V.I. Yukhnov**

## EFFECTIVE MEANS OF SECURING THE LOCAL NETWORK

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: local network, security, antivirus software, anti-virus software, information protection against unauthorised access, security analysis tool, domain name system service protection, access control lists, tunnelling, data encryption, firewall filtering.

The article considers the issues of local network infrastructure security and the need to analyze threats to information security in order to determine the ways of threats and eliminate their consequences.

Целью работы являются возможные решения по безопасности для локальных сетей различного типа.

Рассмотрение вопросов безопасности при проектировании локальной сети, позволяет избежать проблемы масштабирования сети и повышения ее эффективности, возникающих при добавлении средств безопасности к уже законченному проекту. При этом необходимо учитывать безопасность сетевой инфраструктуры и информационную безопасность.

Для анализа угроз безопасности информации необходимо определить возможные способы реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учетом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов значимого объекта, взаимодействия с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями, а также особенностей функционирования значимого объекта.

В рамках обеспечения комплекса безопасности сети требуется рассмотреть вопросы защиты каналов связи, системы контроля доступа пользователей, защиты от вирусов и защиту от спама, утечку информации и т.д.

---

В основе любой системы информационной безопасности лежит предполагаемая модель угроз. Необходимо учитывать две категории угроз при планировании системы защиты: внешние и внутренние угрозы.

Внешние угрозы достаточно предсказуемы, так как компания располагает информацией о доступных извне услугах, о программно-аппаратных ресурсах, обеспечивающих связь между этой услугой и Интернетом.

Пользователи в локальной сети имеют разный уровень доступа, поэтому с внутренними угрозами бороться гораздо сложнее. У внутреннего злоумышленника цель – получить контроль над электронными информационными ресурсами сети LAN, включая средства их обработки, хранения и предоставления на доступном ему уровне.

Меры по обеспечению безопасности сети необходимо реализовывать с использованием нескольких решений.

Традиционный выбор средств для решения проблем безопасности: антивирусное и антишпионское ПО, средство защиты информации от несанкционированного доступа, средство анализа защищённости, защита службы системы доменных имен, списки контроля доступа, туннелирование, шифрование данных, фильтрация на межсетевом экране, выделенные межсетевые экраны.

### **Антивирусное и антишпионское ПО.**

Критериями для сравнительного анализа антивирусных систем необходимо выбирать технические характеристики. Предпочтение отдавать антивирусному ПО, которое оказывает минимальное влияние на работу системы и наименьшую нагрузку на сеть. Антивирусная защита должна обеспечивать защиту самих объектов сети, а также иных сервисов и обновлять базы данных признаков вредоносных компьютерных программ.

### **Средство защиты информации от несанкционированного доступа.**

Для организации идентификации и аутентификации пользователей, их процессов и устройств следует использовать системы защиты информации от несанкционированного доступа. Система защиты информации от несанкционированного доступа предназначена для управления учетными записями, разделением полномочий и назначением необходимых прав пользователям. Функционал средств защиты информации включает в себя: двухфакторную аутентификацию, дискреционный принцип контроля доступа к ресурсам системы, создание замкнутой программной среды пользователя, регистрацию событий безопасности, контроль целостности защищаемых ресурсов системы, управление пользователями и устройствами.

### **Средство анализа защищённости.**

Аппаратно-программный комплекс обнаружения компьютерных атак должен быть способен выявлять, анализировать и сообщать о компьютерных инцидентах, а также применять меры по предотвращению и ликвидации последствий компьютерных инцидентов.

### **Защита службы системы доменных имен.**

Серверы системы доменных имен (DNS) должны находиться под строгим контролем и постоянным наблюдением. Преобразование имен в адреса является критически важным для любой сети. DNS-серверы должны быть защищены с помощью пакетных фильтров на роутерах и версий программного обеспечения DNS, выполняющих функции защиты.

Как правило, в системе DNS не существует способа проверки информации, полученной от DNS в ответ на запрос. Злоумышленник может перехватить запрос и

---

вернуть ложное преобразование имени в адрес. Для предотвращения угроз безопасности к протоколу добавлены цифровая подпись и другие средства защиты. [1]

#### **Списки контроля доступа.**

Списки контроля доступа обеспечивают фильтрацию пакетов для контроля потока трафика. Разработчики сетей используют межсетевые экраны для защиты сети от несанкционированного доступа. Межсетевые экраны или брандмауэры – это программные или аппаратные решения для повышения защиты сети. Простой брандмауэр можно настроить на роутере для фильтрации трафика на базовом уровне с помощью списков контроля доступа, использование которых позволяет фильтровать трафик, разрешая или блокируя только определенные пакеты. [2]

#### **Туннелирование.**

Туннелирование позволяет разделять пакеты различных типов протоколов внутри IP-туннелей и создавать канал «точка-точка» с роутерами в удаленных точках IP-сети. Протокол туннелирования предназначен для управления передачей IP-трафика между площадками, которые взаимодействуют только по IP.

#### **Шифрование данных.**

Шифрование следует использовать в тех случаях, когда пользователь, проанализировав возможные угрозы, пришел к выводу о серьезных последствиях нарушения конфиденциальности данных, а также если аутентичность отправителя данных не гарантируется. Шифрование рекомендуется для организаций, которые взаимодействуют через Интернет с использованием VPN для обеспечения конфиденциальности данных организации.

#### **Фильтрация на межсетевом экране.**

Межсетевые экраны с фильтрацией пакетов не используют модули доступа для каждого протокола, поэтому могут применяться с любым IP-протоколом. Некоторые протоколы требуют от брандмауэра распознавания выполняемых ими действий. Передача файлов невозможна, если брандмауэр не умеет считывать трафик и определять порты, которые будут использоваться новым соединением.

Таким образом реализованные решения безопасности сети должны адаптироваться к росту сетей и изменяющимся требованиям.

### **СПИСОК ЛИТЕРАТУРЫ**

1. Юхнов В. И., Бородин А.А. ВЫБОР СРЕДСТВ CISCO ДЛЯ РЕШЕНИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ. Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. С. 300-303.
2. Юхнов В. И., Бородин А.А. АНАЛИЗ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ CISCO ДЛЯ ОБЕСПЕЧЕНИЯ ВНУТРЕННЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ. Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2021. С. 273-277.

---

## **ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В СФЕРЕ ОБРАЗОВАНИЯ, ЭКОНОМИКИ И МЕНЕДЖМЕНТА**

### **INFORMATION AND COMMUNICATION TECHNOLOGY IN EDUCATION, ECONOMICS AND MANAGEMENT**

**И.В. Головина<sup>1</sup>, Т.Я. Александрова<sup>2</sup>**

#### **ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СФЕРЕ ОБРАЗОВАНИЯ: ЭТИЧЕСКИЙ АСПЕКТ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Частное образовательное учреждение высшего образования «Московский университет имени С.Ю. Витте», г. Москва, Россия<sup>2</sup>

Ключевые слова: интеллектуальные системы, искусственный интеллект, ChatGPT, этика, этический кодекс, академическая честность

В статье раскрываются возможности и угрозы, связанные с использованием искусственного интеллекта в сфере высшего образования. Авторы выделяют этические риски, возникающие в условиях недостатка контроля за использованием интеллектуальных систем в вузе. В статье предлагаются меры по обеспечению академической честности и делается вывод о необходимости разработки этических кодексов, ориентирующих на ответственное и добросовестное применение искусственного интеллекта в процессе обучения студентов.

**I.V. Golovina<sup>1</sup>, T.Ya. Alexandrova<sup>2</sup>**

#### **ARTIFICIAL INTELLIGENCE IN EDUCATION: ETHICAL ASPECT**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Private educational Institution of Higher Education "S.Y. Witte Moscow University",  
Moscow, Russia<sup>2</sup>

Keywords: intelligent systems, artificial intelligence, ChatGPT, ethics, code of ethics, academic integrity

The article reveals the opportunities and threats associated with the use of artificial intelligence in higher education. The authors identify ethical risks arising in conditions of lack of control over the use of intelligent systems in higher education. The article suggests measures to ensure academic integrity and concludes that it is necessary to develop ethical codes that focus on the responsible and conscientious use of artificial intelligence in the process of teaching students.

Технологии на основе искусственного интеллекта, стремительно развивающиеся в последнее десятилетие, демонстрируют высокую эффективность в различных отраслях. В то же время становятся все более очевидными риски, связанные с широким распространением искусственного интеллекта. Если первоначально исследователями

---

высказывались опасения о доминировании машин над людьми и гибели человечества, то теперь все большее внимание привлекают не экзистенциальные, а этические риски использования интеллектуальных систем. Об этом свидетельствует, например, подписание «Кодекса этики искусственного интеллекта», состоявшееся на I Международном форуме «Этика искусственного интеллекта: начало доверия» в 2021 году. Этому предшествовало принятие 193 странами первой мировой Рекомендации об этике искусственного интеллекта. К настоящему времени более 30 ведущих мировых компаний опубликовали корпоративные принципы этики искусственного интеллекта.

Разумеется, принятый в Москве этический кодекс имеет рекомендательный характер, однако налицо осознание ответственности при создании и использовании интеллектуальных систем, стремление создать среду доверенного развития технологий искусственного интеллекта.

Какие же этические риски являются наиболее серьезными? В упомянутых этических кодексах чаще всего речь идет о таких рисках, как безответственное использование персональных данных, нарушение приватности, дискриминация, рост зависимости людей от информационных технологий, ослабление когнитивных способностей пользователей и пр. Разумеется, нейтрализовать эти риски в полном объеме едва ли удастся, однако использование «мягкой силы» в отношении регулирования применения технологий искусственного интеллекта (а кодексы этики искусственного интеллекта как раз и являются таким «мягким» инструментом), может оказаться эффективным в решении этих проблем.

Важно отметить не только сам факт идентификации рисков и обоснование человеко-ориентированного подхода к разработке технологий искусственного интеллекта, но и начавшийся процесс институционализации отношений и взаимодействия всех акторов, включая разработчиков, государство, пользователей. Ведь за подписанием этического кодекса последует создание комиссий по этике, назначение уполномоченных по этике, разработка методик и руководств по соблюдению этических принципов, ведение публичного реестра компаний и организаций, поддерживающих кодексы этики. Другими словами, процесс использования новых информационных технологий войдет в нормативное русло, укоренятся «правила игры», построенные на гуманистических принципах. Сказанное, безусловно, относится и к сфере образования, где также наблюдается активное внедрение технологий искусственного интеллекта и, помимо уже известных, обнаруживаются новые этические риски и проблемы, специфичные именно для образовательного процесса. Речь, в частности, идет об использовании программы ChatGPT, появившейся в конце 2022 года и уже набравшей более 100 миллионов пользователей. Возможности ChatGPT, особенно его новой версии ChatGPT-4, таковы, что более 1000 экспертов, включая Илона Маска и Стива Возняка, выступили с призывом приостановить разработки в этом направлении, пока не будут созданы протоколы безопасности, чтобы искусственный интеллект можно было надежно контролировать.

Популярность ChatGPT в образовательной сфере объясняется тем, что он способен создавать эссе, конспекты лекций, резюме научных статей и даже компьютерные коды. Тем самым появляются новые возможности для оптимизации образовательного процесса за счет сокращения времени на рутинную деятельность, автоматизации функций контроля и мониторинга различных показателей и т.п. Кроме того, как отмечают эксперты, новый ресурс может быть использован для перехода к личностно-ориентированному обучению, к решению проблемы индивидуальной образовательной траектории для каждого студента.

Однако, наряду с очевидным потенциалом использования моделей искусственного интеллекта, выявились и проблемы, которые, как представляется, требуют безотлагательного решения, поскольку затрагивают этические принципы образования. Прецедент выполнения и успешной защиты выпускной квалификационной работы с использованием ChatGPT в одном из московских вузов вызвал острые дискуссии среди академического сообщества и привел к осознанию неготовности высшей школы к

---

принятию новых цифровых реалий. Работа была выполнена буквально за сутки и содержала более 80% оригинального текста. При этом работа будущего бакалавра свелась главным образом к тому, чтобы корректно формулировать запросы и редактировать текст, сгенерированный искусственным интеллектом.

В связи с этим прежде всего возникает вопрос об авторстве подобной работы. В самом деле, кому может принадлежать текст, почти не содержащий плагиата? На этот вопрос пока не найден однозначный ответ, однако, совершенно очевидно, что этим автором никак не может быть пользователь модели искусственного интеллекта. Возвращаясь к выполненному с помощью ChatGPT диплому, следует заметить, что стандартными критериями оценивания выпускной квалификационной работы являются оригинальность и новизна полученных результатов, степень самостоятельности и творческого участия студента, уровень и новизна задач и пр. Этим критериям подобная работа явно не отвечает. Разумеется, определенный объем интеллектуальных усилий был им затрачен, но отражает ли созданная нейросетями дипломная работа степень сформированности профессиональных компетенций? Свидетельствует ли сгенерированный текст о готовности выпускника к профессиональной деятельности в конкретной области? Едва ли. В данном случае можно оценивать разве что цифровые компетенции студента, его умение работать с информационными технологиями и владение промптингом, т.е. умением грамотно формулировать поисковые запросы.

Возникают и другие вопросы, например: подлежат ли процедуре защиты подобные работы, особенно если их выполнение с помощью интеллектуальных систем станет распространенной практикой? Не имеем ли мы дело с новыми формами академического обмана, если государственная экзаменационная комиссия не поставлена в известность об участии чат-ботов в выполнении дипломной работы? Не открываются ли новые возможности для околотовузовского теневого бизнеса по выполнению различных письменных работ, включая дипломы?

С сожалением приходится констатировать, что риски академической недобросовестности могут усилиться на фоне отсутствия должного контроля за использованием нейросетей в образовательном процессе. Тем более, что, по мнению экспертов, чат-боты с искусственным интеллектом способны выдавать в ответ на запросы тенденциозные тексты, поскольку разработчики, занимающиеся машинным обучением, могут привнести собственную предвзятость, что вызовет искажение информации. Возможна и откровенно ложная информация, ссылки на несуществующие источники, устаревшие данные и т.п. Как итог — пользователь перестает различать правду и ложь, поддается нежелательному, подчас вредоносному идеологическому влиянию, перестает развивать собственные поисковые навыки и умения, полагаясь на искусственный интеллект.

Справедливости ради стоит отметить, что генеративный искусственный интеллект более успешно справляется с теоретической частью дипломной работы, да и любой письменной работы, где раскрываются ключевые понятия, характеризуется методология, делается обзор точек зрения по избранной проблематике. Что касается практической части, то здесь возможности искусственного интеллекта ограничены, поскольку для этой части требуется первичная информация, собранная студентом самостоятельно, например, на основе эксперимента, наблюдений во время производственной практики, социологических опросов, интервью, анализа отчетности конкретного предприятия и пр. Подобные задачи искусственному интеллекту пока недоступны, во всяком случае, как показал опыт с использованием ChatGPT, с практическими аспектами дипломной работы искусственный интеллект справляется гораздо менее успешно, хотя бы потому, что он обучен на данных предшествующих периодов, да и объем этих данных едва ли простирается до уровня конкретного предприятия, являющегося объектом изучения в дипломной работе. Представляется, что данным этапе генеративный искусственный интеллект обеспечивает главным образом репродуктивное обучение, которое все еще

---

востребовано в современном образовании, однако приоритет все же за продуктивными методами, требующими более активных интеллектуальных усилий, нежели обращение к чат-боту за готовыми резюме тех или иных статей.

Итак, назрела необходимость определить критерии добросовестной работы с помощью искусственного интеллекта. Разумеется, ограничением доступа или запретом на использование ChatGPT (а к этому уже прибегают в ряде стран) проблему не решить. Однозначно объявлять мошенничеством и плагиатом работы, выполненные с применением чат-бота, тоже, вероятно, не стоит. Обучение очередной версии ChatGPT сейчас приостановлено, но это отнюдь не означает моратория на применение интеллектуальных систем в образовании со всеми сопряженными с этим этическими рисками.

Наиболее трудной задачей является выявление плагиата в выпускных квалификационных работах. Обычно вузы требуют не менее 70-80% оригинального текста, хотя юридически эта норма нигде не закреплена. Однако проверка текста, сгенерированного нейросетями, на наличие заимствований, окажется абсолютно бесполезной. Формальное требование будет соблюдено, а фактически подобная работа окажется стопроцентным плагиатом. В принципе, любой текст, выполненный генеративным интеллектом, по определению является плагиатом. В подобном тексте не находит отражения авторская позиция, поскольку искусственный интеллект обучался на множестве текстов, принадлежащих разным авторам. Дело даже не в том, что создается текст, не имеющий конкретного автора. Хуже, что в сознании студента, представляющего подобный текст к защите, будь то курсовая или дипломная работа, размываются различия между собственным вкладом и чужими идеями. Тем самым академический обман обретает новую почву, укореняется как допустимая норма поведения, а стандартные контрольные процедуры в вузе фактически скомпрометированы.

Разумеется, проблема авторства текста, сгенерированного искусственным интеллектом, не решается только в академических стенах, тем более что и в правовом отношении полная ясность здесь отсутствует. Однако, совершенно очевидно, что на нынешнем этапе необходимо обеспечивать информирование всех участников образовательной деятельности, включая преподавателей и студентов, об использовании технологий искусственного интеллекта как при выполнении письменных работ, так и при проведении контрольных процедур.

Исчерпали ли себя письменные работы — рефераты, эссе, курсовые и, наконец, дипломные работы, — как средства контроля за успеваемостью и освоением заданных стандартом компетенций? Безусловно, если использование искусственного интеллекта в образовании приобретет массовый характер, то, вероятно, сам формат обучения в высшей школе будет существенно пересмотрен. Это не отменяет необходимости уже сегодня искать такие пути интеграции интеллектуальных систем в процесс обучения, которые по возможности не нарушали бы принципов академической честности.

В первую очередь необходимо активнее развивать академическую культуру, разрабатывать этические кодексы, четко очерчивающие границы этического и неэтического поведения, в том числе при работе с искусственным интеллектом. Академические ценности не должны навязываться участникам образовательного процесса; этические кодексы следует разрабатывать и принимать при участии как студентов, так и преподавателей. Практика подобного рода имеется, однако во многих случаях ценностные ориентиры в таких кодексах подменяются общими правилами поведения в вузе и носят формальный характер.

Далее, необходимо изменить подход к разработке тематики письменных работ, которая носит рутинный характер и обычно переутверждается из года в год в неизменном виде. Речь идет не просто об усложнении заданий, а об их актуализации, увязке с современными реалиями и потребностями сегодняшней, а не вчерашней практики. Кроме того, следует усилить поисковую направленность тем письменных работ с тем, чтобы

---

стимулировать интеллектуальную деятельность студента. Наконец, все письменные работы, включая рефераты и эссе, должны подлежать защите на практическом занятии или во время специальной процедуры с тем, чтобы можно было полноценно оценить собственный вклад студента в создание работы. От преподавателя, заинтересованного в преодолении академического обмана, потребуется довольно серьезная работа по обновлению заданий и критериям их оценивания.

Перечисленные меры носят тактический характер; их эффективность может проявиться скорее в краткосрочном периоде. В перспективе же необходима разработка стратегии, предусматривающей развитие и реформирование высшего образования в свете новых вызовов, связанных с активным проникновением генеративных интеллектуальных систем.

#### СПИСОК ЛИТЕРАТУРЫ

1. Национальная стратегия развития искусственного интеллекта на период до 2030 года. — <https://base.garant.ru/72838946/>
2. Кодекс этики в сфере искусственного интеллекта. — <https://ethics.a-ai.ru/>
3. Гамбеева Ю.Н., Глотова А.В. Искусственный интеллект как часть концепции современного образования: вызовы и перспективы // Известия Волгоградского государственного педагогического университета. — 2021, № 10, с. 10-16.
4. Головина И.В., Александрова Т.Я. Качество высшего образования: взгляд изнутри // Научно-практический журнал: Наука и образование: хозяйство и экономика; предпринимательство; право и управление. — 2020, № 4 (119), с. 58-68, <http://www.journal-nio.com/images/2020/4-119.pdf>
5. Ивахненко Е.Н., Никольский В.С. ChatGPT в высшем образовании и науке: угроза или ценный ресурс // Высшее образование в России. — 2023, № 4, с. 9-22.
6. Резаев А.В., Трегубова Н.Д. Искусственный интеллект в университетах: какое будущее нас ожидает? // Высшее образование в России. — 2023, № 6, с. 19-37.

**Я.Б. Константинова, О.А. Бадёрная, Ю.Д. Кокоулина**

#### **ВЛИЯНИЕ СТРУКТУРНЫХ ДЕФЕКТОВ НА СТЕПЕНЬ РАЗМЫТИЯ ФАЗОВЫХ ПЕРЕХОДОВ В СЕГНЕТОЭЛЕКТРИКАХ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: сегнетоэлектрики, переход, дефекты, дислокации, домены

В статье обсуждаются результаты исследования сегнетоэлектриков с размытым фазовым переходом. Показано, что существенными факторами, влияющими на размытие фазовых переходов, являются структурные дефекты и связанные с ними доменные и межфазные границы.



## INFLUENCE OF STRUCTURAL DEFECTS ON THE DEGREE OF BLURING OF PHASE TRANSITIONS IN FERROELECTRIC

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: ferroelectrics, transition, defects, dislocations, domains

The article discusses the results of a study of ferroelectrics with a diffuse phase transition. It is shown that structural defects and associated domain and interfacial boundaries are significant factors affecting smearing.

В настоящее время сегнетоэлектрические материалы находят широкое применение в различных областях науки и техники. Изучению факторов, влияющих на их свойства, посвящено много работ. В частности, в качестве критерия, на основании которого анализируют технические свойства сегнетоэлектриков, используют анализ степени размытия сегнетоэлектрического фазового перехода (ФП). В области ФП поведение диэлектрической проницаемости подчиняется закону Кюри-Вейсса крайне редко. Это связано с особенностями реальной структуры сегнетоэлектриков, приводящей к размытию ФП. Рассмотрим, как влияют структурные дефекты на размытие ФП.

Существует ряд факторов, приводящих к появлению локальных неоднородностей структуры и влияющих тем самым на ФП в сегнетоэлектриках. Одним из них является наличие протяженных структурных дефектов (микрореформаций) в кристаллической решетке. Структурные дефекты являются очагами возникновения межфазных и доменных границ, отличающихся по составу и свойствам, в том числе, по величинам температуры Кюри и константы Кюри-Вейсса, что приводит к расширению пика зависимости диэлектрической проницаемости от температуры и влияет на сегнетожесткость образцов.

В работе /1/ рассмотрен вклад в диэлектрические и пьезоэлектрические свойства движущихся сегнетоэлектрических доменных границ и их взаимодействие с локальными электрическими полями дислокаций. На основе исследования пьезокерамики ЦТС делается вывод, что увеличение количества дислокаций и их локальных полей, снижая подвижность доменных стенок, приводит к росту сегнетожесткости материала. При увеличении степени сегнетожесткости повышается значение точки Кюри. В реальном сегнетоэлектрике распределение плотности дислокаций неоднородно по объему. Поэтому эффект от взаимодействия доменных стенок с полями дислокаций (в данном случае сдвиг точки Кюри) в различных микрообластях будет различный. Появится (или увеличится) разброс значений по микрообластям, и, как следствие, увеличится размытие ФП. Следовательно, величина размытия ФП в сегнетоэлектриках должна зависеть от количества доменных стенок и числа дислокаций в единице объема.

BaTiO<sub>3</sub> в качестве объекта исследования /2/, позволил исключить влияние возможных в соединениях типа АВ<sup>п</sup>В<sup>п</sup>О<sub>3</sub> эффектов упорядочения и флуктуаций состава, о которых упоминалось в работе /3/.

Существенен вклад в диэлектрические и пьезоэлектрические свойства движущихся сегнетоэлектрических доменных границ и их взаимодействие с локальными электрическими полями дислокаций. На основе исследования пьезокерамики ЦТС можно заключить, что увеличение количества дислокаций и их локальных полей, снижая подвижность доменных стенок, приводит к росту сегнетожесткости материала. При увеличении степени сегнетожесткости повысится значение точки Кюри. В реальном сегнетоэлектрике распределение плотности дислокаций неоднородно по объему. Поэтому эффект от взаимодействия доменных стенок с полями дислокаций (в данном случае сдвиг температуры Кюри) в различных микрообластях будет различный. Появится (или

---

увеличится) разброс значений температуры Кюри по микрообластям, и, как следствие, увеличится размытие ФП. Следовательно, величина размытия ФП в сегнетоэлектриках должна зависеть от количества доменных стенок и числа дислокаций в единице объема.

Сегнето-антисегнетоэлектрическое взаимодействие также оказывает влияние на характеристики ФП. Взаимодействие сосуществующих сегнетоэлектрической и антисегнетоэлектрической фаз должно приводить к повышению точки Кюри в локальных объемах кристалла, на которые оно распространяется. Экспериментально это явление было обнаружено в твердых растворах ЦТСЛ и ЦТС.

Высокотемпературные отжиги сегнетоэлектрической керамики на основе ЦТСЛ и ЦТС ведут к изменению структурных параметров керамики в сегнетоэлектрическом состоянии. Характерной особенностью этих изменений является появление тетрагональных перовскитовых фаз с большой спонтанной деформацией и малым объемом элементарных ячеек. Наличие весовых потерь наряду с изменением структурных параметров дает основание полагать, что обнаруженные эффекты связаны с переходом оксида свинца в свободное состояние в процессе отжига.

Оксид свинца является весьма летучим соединением. При определенных термодинамических параметрах уже при нагреве до  $700^{\circ}\text{C}$  его весовые потери могут оказаться весьма значительными. В нашем случае твердого раствора оксидов перовскитовой структуры заметные изменения веса образцов начали наблюдаться после отжига при температурах  $800-900^{\circ}\text{C}$ . Одновременно с этим, регистрировались изменения перовскитовой структуры на поверхности образцов. Они заключались, в частности, в увеличении процентного содержания тетрагональной фазы (по сравнению с ромбоэдрической фазой), а также в появлении новых тетрагональных фаз. Причина наблюдаемых структурных изменений заключена в испарении из поверхностных слоев керамики оксида свинца  $\text{PbO}$ .

На рисунке 1 представлены результаты исследований изменения физических свойств образцов от температуры отжига (Тотж). Как можно видеть, интенсивные потери веса  $P$  керамических образцов (на рисунках приведены данные по весовым потерям, усредненные по партиям из 10 образцов) начинаются после отжига при Тотж  $>850^{\circ}\text{C}$ . Кроме того, наблюдаются изменения температуры максимума диэлектрической проницаемости  $T_m$  и диэлектрической проницаемости при этой температуре  $\epsilon(T_m)$ . Кроме того, здесь же представлены зависимости параметра размытия ФП  $\Delta$  от Тотж. С ростом Тотж, начиная с не которых пороговых температур, во всех изученных керамиках наблюдается тенденция к увеличению размытия ФП и уменьшению  $\epsilon(T_m)$ , в зависимостях  $T_m$  (Тотж) имеется небольшой минимум, после которого имеет место резкое (на  $30-40^{\circ}\text{C}$ ) увеличение  $T_m$ .

Следует отметить, что обсуждаемые изменения физических свойств, происходящие в образце в процессе отжига однозначно связаны со структурными изменениями. Начиная с некоторых Тотж по дифрактограммам можно сделать вывод о появлении в образцах несвязанного оксида  $\text{ZrO}_2$ .

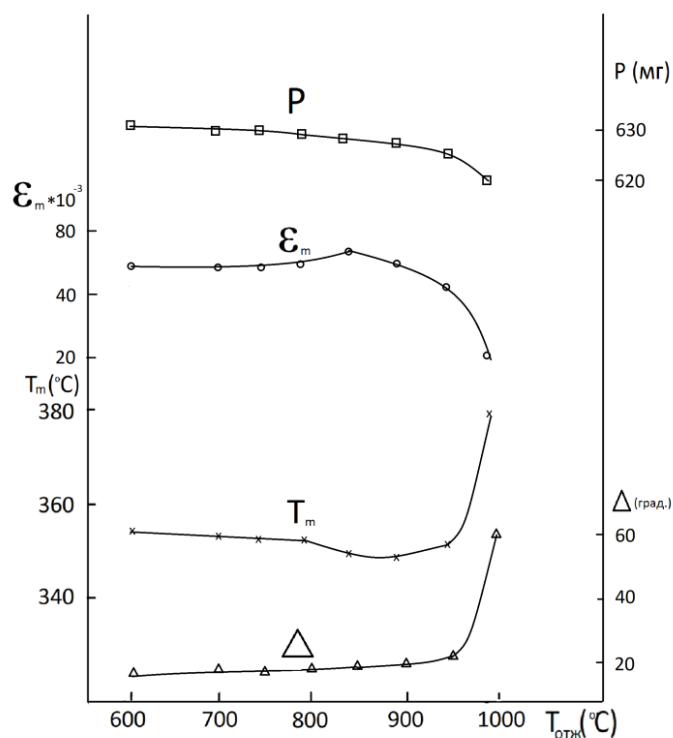


Рисунок 1

Увеличение содержания структурных дефектов, доменных и межфазных границ вносит локальные изменения в свойства кристаллов по их объему. Деление сегнетоэлектрика на микрообласти, связанное с отклонением от идеального дальнего порядка или флуктуациями концентраций дополняется уменьшением размеров микрообластей благодаря локальным структурным неоднородностям.

#### СПИСОК ЛИТЕРАТУРЫ

1. Константинов Г.М., Рыбнянец А.Н., Швецова Н.А., Константинова Я.Б. Взаимосвязь структурных дефектов и технологических режимов приготовления сегнетокерамик на основе ЦТС.// Сборник трудов XX Всероссийской конференции по физике сегнетоэлектриков, 18-22 августа 2014 г., Красноярск, ИФ СО РАН с. 181.
2. Михайлов М.М., Алексеева О.А., Юрьев С.А. и др. Фазовые переходы и спектры диффузного отражения твердых растворов титаната-цирконата бария. // СПбГПУ, физико-математические науки 14(2) 2021, с.16-25.
3. Константинова Я.Б., Константинова М.Г. Влияние композиционного порядка и флуктуаций состава на степень размытия сегнетоэлектрических фазовых переходов./ СТАНОВЛЕНИЕ И РАЗВИТИЕ НОВОЙ ПАРАДИГМЫ ИННОВАЦИОННОЙ НАУКИ В УСЛОВИЯХ СОВРЕМЕННОГО ОБЩЕСТВА.// Сборник статей Международной научно-практической конференции. Уфа, 2023. С. 12-15.

## ОСОБЕННОСТИ ЗАРУБЕЖНЫХ ПРОГРАММ БЕЗОПАСНОСТИ ТРУДА

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: программа безопасности, уровни программы.

Приведен анализ программ безопасности на зарубежных предприятиях. Показано, что наибольшего успеха добиваются при использовании программ с наибольшим числом уровней.

E.A. Bineev

## FEATURES OF FOREIGN LABOR SAFETY PROGRAMS

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Key words: security program, program levels.

The analysis of security programs at foreign enterprises is given. It is shown that the greatest success is achieved when using programs with the largest number of levels.

Анализ зарубежных информационных и научных материалов показывает [1-3], что профилактическая текущая и долговременная работа по обеспечению безопасных и здоровых условий труда строится на простой экономической формуле: расходы на выполнение трудоохранных программ всегда меньше, чем выплаты по последствиям несчастных случаев, производственно обусловленной заболеваемости и аварий. Таким образом, расходы на охрану труда не снижают прибыль, а экономят ее. Из этого вовсе не следует, что за рубежом нет проблем ни с травматизмом, ни с заболеваемостью, ни с авариями. Но на подавляющем большинстве предприятий названная формула работает и приносит свои плоды.

Важнейшим принципом совокупного опыта является понимание, что простых причин несчастных случаев и аварий не существует, а есть сложные взаимосвязанные причины. Как аксиома работает так же принцип комплексности решений: нельзя добиться успеха в оздоровлении производственной среды простыми, отдельными средствами - нужен комплекс мер. Основным плановым документом в связи с этим является программа безопасности на предприятии. Программа безопасности всегда мотивирована. Ею ставятся конкретные цели: снизить травматизм с такого-то до такого-то уровня, а не планируется работа вообще. То есть, профилактическая работа имеет свой измеритель, равно как и собственно производство.

Успех программы безопасности на предприятиях во многом зависит от широты спектра применяемых мер стимулирования безопасности труда. Очень интересно, что рабочих и специалистов поощряют также за внесенные предложения по совершенствованию безопасности, за групповые достижения. Другими словами, поощряется взаимный контроль и ответственность работающих. Собственно меры стимулирования самые разные: от бесплатного кофе с печеньем до ценных подарков, включая часы, посуду, настольные лампы, куртки, радиоприемники, телевизоры. Денежные премии выдаются редко. Установлено, что эффективность стимулирования денежными суммами значительно уступает эффекту от вещевого подарка. Хорошие результаты дает и такая составляющая морального стимулирования, как приглашение членов семьи на церемонию вручения подарков.

---

Однако, как показывает опыт, не все программы, даже разработанные квалифицированно, оказываются эффективными. В то же время, на некоторых предприятиях, не имеющих четко выраженных программ, имеются положительные результаты по снижению травматизма. Почему же это происходит? Проведенные американскими учеными исследования позволили выявить иерархическую зависимость между отдельными элементами программ. Наибольшего успеха добиваются те предприятия, где используют программы, состоящие из наибольшего числа элементов (уровней).

Программу безопасности в этом случае представляют графически, в виде пирамиды. Основанием ее является участие администрации в реализации программы, которое должно быть постоянным, поскольку без него любому мероприятию по безопасности будет отводиться мало времени, материальных средств и других ресурсов.

На втором по значимости уровне стоит ответственность специалистов за безопасность на предприятии и в подразделении; их административные полномочия для действий в этой области; перечень отчетной документации. Отчетность необходима для оценки работы подразделений по безопасности труда.

Третий уровень определяет цели и конкретные рубежи. Показатели безопасности должны быть измеримы и иметь смысл для всех, кого они касаются. Они могут выражаться, например, в виде снижения частоты аварий, случаев травмирования или в виде числа необходимых мероприятий - контрольных проверок, собраний, анализов уровней опасности и т.п.

Следующий уровень - наличие ресурсов: времени, оборудования, денежных средств, квалифицированных кадров, необходимых для разработки программы, ее реализации и совершенствования.

На следующем уровне ("мотивация") внимание уделяется системе поощрений и наказаний для того, чтобы стимулировать безопасную работу. Для успешной мотивации безопасной работы необходимо усвоить два принципа:

1. Люди не станут намеренно рисковать в работе, т.е. если человек нарушил правила безопасности, значит им руководили мотивы более сильные, чем страх получить травму. Эти мотивы необходимо выяснить и устранить;
2. Факторы стимулирования должны способствовать удовлетворению запросов работников. Один предпочитает материальное поощрение, для других более важно общественное признание их достижений и т.д.

Последняя функция в работе по безопасности - контроль эффективности каждого отдельного элемента программы и обеспечение обратной связи для доведения результатов до соответствующего уровня административного управления предприятием, чтобы поддержать и усилить эффективность программы.

## СПИСОК ЛИТЕРАТУРЫ

1. Безопасность и охрана труда: Учебное пособие для вузов / Под редакцией О.Н. Русака.- СПб.: Изд-во МАНЭБ,2001.- 279с.
2. Бинеев Э.А. Безопасность и охрана труда в пищевой промышленности: Учебное пособие для вузов.- Ростов н/Д: Изд-во Ростовского университета, 2004.- 352с.
3. Бинеев Э.А., Бородин А.В., Попова В.П. Безопасность жизнедеятельности. Курс лекций: Учебное пособие для вузов.- 2-е изд.- Ростов н/Д: СКФ МТУСИ, 2018.- 268с.

## ФИЛОСОФИЯ УСТОЙЧИВОСТИ И РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Федеральное государственное бюджетное образовательное учреждение высшего образования "Ростовский государственный экономический университет (РИНХ)",  
Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: компьютерные науки, инновационные открытия, философия устойчивости.

В статье рассматриваются крупные инновации, произошедшие в период с конца 20-го по начало 21-го века, которые представляют собой как технологии, в разработке которых принимали непосредственное участие ученые-информатики, так и технологии, в которых ученые-информатики сыграли важную вспомогательную роль, разработав управляющее программное обеспечение.

N.I. Zabarenko<sup>1</sup>, Yu.A. Petrova<sup>1,2</sup>

## THE PHILOSOPHY OF SUSTAINABLE DEVELOPMENT AND INFORMATION TECHNOLOGIES

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Federal State Budget Educational Institution of higher education "Rostov-on-Don State  
University of Economics", Rostov-on-Don, Russia<sup>2</sup>

Keywords: computer science, innovative discoveries, sustainability philosophy.

The article deals with the problem of huge innovations happened at the period from the end of 20th century until the beginning of 21st century, that were both technologies in development of which the IT scientists had participated directly and technologies in development of which the IT scientists had participated at an important auxiliary role by developing its controlling software.

В основе информатики лежит обработка информации на цифровых компьютерах и, возможно, на квантовых компьютерах в недалеком будущем. Фокусируясь на разработке алгоритмов для решения сложных задач, информатика решает два типа проблем: те, которые можно решить путем вычислений, и те, которые таким образом решить нельзя. Для решения проблемы первого типа необходимо описать вычислительную процедуру, которая ее решает. Для рассмотрения второго типа необходимо показать, что такой процедуры не существует. Обычно это предполагает доказательство математической теоремы о том, что рассматриваемая проблема не может быть решена вычислительным путем. Если взять инновации в области информатики с конца 20 века и до наших дней, в разработке которых принимали непосредственное участие ученые-информатики, мы получим внушительный перечень. Это, к примеру, интернет, широкополосный доступ, WWW (браузер и HTML), ПК и портативные ПК, электронная почта, офисное программное обеспечение (таблицы, текстовые процессоры), программное обеспечение и услуги с открытым исходным кодом (например, Linux, Wikipedia), интернет-магазины/электронная коммерция/аукционы (например, eBay), сжатие информации (jpeg, mp3), цифровая фотография/видеосъемка, социальные сети и многое другое.

---

Ученые-информатики сыграли важную вспомогательную роль в разработке программного обеспечения для таких технологий, как мобильные телефоны, МРТ, тестирование и секвенирование ДНК, микропроцессоры, роботизированная хирургия и т.д. Большинству инновационных открытий не существовало бы без информатики. За последние несколько десятилетий по всему миру стало понятно, что инновации существенно изменили и улучшили общество, в котором мы живем, и они стали неотъемлемой частью развития общества, так как с их помощью масштаб возможностей решения проблем также сильно увеличился. Говорят, что «лучший способ предвидеть будущее – создать его», и это лучшее объяснение всей важности инноваций в таких областях, как робототехника, компьютерное зрение и обработка компьютером естественного языка, машинное обучение, теории нейронных сетей, передача информации и облачные сервисы, Triple Play и многое другое [1].

Рассматривая инновационные разработки вне контекста, следует отметить, что, в отличие от изобретений, «инновации – это реализации новых идей с экономической и социальной стороны» [2]. Поэтому ценность инновационной деятельности зависит от максимальной экономической выгоды. Способствуя обеспечению устойчивости при разработке и внедрении инноваций, компании могут создавать продукты, услуги и процессы, приносящие пользу как обществу, так и организациям. Заметность изменения окружающего мира является сегодня актуальным вопросом, стоящим перед человечеством. С использованием Интернета эти изменения происходят намного быстрее. Мы живем во время эпохальных преобразований, которые имеют далеко идущие масштабы [3].

Инновации не приходят сразу. Правительства и организации ежегодно инвестируют значительные средства в исследования и разработки, научные публикации и другие области исследований в целях стимулирования инноваций. Такие гиганты, как Amazon, Microsoft Corporation, Сбербанк, добились значительных успехов благодаря своей философии инвестирования в искусственный интеллект.

Дифференцирование инноваций по приоритетности достижения экономической, экологической и социальной устойчивости, ставшее философией новаторов-разработчиков, «может избавить человечество от антропологической катастрофы исчезновения жизни на планете Земля» [4].

Например, капсульные кофемашины, позволяющие получить кофе по одному нажатию кнопки, качеством как в кофейне или кафе, но при этом не выходя из дома. Они чрезмерно популярны, но по подсчетам экспертов, как результат – каждую минуту в мире на свалках оказываются 29 000 пластиковых капсул [5]. «Устойчивые инновации» выявляют и учитывают такие социальные и экологические факторы. Это значит, что компании могут поставлять товары и услуги, которые хороши и для них, и для общества в долгосрочной перспективе. Устойчивые инновации подразумевают преднамеренное внесение изменений в товары, услуги и процессы компании с учетом долгосрочной пользы для общества и окружающего мира при извлечении экономической выгоды для компании. Это определение предложил исследователь Ричард Адамс на основе академических и промышленных исследований на данную тему.

Устойчивые инновации влияют на товары и услуги следующим образом:

1. Они создают новые товары и услуги. Благодаря устойчивым инновациям компании могут изобретать и предлагать совершенно новые конечные продукты и системы, которые вносят значительный вклад в достижение устойчивости. Хорошим примером этого является разработка «Bio-bean», экологичного биотоплива из кофейных отходов, которым питают лондонские двухэтажные автобусы [6].

2. Они меняют оперативные процессы. Устойчивая инновационная деятельность не сводится лишь к изобретению новых товаров и услуг. Компании могут также заниматься устойчивой инноватикой над существующими товарами и услугами,

---

изменяя процессы их производства. Эти изменения могут происходить в разных сферах. Например, голландский производитель электроники «Fairphone», который разрабатывает и производит смартфоны с расчетом на меньший экологический след и более благоприятный социальный эффект, в сравнении со средними показателями в данной отрасли промышленности [7]. Они используют переработанные и ответственно добытые материалы, чтобы предоставить работникам честную зарплату и хорошие условия труда. Следует отметить, что компания продумывает свои устройства до последней детали, поскольку их продукция вырабатывает на 80% меньше отходов.

Сравнительный анализ инновационных достижений наглядно демонстрирует достижения и перспективы философии устойчивости и развитие инновационных технологий. Города являются ключевыми системами для глобального экономического роста, а также являются движущими силами деградации окружающей среды, влияя на баланс между людьми и естественными системами [8]. Финансирование разработок и внедрения инноваций жизненно важны для роста и выживания компаний. Фирмы, не занимающиеся инновациями, остаются позади конкурентов и рано или поздно приходят к банкротству. С другой стороны, традиционные виды инноватики могут обеспечивать прибыльные продукты и услуги для компаний, но в то же время оказывать негативное воздействие как на здоровье персонала, так и на окружающую среду в целом, а также злоупотреблять природными ресурсами.

#### СПИСОК ЛИТЕРАТУРЫ

1. Reshetnikova I.V. To the question of Triple Play / I.V. Reshetnikova, V.A. Chuchupalova, N.O. Svetlichnaya // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2015, No. 2, p. 326-327, EDN VJGSAF.
2. Шумпетер Й. Теория экономического развития. Капитализм, социализм и демократия. (перевод с англ. Capitalism, Socialism, and Democracy, 1934). – М.: Эксмо, 2008. 2007, 864 с.
3. Петрова Ю.А. Трансформации в культурах в период глобализации под влиянием информационных технологий / Ю.А. Петрова // Язык и коммуникация в второй культуре: Материалы международной научно-практической онлайн-конференции, Ростов-на-Дону, 21 апреля 2021 года. – Ростов-на-Дону: Ростовский государственный экономический университет «РИНХ», 2021, с. 32-34, EDN LWRVTH.
4. Petrova Yu.A. Environmental intelligence and value orientations of youth towards innovation in achieving sustainable development goals, International Journal of Human Capital in Urban Management. – 2023, vol. 8, No. 2, p. 291-302. – DOI 10.22034/IJHCUM.2023.02.10, EDN CIJYJD.
5. Кофейные капсулы разлагаются около 500 лет. Эксперты называют их «ненужным одноразовым продуктом», 2021. [Электронный ресурс], URL: <https://www.techinsider.ru/science/news-758153-kofeynye-kapsuly-razlagayutsya-okolo-500-let-eksperty-nazyvayut-ih-nenuzhnym-odnorazovym-produktom/>
6. Учёные нашли шесть новых способов применения кофейной гущи. В том числе в качестве топлива, 2021. [Электронный ресурс], URL: <https://tea.ru/article/uchenyenashli-shest-novykh-sposobov-primeneniya-kofeynoy-gushchi-v-tom-chisle-v-kachestve-topliva/>
7. Голландская компания Fairphone создала экологичный смартфон, который легко отремонтировать, 2021. [Электронный ресурс], URL: <https://incrussia.ru/news/ekologichnyj-smartfon-fairphone/>



- 
8. Petrova Yu., Dzhioeva D., Edilsultanova L. The role of youth leadership in achieving sustainable development, environmental safety / AIP Conference Proceedings 2021 года. – Грозный, 2021, P. 060001. – DOI 10.1063/5.0075301.

**Е.В. Агаркова**

## **АНАЛИЗ ДАННЫХ УЧЕБНОГО ПРОЦЕССА В ОБРАЗОВАНИИ**

Донской государственный технический университет,  
Ростов-на-Дону, Россия

Ключевые слова: анализ данных, образование, статистика, машинное обучение, тренды, визуализация.

В статье проведено теоретическое исследование, основанное на внедрении анализа данных в современную систему образования. Описываются популярные аспекты внедрения системы анализа, а также производится обзор методов, помогающих реализации анализа данных. В результате за счет описания каждого инструмента и его влияния на систему образования делается вывод о пользе анализа данных в процессе обучения и создания методических программ.

**E.V. Agarkova**

## **DATA ANALYSIS OF THE EDUCATIONAL PROCESS IN EDUCATION**

Don State Technical University,  
Rostov-on-Don, Russia

Keywords: data analysis, education, statistics, machine learning, trends, visualization.

The article presents a theoretical study based on the introduction of data analysis into the modern education system. The popular aspects of the implementation of the analysis system are described, as well as an overview of methods that help implement data analysis. As a result, due to the description of each tool and its impact on the education system, a conclusion is made about the benefits of data analysis in the learning process and the creation of methodological programs.

В настоящее время образование является одним из ключевых факторов в развитии общества. Однако, для обеспечения высокого качества образования и успешного развития учащихся, необходимо иметь доступ к достоверным и полезным данным. Анализ данных в образовании представляет собой мощный инструмент, который позволяет собирать, анализировать и интерпретировать данные, связанные с образовательными процессами. Одной из главных проблем, которую можно решить за счет анализа данных, является низкая успеваемость учащихся в определенных предметах. Она может быть вызвана различными факторами, такими как неэффективные методы обучения, недостаточное количество образовательных ресурсов или отсутствие персонализированного подхода к обучению. Анализ данных в образовании позволяет выявить проблемные дисциплины и определить причины низкой успеваемости, чтобы разработать соответствующие стратегии и методы для их решения. За счет данного подхода можно поднять уровень знаний учащихся, разработав соответствующие планы обучения, чтобы улучшить образовательный процесс.

---

Цель статьи – показать, как анализ данных в образовании может помочь нам принимать обоснованные решения и улучшать образовательные процессы для всех учащихся. Задачей является рассмотрение различных аспектов анализа данных в образовании, таких как анализ успеваемости, анализ прогресса учеников, анализ посещаемости. Также в теоретическое исследование входит обзор различных инструментов и методов, которые можно использовать для анализа данных в образовании, такие как статистический анализ, машинное обучение и визуализация данных.

Анализ – преобладание данных в выводах, на основе которых будут приниматься решения и строиться действия с помощью людей, процессов и технологий [1]. Анализ данных является важным этапом в исследованиях. Он позволяет извлечь ценную информацию и понять скрытые закономерности и взаимосвязи, помогает принять обоснованные решения, определить тренды и предсказать будущие события. Анализ данных также позволяет проверить гипотезы и подтвердить или опровергнуть предположения. Благодаря чему исследователи могут лучше понять свою аудиторию, улучшить продукты и услуги, а также принимать более эффективные решения на основе фактов и доказательств. Пропустив этап анализа, есть риск исказить выводы, а именно упустить детали, перепутать, к кому из опрошенных пользователей относится полученный факт или запомнить только яркие инсайты, но не проверить, характерны ли они для всех пользователей [2]. Чтобы лучше понять роль анализа данных именно в сфере образования необходимо рассмотреть разного рода аспекты его применения, в основном их выделяют три: успеваемость, прогресс обучения, посещаемость.

Анализ успеваемости студентов является важным аспектом исследования данных в образовании. Он позволяет выявить общую картину успехов учеников, определить тренды и понять, какие факторы могут влиять на успехи или неудачи учащихся. Чтобы провести анализ успеваемости, необходимо собрать и структурировать данные об успехах студентов, а затем применить различные статистические методы и визуализации для их интерпретации.

Анализ прогресса учеников помогает оценить их развитие и рост в процессе обучения. Этот аспект анализа в образовании позволяет определить, какие ученики демонстрируют наибольший прогресс, какие области знаний требуют дополнительного внимания, а также оценить эффективность образовательных программ. Для анализа прогресса учеников необходимо собирать и систематизировать данные о их достижениях, проводить оценки и тесты, а также устанавливать цели и отслеживать их выполнение.

Анализ посещаемости представляет возможность для изучения данных в образовании. Он позволяет определить уровень посещаемости студентов, выявить паттерны пропусков и связать их с успехами или провалами в учебе. Анализ посещаемости может также помочь выявить причины низкой посещаемости и предпринять меры для ее улучшения. Для проведения анализа необходимо регулярно отслеживать посещаемость, записывать данные и использовать соответствующие инструменты или программное обеспечение для анализа этих данных.

Описанные аспекты необходимо учитывать при работе с данными и делать на них акцент. Чтобы реализовать качественную работу анализа данных необходимо применять подходы и методы, которые наилучшим образом соответствуют аналитическим требованиям и обеспечивают достоверность и полезность результатов. Существует множество методов для анализа данных, они могут помочь в извлечении знаний и понимании данных. Однако, важно учитывать, что выбор методов для анализа данных должен быть основан на конкретных целях и требованиях исследования.

В контексте данной работы понятие статистики — значит отрасль практической деятельности, целью которой является сбор, обработка и анализ данных о разнообразных явлениях общественной жизни; полученная в результате статистического исследования информация позволяет решать задачи выявления реально существующих закономерностей, свойственных описываемым процессам и явлениям [3]. Статистический

---

анализ основан на принципах вероятности и статистики, и используется для описания и интерпретации данных, выявления связей и закономерностей, а также для проверки гипотез.

В образовании статистический анализ играет важную роль в понимании и улучшении учебного процесса. Он позволяет получить ценные данные об успеваемости учащихся, эффективности учебных программ и эффективности преподавания. Анализ статистических данных позволяет выявить тренды, понять влияние различных факторов на образовательные результаты и определить области, требующие дальнейшего улучшения. Благодаря статистическому анализу, можно определить сильные и слабые стороны образовательной системы, обозначить проблемные места и разработать целенаправленные стратегии для повышения качества образования. Такой анализ помогает принимать информированные решения на основе данных, а не только интуиции или предположений. Кроме того, статистический анализ в образовании позволяет оценить эффективность внедрения новых методик и технологий, а также сравнивать образовательные программы и системы на основе объективных данных. Он играет важную роль в оценке достижений учащихся, определении образовательных потребностей и разработке индивидуализированных подходов к обучению, помогая понять, как улучшить образовательный процесс и обеспечить наилучшие результаты.

Машинное обучение – это методики анализа данных, которые позволяют аналитической системе обучаться в ходе решения множества сходных задач. Машинное обучение базируется на идее о том, что аналитические системы могут учиться выявлять закономерности и принимать решения с минимальным участием человека [4]. Оно позволяет эффективно обрабатывать и анализировать большие объемы информации, а главное предсказывать образовательные результаты.

Одно из главных преимуществ машинного обучения является его способность работать с различными типами данных, включая текстовую информацию, изображения и аудиофайлы. Это позволяет нам получить более полное представление о процессе обучения и эффективности учебных программ. Оно также помогает автоматизировать процессы сбора и анализа данных, что существенно экономит время и ресурсы. Алгоритмы машинного обучения могут быстро обрабатывать большие объемы информации и выявлять важные тренды и закономерности, которые могут быть незаметны при традиционном анализе. Благодаря этому появилась возможность можем предсказывать успех обучающихся, определять образовательные потребности и разрабатывать индивидуализированные подходы к обучению. Это позволяет эффективно адаптировать учебные программы и методики под потребности каждого студента, обеспечивая наилучшие результаты. Машинное обучение играет более широкую роль в образовательном применении и системе, так как за счет него происходит создание необходимых приложений. Эти приложения могут быть использованы для настройки модуля курса, репетиторства, оценки, определения результатов обучения и даже для прогнозирования карьеры. Адаптивные системы обучения могут быть адаптированы в соответствии с когнитивными навыками и поведением отдельных студентов или группы студентов [5].

Визуализация данных – это наглядное представление массивов различной информации. Визуальная информация лучше воспринимается и позволяет быстро и эффективно донести до зрителя собственные мысли и идеи. Физиологически, восприятие визуальной информации является основной для человека [6]. Визуализация данных играет значимую роль в образовании, предоставляя наглядные и понятные графические представления информации. Это позволяет лучше понять и интерпретировать данные, выявлять тренды, паттерны и важные закономерности.

Визуализация данных дает возможность представить сложные данные в удобной и понятной форме. С помощью графиков, диаграмм и других визуальных элементов можно проще интерпретировать информацию, что помогает учащимся лучше понять и запомнить

---

материал. Анализируя графики и диаграммы, учащиеся могут заметить связи между разными переменными и понять, какие факторы влияют на определенные результаты. Это способствует развитию критического мышления и способности анализировать информацию. Визуализация данных может помочь учащимся развить навыки коммуникации. Представляя свои исследования или результаты в виде графиков и диаграмм, учащиеся могут более ясно и наглядно объяснить свои идеи и выводы другим людям. Таким образом, визуализация данных играет важную роль в образовании, помогая учащимся лучше понимать информацию, анализировать данные и развивать навыки для личностного роста.

Благодаря всем этим методам становится понятно, что применение анализа данных в образовании имеет огромное значение. Конечно, стоит учитывать затратность некоторых моментов, которые необходимы для сбора данных, а также для применения машинного обучения, но в данном случае все усилия будут оправданы. Важно отметить, что с развитием технологий и доступностью инструментов анализа данных, их применение в образовании становится все более доступным и эффективным.

Анализ данных позволяет обнаружить тренды, паттерны и закономерности, которые помогают преподавателям и обучающимся принимать обоснованные решения. За счет грамотного использования имеющихся инструментов можно выявить сильные и слабые стороны в образовательном процессе, а также определить эффективность различных методов обучения. Внедрение анализа данных помогает улучшить качество образования, разработать персонализированный подход к каждому студенту и создать оптимальные условия для их успеха. Таким образом, применение анализа данных в образовании является важным шагом в современной системе образования.

#### СПИСОК ЛИТЕРАТУРЫ

1. Карл Андерсон. Аналитическая культура. От сбора данных до бизнес-результатов. – М.: Манн, Иванов и Фербер, 2017. 336 с.
2. Анализ данных исследования [Электронный ресурс] // Контур Гайды: [сайт]. – URL: <https://guides.kontur.ru/principles/user-research/resultanalysis/> (дата обращения: 03.10.2023).
3. Шорохова И. С., Кисляк Н. В., Мариев О. С. Статистические методы анализа // Уральский государственный университет. – Екатеринбург: Издательство Уральского университета, 2015, с. 300
4. Что такое Machine Learning и каким оно бывает [Электронный ресурс] // Завтра облачно: [сайт]. – URL: <https://mcs.mail.ru/blog/what-is-machine-learning> (дата обращения: 04.10.2023).
5. Мухамадиева К. Б. Машинное обучение в совершенствовании образовательной среды // Образование и проблемы развития общества. – 2020, № 4, с. 70-77.
6. Зачем и как использовать визуализацию данных? [Электронный ресурс] // Хабр: [сайт]. – URL: <https://habr.com/ru/companies/developersoft/articles/240325/> (дата обращения: 05.10.2023).

## ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В ПРЕПОДАВАНИИ ГУМАНИТАРНЫХ ДИСЦИПЛИН

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: нейронные сети, гуманитарные дисциплины, анализ текстов, визуализация обучения

Рассмотрены ключевые аспекты использования нейронных сетей в преподавании гуманитарных дисциплин. Проанализированы преимущества технологий искусственного интеллекта при создании интерактивных и индивидуально ориентированных подходов к гуманитарному обучению. Особое внимание уделено внедрению нейронных сетей в области обработки естественного языка на примере анализа текстов в гуманитарных дисциплинах.

S.A. Dokuchaev, G.S. Kostetskaya, N.O. Svetlichnaya

## USING NEURAL NETWORKS IN TEACHING HUMANITIES SUBJECTS

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: neural networks, humanities disciplines, text analysis, visualization of learning

Key aspects of using neural networks in teaching humanities subjects have been examined. The advantages of artificial intelligence technologies in creating interactive and individually tailored approaches to humanities education have been analyzed. Special attention has been given to the implementation of neural networks in the field of natural language processing, exemplified by text analysis in humanities disciplines.

Нейросети – одна из наиболее перспективных и быстро развивающихся областей искусственного интеллекта. В последнее время возможности нейросетей начали использовать не только в производственной сфере, но и в образовании [1].

Современная эпоха быстрого технологического развития и его интеграции в различные академические области характеризуется инновационными изменениями педагогических подходов и методов исследования. Несмотря на то, что нейронные сети чаще ассоциируются с техническими и научными областями, их применение в гуманитарных дисциплинах открывает перед преподавателями и студентами новые возможности.

Нейронные сети предоставляют широкий спектр инструментов для анализа текстов, автоматического перевода, визуализации данных, симуляции исторических событий. Это позволяет глубже исследовать материал, автоматизируя рутинные задачи и концентрируясь на интерпретации и критическом анализе.

Нейронные сети оказались революционным инструментом в области обработки естественного языка (NLP, Natural Language Processing). Рассмотрим, как они могут быть применены для анализа текстов в гуманитарных дисциплинах:

1. Распознавание темы и классификация текста. С помощью нейронных сетей можно автоматически определить основную тему или жанр текста. Это может быть полезно при анализе больших корпусов литературных произведений, исследований или новостных статей.

2. Семантический анализ. Нейронные сети способны определять не только отдельные слова, но и общий смысл или настроение текста. Это позволяет анализировать эмоциональную окраску текста, выявляя, например, субъективные мнения автора.
3. Извлечение ключевых слов и фраз. Для выделения наиболее важной информации из текста можно использовать алгоритмы, основанные на нейронных сетях, которые определяют ключевые слова и фразы, характеризующие содержание.
4. Распознавание именных существей. Сети могут распознавать имена, географические названия, даты и другие конкретные детали, что может быть полезно при исследовании исторических документов или литературных произведений.
5. Анализ стиливых особенностей. Исследование стилистики автора, например, особенностей его словарного запаса, синтаксиса или ритмики, может быть автоматизировано с помощью нейронных сетей. Это позволяет быстро сравнивать стиль разных авторов или определять авторство неизвестных текстов.
6. Создание текстовых суммаризаций. Нейронные сети могут автоматически генерировать краткие и содержательные резюме больших текстов, сохраняя ключевую информацию.

Исследуя использование нейросетей в преподавании гуманитарных дисциплин, невозможно обойти вниманием такую актуальную область, как машинный перевод. До появления глубокого обучения и нейронных сетей перевод в основном основывался на статистических методах и правилах. С внедрением секвенционных нейронных сетей, BERT моделей, Transformer архитектуры процесс перевода стал гораздо более точным и натуральным.

Применение нейронных сетей в гуманитарных дисциплинах может казаться неожиданным, но такой подход может радикально изменить процесс обучения, делая его более интерактивным, глубоким и индивидуально ориентированным. Нейронные сети могут служить мостом между традиционными методами преподавания и передовыми технологиями, обогащая гуманитарное образование.

## СПИСОК ЛИТЕРАТУРЫ

1. Хабибуллин, И. Р. Актуальность использования нейросетей в образовательных целях / И. Р. Хабибуллин, О. В. Азовцева, А. Д. Гареев. — Текст: непосредственный // Молодой ученый. — 2023. — № 13 (460). — С. 176-178. — URL: <https://moluch.ru/archive/460/101127/> (дата обращения: 20.10.2023).

**С.А. Докучаев, Г.С. Костецкая, Б.Б. Конкин**

## **ЦИФРОВАЯ ЛЕКЦИЯ КАК ЭФФЕКТИВНЫЙ ЭЛЕМЕНТ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА В ТЕХНИЧЕСКОМ ВУЗЕ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: цифровые технологии, цифровая лекция, интерактивность, визуализация обучения

---

Подчеркнута важная роль цифровой лекции в формировании цифровой среды в современном техническом вузе. Особое внимание уделено структуре цифровой лекции и ее месту в образовательном процессе. Проанализированы преимущества цифровизации по сравнению с традиционными методами обучения.

**S.A. Dokuchaev, G.S. Kostetskaya, B.B. Konkin**

## **DIGITAL EDUCATIONAL STREAMING PORTAL AS AN EFFECTIVE WAY TO FORM DIGITAL COMPETENCIES IN STUDENTS**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: digital technologies, digital lecture, interactivity, visualization of learning

The important role of the digital lecture in shaping the digital environment in a modern technical university is emphasized. Special attention is paid to the structure of the digital lecture and its place in the educational process. The advantages of digitalization compared to traditional teaching methods have been analyzed.

В современном мире цифровые технологии все больше проникают в различные сферы жизни, в том числе и в образование. Одно из самых прогрессивных и многогранных направлений – создание цифровых лекций. Цифровые лекции в технических вузах становятся неотъемлемой частью учебного процесса, предоставляя преподавателям и студентам значительный ряд преимуществ.

Цифровая лекция представляет собой электронный образовательный ресурс, созданный с использованием современных технологий для представления информации в интерактивной и визуально привлекательной форме. Цифровые лекции могут быть представлены в различных форматах, таких как видео, презентации, виртуальная доска, и т.д.

В структуре цифровой лекции явно выделяются следующие элементы:

- заголовок, содержащий четкое и краткое наименование темы лекции;
- основное содержание, которое состоит из теоретической части, практического блока и интерактивных элементов для проверки знаний студентов;
- дополнительные материалы, включающие в себя ссылки на дополнительные ресурсы, видео, статьи и другие материалы для углубленного изучения темы;
- обратная связь, позволяющая студентам вне аудитории задавать вопросы, оставлять комментарии или предложения по улучшению материала.

Для решения проблемы обратной связи авторами активно используются системы управления обучением (Learning Management System, LMS), в частности LMS Moodle и LMS MasterStudy. Данные LMS обеспечивают педагогические условия для эффективного дистанционного обучения студентов и их оперативного взаимодействия с преподавателем посредством чата, анкетирования, тестирования, форумов, опросов, рабочих тетрадей, семинаров [1].

При создании цифровой лекции важно учитывать не только содержательную, но и визуальную составляющую, делая материал интересным и понятным для аудитории. В частности, одним из результативных способов визуализации образовательного контента является инфографика - графический способ подачи информации, данных и знаний, целью которого является быстро и четко преподнести сложную информацию [2].

Незаменимым помощником преподавателя при проведении цифровой лекции выступает виртуальная доска – цифровой инструмент, расширяющий возможности традиционной доски благодаря интерактивности и технологическим преимуществам. Современные виртуальные доски, например Lekh Board, позволяют не только отображать информацию, но и взаимодействовать с ней в реальном времени. Преподаватели могут

---

подчеркивать, выделять, перемещать элементы, а студенты — активно участвовать, делая заметки или рисуя на доске. После завершения лекции содержимое доски можно сохранить и предоставить студентам для повторения и самостоятельной работы.

Цифровые лекции в технических вузах становятся неотъемлемой частью учебного процесса, предоставляя преподавателям и студентам ряд преимуществ:

1. **Интерактивность и визуализация:** использование разнообразных мультимедийных инструментов (графики, анимации, видео) особенно актуально для технических дисциплин, где требуется наглядно показать сложные процессы или конструкции;
2. **Доступность и гибкость:** цифровые лекции доступны студентам в любое время и в любом месте, что предоставляет им возможность учиться в удобном режиме;
3. **Индивидуализация обучения:** каждый студент может повторить пройденный материал столько раз, сколько ему нужно с учетом индивидуальных особенностей восприятия информации;
4. **Актуализация материала:** цифровые лекции легко обновлять и дополнять новой информацией, что позволяет поддерживать учебный материал в актуальном состоянии.

В современном образовательном процессе все большее применение находят технологии искусственного интеллекта, в частности, нейронные сети. При проведении цифровой лекции их возможности могут быть использованы для оптимизации и повышения эффективности обучения. Например, с помощью нейронных сетей можно оценить уровень внимания и интереса аудитории к представленному материалу, анализируя мимику, жесты или движения глаз. Это позволяет преподавателю мгновенно корректировать ход лекции, делая ее более захватывающей. Нейронные сети могут помочь в автоматическом создании и оптимизации визуальных материалов, таких как графика, диаграммы или анимации, делая их более понятными и интерактивными, а после завершения лекции автоматически анализировать ответы студентов на тестовые вопросы, выдавая моментальный фидбэк и рекомендации по дальнейшему изучению темы.

Цифровые лекции в технических вузах открывают новые возможности для образовательного процесса. Они делают обучение более наглядным, доступным и актуальным. При правильном подходе и сочетании с другими методами обучения, цифровые лекции могут значительно повысить качество и эффективность образования.

#### СПИСОК ЛИТЕРАТУРЫ

1. Докучаев С.А., Костецкая Г.С., Ефимов С.В. О цифровых образовательных технологиях в образовательной экосистеме технического вуза. Труды СКФ МТУСИ. Международная научно-практическая конференция СКФ МТУСИ, Ростов-на-Дону. 2021, с.363-365.
2. Докучаев С.А., Костецкая Г.С., Светличная Н.О., Колдынская Л.М. Современные средства визуализации учебного контента. Труды СКФ МТУСИ. Международная научно-практическая конференция СКФ МТУСИ, Ростов-на-Дону. 2021, с.365-367.



---

**И.В. Калиенко<sup>1</sup>, О.Ю. Назарова<sup>1</sup>, И.В. Решетникова<sup>2</sup>,  
Ахмед Абдулмалек Абдулкадер Мохаммед<sup>1</sup>, Д.Е. Каун<sup>3</sup>**

**ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ И МОДЕЛИРОВАНИЕ РАБОТЫ  
АНАЛОГО-ЦИФРОВОГО ПРЕОБРАЗОВАТЕЛЯ В ПРОГРАММЕ  
КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ EWB ELECTRONICS WORKBENCH**

Донской государственный технический университет, г. Ростов-на-Дону<sup>1</sup>  
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>  
Ростовский-на-Дону колледж радиоэлектроники,  
информационных и промышленных технологий, Ростов-на-Дону, Россия<sup>3</sup>

Представлены результаты компьютерного и натурального моделирования аналого-цифрового и цифроаналогового преобразования в учебном процессе обучения специалистов в области телекоммуникаций. Предоставлена возможность моделирования как нормальной работы ЦАП и АЦП, так и моделирование ошибок, сбоев, нештатных ситуаций. Разработаны варианты индивидуальных заданий для обучаемых.

**I.V. Kaliyenko<sup>1</sup>, O.YU. Nazarova<sup>1</sup>, I.V. Reshetnikova<sup>2</sup>,  
Akhmed Abdulmalek Abdulkader Mokhammed<sup>1</sup>, D.Ye. Kaun<sup>3</sup>**

**EXPERIMENTAL RESEARCH AND SIMULATION OF THE OPERATION OF  
ANALOG-DIGITAL CONVERTER IN THE COMPUTER SIMULATION PROGRAM  
EWB ELECTRONICS WORKBENCH**

Don State Technical University, Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>  
Rostov-on-Don College of Radio Electronics,  
information and industrial technologies, Rostov-on-Don, Russia<sup>3</sup>

The results of computer and full-scale modeling of analog-to-digital and digital-to-analog conversion in the educational process of training specialists in the field of telecommunications are presented. It is possible to simulate both the normal operation of the DAC and ADC, as well as the simulation of errors, failures, and emergency situations. Options for individual assignments for students have been developed.

В настоящее время в нашей стране осуществляется полный переход на цифровые методы представления информации. Поэтому подготовка специалистов в области телекоммуникаций и передаче цифровой информации без сбоев, без искажений, с заданной достоверностью является важной задачей.

Следовательно, тема представленной работы является актуальной.

Разработка учебных макетов и тренажеров имеет существенные отличия от реальной аппаратуры. Реальная аппаратура должна работать исправно, не допускать никаких сбоев, наилучшим образом выполнять свои функции.

На учебных тренажерах и макетах НЕОБХОДИМО моделировать и изучать возможные нештатные ситуации, сбои, ложные срабатывания, возникновение неисправностей. Поэтому разработка учебных макетов является отдельной задачей.

*Объект разработки* – учебный тренажер-макет моделирования алгоритмов аналого-цифрового и цифроаналогового преобразования в учебном процессе обучения специалистов в области телекоммуникаций.

*Цель работы* – разработать учебный тренажер-макет для возможности изучения и демонстрации работы алгоритмов аналого-цифрового и цифроаналогового преобразования в учебном процессе обучения специалистов в области телекоммуникаций.

*Полученные результаты и их новизна* – в работе рассмотрен вопрос применения разработанного учебного тренажер-макета моделирования алгоритмов аналого-цифрового и цифроаналогового преобразования в учебном процессе обучения специалистов в области телекоммуникаций для обучения и подготовки специалистов в области радиоэлектроники и систем связи. В работе проведены экспериментальные испытания в проверки разработанного компьютерного и натурального учебного тренажер-макета. Результат исследований показал, что разработанный компьютерный макет адекватно представляет работу аппаратуры связи при обработке цифрового информационного сообщения.

В рамках исследований алгоритмов циклического кода на аппаратуре кафедры «Радиоэлектроника» в целях обучения и демонстрации работы, необходимо измерять и строить параметры и характеристики.

### Экспериментальное исследование аналого-цифрового преобразователя

#### 1. Моделирование работы аналого-цифрового преобразователя в программе компьютерного моделирования EWB Electronics Workbench

Проведем моделирование работы аналого-цифрового преобразователя в программе компьютерного моделирования EWB Electronics Workbench.

Работа аналого-цифрового преобразователя заключается в формировании кодовой комбинации, соответствующей аналоговому измеряемому напряжению. Кодовая комбинация АЦП формируется четырехразрядным счетчиком с матрицей R-2R, подключенной к выходным разрядам.

Работа счетчика останавливается, когда сигнал с выхода матрицы R-2R превысит аналоговый измеряемый сигнал. При этом на выходе компаратора возникает сигнал «логического 0» об остановке счета.

Рассмотрим формирование кодовой комбинации ЦАП с матрицей R-2R. Такая кодовая четырехразрядная комбинация имеет вид от 0000 до 1111:

Схема компьютерного моделирования ЦАП с матрицей R-2R представлена на рисунке 1.

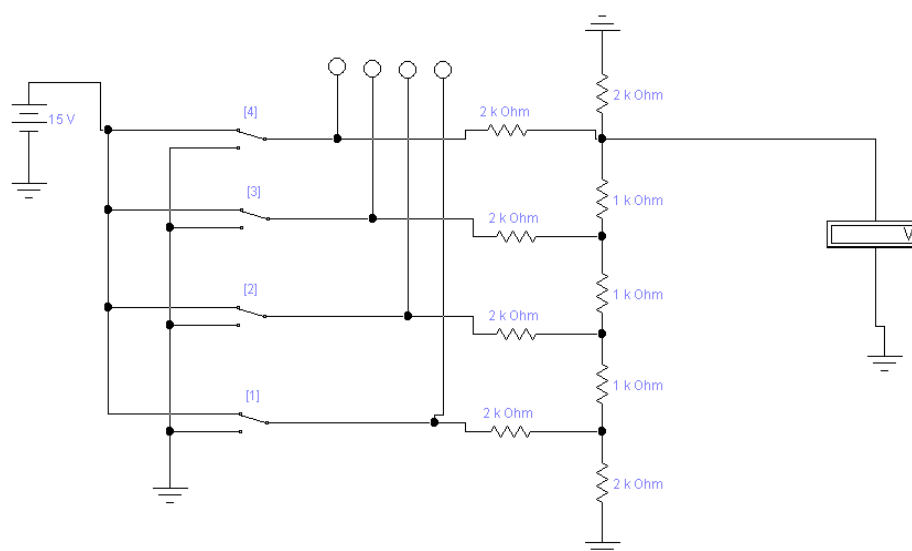


Рисунок 1. Схема компьютерного моделирования ЦАП с матрицей R-2R

Работа компьютерной модели ЦАП с матрицей R-2R происходит следующим образом.

Счетчик формирует на своем выходе последовательно цифровой сигнал от 0000 до 1111. На выходе матрицы R-2R формируется ступенчатое аналоговое напряжение, соответствующее каждой кодовой комбинации. Моделирование работы счетчика осуществляем с помощью четырех переключателей.

В таблице 1 показаны такты работы ЦАП с матрицей R-2R

Таблица 1. Такты работы ЦАП с матрицей R-2R

Дес. число	Двоичный код, разряды счетчика				Напряжение на выходе ЦАП с матрицей R-2R, В
	4	3	2	1	
0	0	0	0	0	0
1	0	0	0	1	0,625
2	0	0	1	0	1,25
3	0	0	1	1	1,87
4	0	1	0	0	2,5
5	0	1	0	1	3,123
6	0	1	1	0	3,75
7	0	1	1	1	4,37
8	1	0	0	0	5,00
9	1	0	0	1	5,62
10	1	0	1	0	6,25
11	1	0	1	1	6,87
12	1	1	0	0	7,5
13	1	1	0	1	8,12
14	1	1	1	0	8,744
15	1	1	1	1	9,37

Измерения работы ЦАП с матрицей R-2R проводились при напряжении опорного питания, равное 15 В.

Из таблицы видны следующие особенности работы ЦАП с матрицей R-2R.

В результате сформировано ступенчатое напряжение с шагом 0,625 В. Этот шаг является максимальной величиной погрешности моделируемого АЦП. Уменьшение погрешности в реальных условиях достигается уменьшением шага, увеличением числа разрядов. Однако в учебных целях для обеспечения наглядности работы модели большое число разрядов выбирать нецелесообразно.

При моделировании работы АЦП с матрицей ЦАП с матрицей R-2R два сигнала: 1) с выхода ЦАП с матрицей R-2R и 2) измеряемый аналоговый сигнал подают на два входа компаратора.

Когда сигнал с выхода ЦАП с матрицей R-2R меньше измеряемого аналогового сигнала, на выходе компаратора формируется уровень «логической 1», который свидетельствует о продолжении счета, наращивании кодовой комбинации на выходах счетчика.

Когда сигнал с выхода ЦАП с матрицей R-2R больше измеряемого аналогового сигнала, на выходе компаратора формируется уровень «логического 0», который свидетельствует об остановке счета, фиксации кодовой комбинации на выходах счетчика.

Данная фиксированная комбинация является выходным кодом АЦП с погрешностью, не превышающей шаг ЦАП.

На рисунках 2, 3 приведена схема компьютерной модели АЦП с матрицей ЦАП с матрицей R-2R при измерении напряжения 6 вольт.

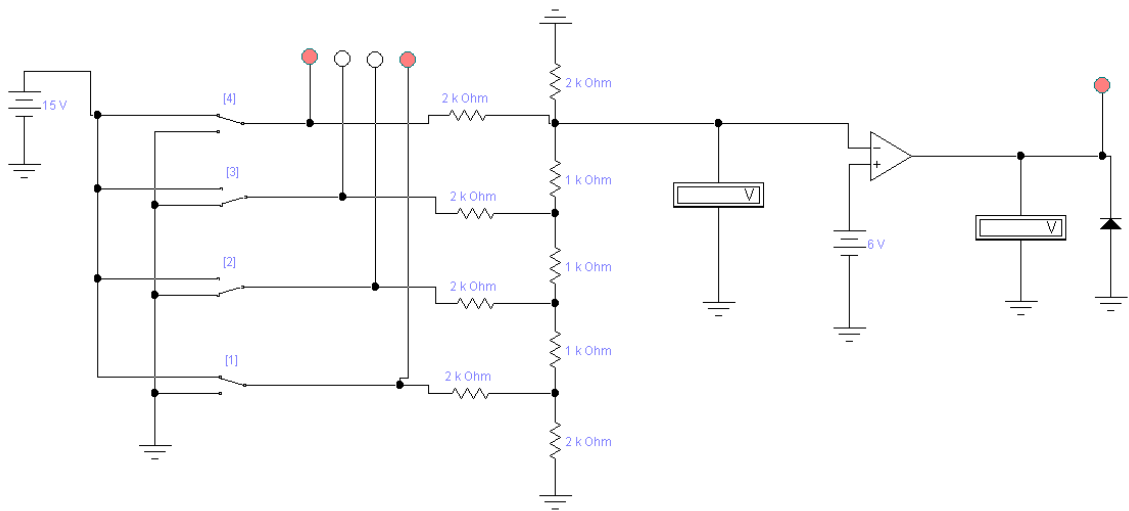


Рисунок 2. Схема компьютерной модели АЦП с матрицей ЦАП с матрицей R-2R при коде 1001

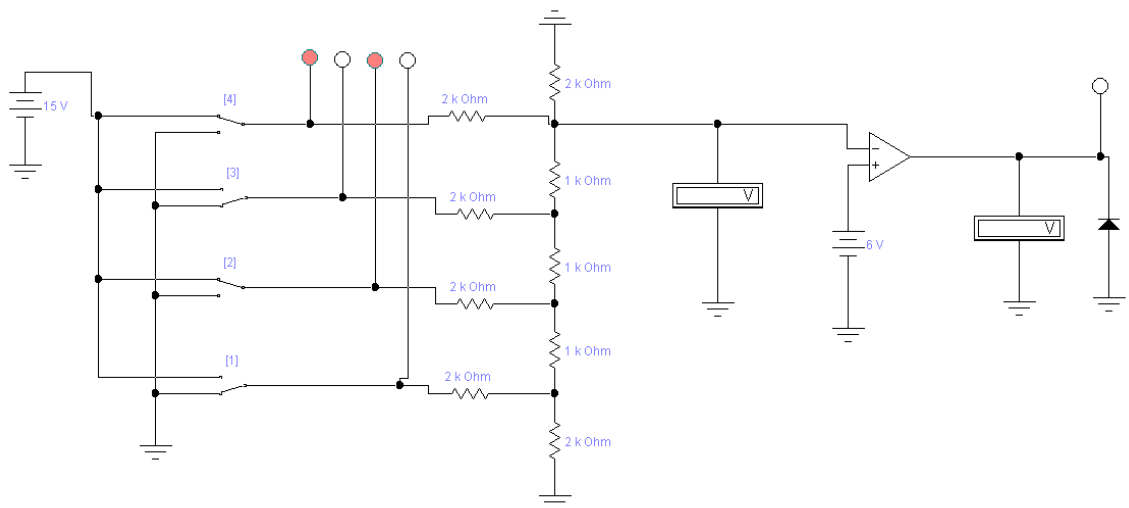


Рисунок 3. Схема компьютерной модели АЦП с матрицей ЦАП с матрицей R-2R при коде 1010

При коде 1001 индикатор с выхода компаратора горит. Счет продолжается.

При коде 1010 индикатор с выхода компаратора не горит. Счет остановлен.

Результаты измерения напряжения 6 вольт приведены в таблице.

Таблица 2. Работа компьютерной модели АЦП с матрицей ЦАП с матрицей R-2R при измерении напряжения 6 вольт

Дес. число	Выходной код				Индикатор компаратора	Напряжение на выходе ЦАП	Измеряемое напряжение
	4	3	2	1			
9	1	0	0	1	Горит	5,62 В	6 В
10	1	0	1	0	Не горит	6,25 В	6 В

Таким образом, проведено компьютерное моделирование работы АЦП с матрицей ЦАП с матрицей R-2R. Наглядно показана его работа по шагам при формировании ступенчатого напряжения. Наглядно показана его работа по шагам при измерении аналогового напряжения и преобразования его в цифровой код.

Предложенные, рассмотренные и исследованные компьютерные модели служат основой для построения натуральных схем учебных макетов преобразователей АЦП и ЦАП на реальных радиоэлементах для использования в учебном процессе.

## 2. Экспериментальное исследование натурной модели АЦП

В данной выпускной квалификационной работе был выполнен натурный расчет четырехразрядного аналогово-цифрового преобразователя. Ниже представлена фотография, готовой для проведения работы, установки.

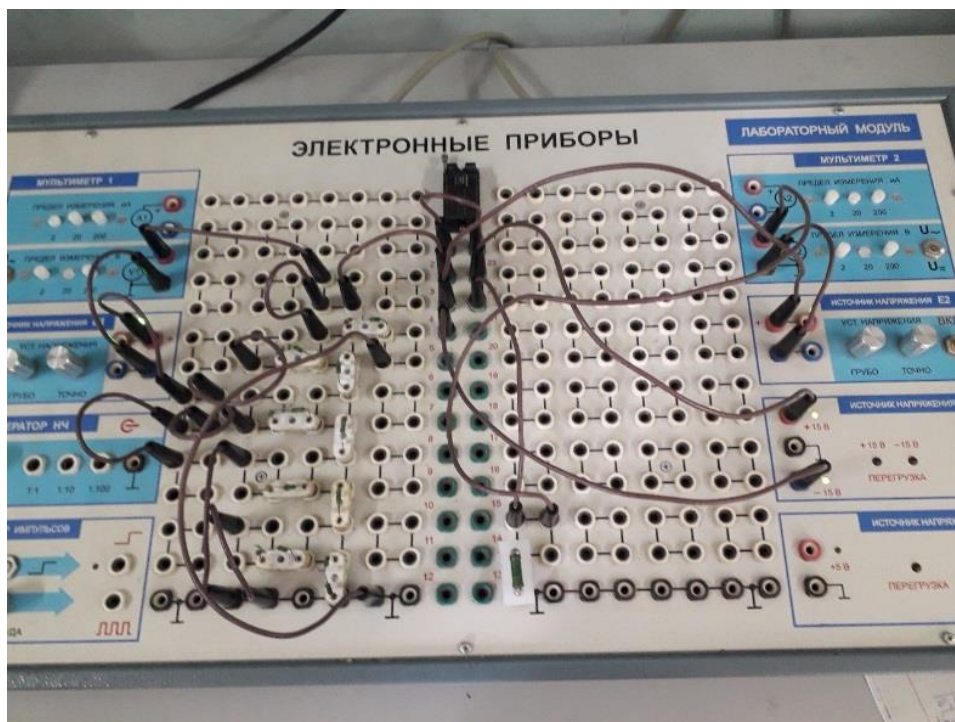


Рисунок 4. Установка для расчета параметров АЦП

Далее в таблице представлены полученные в ходе работы данные.

Таблица 4. Экспериментальное исследование макета АЦП

код	Выход АЦП	Выход компаратора	Измеренное $U$
0000	0	13,09	5,22
0001	0,44		
0010	0,85		
0011	1,33		
0100	1,77		
0101	2,22		
0110	2,66		
0111	3,10		
1000	3,55	-12,25	
1001	3,99		
1010	4,44		
1011	4,88		
1100			
1101	5,33		
1110			
1111			



Рисунок 5. Экспериментальное исследование макета АЦП

Таблица 5. Данные компьютерной модели АЦП при  $E=10В$

код	Вых АЦП	Измер U	Индикатор компаратора
0000	0	5,22	Горит
0001	0,416		
0010	0,832		
0011	1,249		
0100	1,666		
0101	2,082		
0110	2,498		
0111	2,915		
1000	3,330		
1001	3,747		
1010	4,163		
1011	4,580		
1100	4,993	Остановить счетчик	Не горит
1101	5,413		
1110	5,829		
1111	5,829		

АЦП показал, при округлении по верхнему уровню результат 1110. Измеряемое напряжение лежит между уровнями 1101 и 1110, что соответствует напряжениям 5,413В и 5,829В. Шаг квантования составил 0,416В (пошаговое квантование).

### **Выводы.**

В результате исследования компьютерного и натурального моделирования АЦП создана учебная модель, позволяющая изучать порядок обработки принятой цифровой информации, формирования ошибки, обусловленных шагом квантования.

Исходя из условий наглядности, выбран АЦП разрядности 4. Такой выбор позволяет удобно наблюдать весь процесс работы АЦП во всех разрядах одновременно.

Применение АЦП с другим количеством разрядов нецелесообразно в целях демонстрации работы и обучения специалистов. АЦП с большим разрядом неудобны для оценивания всех разрядов одновременно и также не обладают наглядностью.

Учебная компьютерная модель позволяет моделировать и изучать работу АЦП как в штатном режиме при отсутствии ошибок, так и в нештатных режимах при наличии ошибок в аналого-цифрового преобразования.

### **СПИСОК ЛИТЕРАТУРЫ**

1. Безуглов Д.А., Калиенко И.В. Цифровые устройства и микропроцессоры, – Ростов-на-Дону : Феникс, 2008. – 480 с.
2. Коджаспирова, Г.М. Технические средства обучения и методика их использования : учебное пособие для студентов высших учебных заведений / Г.М. Коджаспирова, К.В. Петров. – Москва : Академия, 2001. – 345с.
3. Микросхемы для бытовой радиоаппаратуры : справочник / И.В. Новиченко [и др.]. – Москва : КУБК-а, 1996. – 278 с.
4. Карлацук В.И. Электронная лаборатория на IBM PC. Программа Electronics Workbench и ее применение: - М.: Солон-Р, 2001.
5. Электротехника и электроника в экспериментах и упражнениях. Практикум по Electronics Workbench: Под ред. Д.И.Панфилова. В 2 т. - М.: Додэка, 1999 -2000.

**И.В. Калиенко<sup>1</sup>, О.Ю. Назарова<sup>1</sup>, И.В. Решетникова<sup>2</sup>,  
Ахмед Абдулмалек Абдулкадер Мохаммед<sup>1</sup>, Д.Е. Каун<sup>3</sup>**

### **РАЗРАБОТКА ПРАКТИЧЕСКОГО ЗАНЯТИЯ И МОДЕЛИРОВАНИЕ РАБОТЫ ЦИФРОАНАЛОГОВОГО ПРЕОБРАЗОВАТЕЛЯ В УЧЕБНОМ ПРОЦЕССЕ ОБУЧЕНИЯ СПЕЦИАЛИСТОВ В ОБЛАСТИ ТЕЛЕКОММУНИКАЦИЙ**

Донской государственный технический университет, г. Ростов-на-Дону<sup>1</sup>  
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>2</sup>  
Ростовский-на-Дону колледж радиоэлектроники,  
информационных и промышленных технологий, Ростов-на-Дону, Россия<sup>3</sup>

Представлены результаты компьютерного моделирования цифроаналогового преобразования в учебном процессе обучения специалистов в области телекоммуникаций. Предоставлена возможность моделирования как нормальной работы ЦАП, так и моделирование ошибок, сбоев, нештатных ситуаций. Разработаны варианты индивидуальных заданий для обучаемых.

---

I.V. Kaliyenko<sup>1</sup>, O.YU. Nazarova<sup>1</sup>, I.V. Reshetnikova<sup>2</sup>,  
Akhmed Abdulmalek Abdulkader Mokhammed<sup>1</sup>, D.Ye. Kaun<sup>3</sup>

**DEVELOPMENT OF A PRACTICAL LESSON AND SIMULATION OF THE  
OPERATION OF A DIGITAL TO ANALOG CONVERTER IN THE EDUCATIONAL  
PROCESS OF TRAINING SPECIALISTS IN THE FIELD OF  
TELECOMMUNICATIONS**

Don State Technical University, Rostov-on-Don, Russia<sup>1</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>2</sup>  
Rostov-on-Don College of Radio Electronics,  
information and industrial technologies, Rostov-on-Don, Russia<sup>3</sup>

The results of computer modeling of digital-to-analog conversion in the educational process of training specialists in the field of telecommunications are presented. The ability to simulate both the normal operation of the DAC and the simulation of errors, failures, and emergency situations is provided. Options for individual assignments for students have been developed.

В настоящее время в нашей стране осуществляется полный переход на цифровые методы представления информации. Поэтому подготовка специалистов в области телекоммуникаций и передаче цифровой информации без сбоев, без искажений, с заданной достоверностью является важной задачей.

Следовательно, тема представленной работы является актуальной.

Разработка учебных макетов и тренажеров имеет существенные отличия от реальной аппаратуры. Реальная аппаратура должна работать исправно, не допускать никаких сбоев, наилучшим образом выполнять свои функции.

На учебных тренажерах и макетах НЕОБХОДИМО моделировать и изучать возможные нештатные ситуации, сбои, ложные срабатывания, возникновение неисправностей. Поэтому разработка учебных макетов является отдельной задачей.

*Объект разработки* – учебный тренажер-макет моделирования цифроаналогового преобразования в учебном процессе обучения специалистов в области телекоммуникаций.

*Цель работы* – разработать учебно-методический материал для возможности изучения и демонстрации работы алгоритма цифроаналогового преобразования в учебном процессе обучения специалистов в области телекоммуникаций.

*Полученные результаты и их новизна* – в работе рассмотрен вопрос применения разработанного учебного тренажер-макета моделирования алгоритма цифроаналогового преобразования в учебном процессе обучения специалистов в области телекоммуникаций для обучения и подготовки специалистов в области радиоэлектроники и систем связи. В работе проведены экспериментальные испытания в проверки разработанного компьютерного и натурального учебного тренажер-макета. Результат исследований показал, что разработанный компьютерный макет адекватно представляет работу аппаратуры связи при обработке цифрового информационного сообщения.

В рамках исследований алгоритмов циклического кода на аппаратуре кафедры «Радиоэлектроника» в целях обучения и демонстрации работы, необходимо измерять и строить параметры и характеристики.



## Практическое занятие ЦАП 4 разряд

Начинается с заполнения таблицы.

Таблица 1. Исходные данные для исследования ЦАП

Напряжение питания Епит	Диапазон сигнала А	Максимальное напряжение на выходе Увыхмакс	Минимальное напряжение на выходе Увыхмин	Количество уровней Nур	Разрядность ЦАП n	Шаг квантования hкв
			0 В			

Одни параметры заданы, другие требуется рассчитать по формулам.

Диапазон сигнала  $A = U_{\text{выхмакс}} - U_{\text{выхмин}}$ .

Количество уровней  $N_{\text{ур}} = 2^n$ , где n – число двоичных разрядов ЦАП.

Количество уровней  $N_{\text{ур}} = \frac{A}{h_{\text{кв}}} + 1$ .

Напряжение на выходе ЦАП для заданного номера уровня N

$$U_{\text{вых}} = \frac{1}{3} E_{\text{пит}} \frac{N}{2^{(n-1)}}$$

Напряжение питания  $E_{\text{пит}} = 3 A 2^{(n-1)} / N_{\text{макс}}$ , где  $N_{\text{макс}}$  – номер максимального уровня

Шаг квантования  $h_{\text{кв}} = A / (N_{\text{ур}} - 1)$

### 1 способ выдачи задания.

Например, заданы значения: 1) Разрядность ЦАП n ; 2) Максимальное напряжение на выходе  $U_{\text{выхмакс}}$  (возможно задать другие значения)

Таблица 2. Исходные данные для исследования ЦАП

Напряжение питания Епит	Диапазон сигнала А	Максимальное напряжение на выходе Увыхмакс	Минимальное напряжение на выходе Увыхмин	Количество уровней Nур	Разрядность ЦАП n	Шаг квантования hкв
		10 В	0 В		4	

В результате расчетов получаем

Количество уровней  $N_{\text{ур}} = 2^n = 2^4 = 16$ , где n – число двоичных разрядов ЦАП.

Диапазон сигнала  $A = U_{\text{выхмакс}} - U_{\text{выхмин}} = 10 \text{ В} - 0 \text{ В} = 10 \text{ В}$ .

Напряжение питания  $E_{\text{пит}} = 3 A 2^{(n-1)} / N_{\text{макс}} = 3 * 10 \text{ В} * 2^{(4-1)} / 15 = 15,48 \approx 16$

В.

Шаг квантования  $h_{\text{кв}} = A / (N_{\text{ур}} - 1) = 10 \text{ В} / 15 = 0,667 \text{ В} = 667 \text{ мВ}$ .

В результате расчетов получаем

Таблица 3. Исходные данные для исследования ЦАП

Напряжение питания Епит	Диапазон сигнала А	Максимальное напряжение на выходе Увыхмакс	Минимальное напряжение на выходе Увыхмин	Количество уровней Nур	Разрядность ЦАП n	Шаг квантования hкв
16 В	10 В	10 В	0 В	16	4	0,667 В

Схема для исследования четырехразрядного ЦАП на матрице R-2R

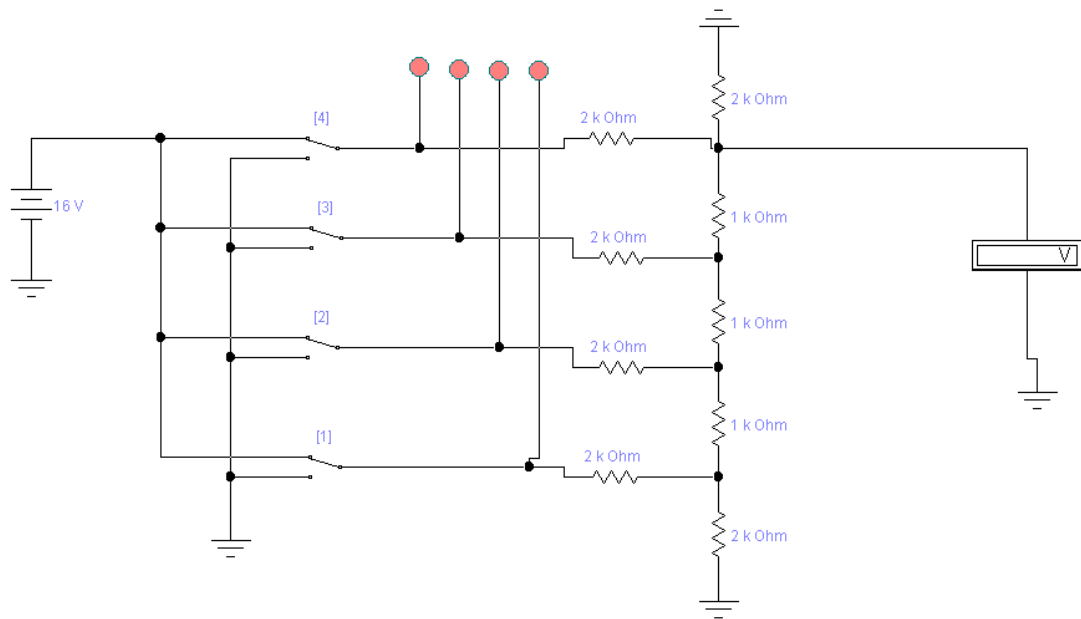


Рисунок 1

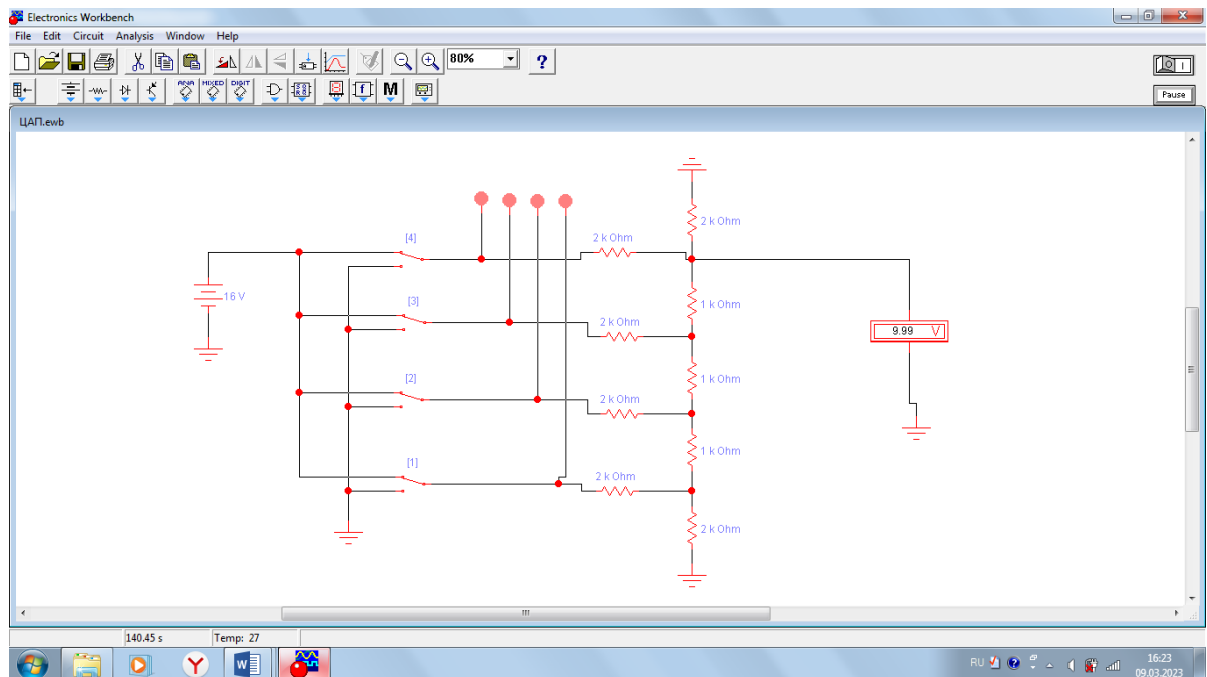


Рисунок 2

Из рисунка видно, что при напряжении питания  $E_{пит} = 16\text{В}$  при максимальном уровне ЦАП на матрице R-2R  $N_{макс} = 11112 = 1510$  напряжение на выходе ЦАП равно  $U_{выхмакс} = 9,99\text{В} \approx 10\text{В}$ .

Увых, В Результаты исследования четырехразрядного ЦАП на матрице R-2R сведены в таблицу

Таблица 4. Результаты исследования ЦАП

Дес число	Двоичный код				Напряжение на выходе ЦАП с матрицей R-2R			
	3	2	1	0	измерено		рассчитано	
					U <sub>вых</sub> , В	h <sub>кв</sub> , В	U <sub>вых</sub> , В	h <sub>кв</sub> , В
0	0	0	0	0	0			
1	0	0	0	1	0,6662			
2	0	0	1	0	1,332			
3	0	0	1	1	1,999			
4	0	1	0	0	2,665			
5	0	1	0	1	3,331			
6	0	1	1	0	3,997			
7	0	1	1	1	4,664			
8	1	0	0	0	5,330			
9	1	0	0	1	5,996			
10	1	0	1	0	6,662			
11	1	0	1	1	7,328			
12	1	1	0	0	7,995			
13	1	1	0	1	8,661			
14	1	1	1	0	9,327			
15	1	1	1	1	9,99			

Возможно выдавать задания другим образом

**2 способ выдачи задания.**

Например, заданы значения: 1) Разрядность ЦАП n ; 2) Шаг квантования h<sub>кв</sub> (возможно задать другие значения)

Таблица 5. Исходные данные для исследования ЦАП

Напря жение пита ния Епит	Диапазон сигнала А	Максимальное напряжение на выходе U <sub>выхмакс</sub>	Минимальное напряжение на выходе U <sub>выхмин</sub>	Количество уровней N <sub>ур</sub>	Разряд ность ЦАП n	Шаг квантования h <sub>кв</sub>
			0 В		4	0,3 В

В результате расчетов получаем

Количество уровней  $N_{ур} = 2^n = 2^4 = 16$ , где n – число двоичных разрядов ЦАП.

Максимальное напряжение на выходе  $U_{выхмакс} = h_{кв} * N_{макс} = 0,3 В * 15 = 4,5 В$

Диапазон сигнала А =  $U_{выхмакс} - U_{выхмин} = 4,5 В - 0В = 4,5 В$ .

Напряжение питания Епит =  $3 A \cdot 2^{(n-1)} / N_{макс} = 3 * 4,5 В * 2^{(4-1)} / 15 = 7,2 В$ .

В результате расчетов получаем.

Таблица 6. Исходные данные для исследования ЦАП

Напря жение пита ния Епит	Диапазон сигнала А	Максимальное напряжение на выходе U <sub>выхмакс</sub>	Минимальное напряжение на выходе U <sub>выхмин</sub>	Количество уровней N <sub>ур</sub>	Разряд ность ЦАП n	Шаг квантования h <sub>кв</sub>
7,2 В	4,5 В	4,5 В	0 В	16	4	0,3 В

Возможно выдавать задания другим образом

**3 способ выдачи задания.**

Например, заданы значения: 1) Разрядность ЦАП n; 2) Напряжение питания Епит (возможно задать другие значения)

Таблица 7. Исходные данные для исследования ЦАП

Напряжение питания Епит	Диапазон сигнала А	Максимальное напряжение на выходе Uвыхмакс	Минимальное напряжение на выходе Uвыхмин	Количество уровней Nур	Разрядность ЦАП n	Шаг квантования hкв
9 В			0 В		4	

В результате расчетов получаем

Количество уровней  $N_{ур} = 2n = 24 = 16$ , где n – число двоичных разрядов ЦАП.

Максимальное напряжение на выходе  $U_{выхмакс} = \frac{1}{3} E_{пит} \frac{N}{2^{(n-1)}} = 6 В$

Диапазон сигнала  $A = U_{выхмакс} - U_{выхмин} = 5,813 В - 0В = 5,813 В$ .

Шаг квантования  $h_{кв} = A / (N_{ур} - 1) = 6 В / 15 = 0,4 В = 400 мВ$ .

В результате расчетов получаем.

Таблица 8. Исходные данные для исследования ЦАП

Напряжение питания Епит	Диапазон сигнала А	Максимальное напряжение на выходе Uвыхмакс	Минимальное напряжение на выходе Uвыхмин	Количество уровней Nур	Разрядность ЦАП n	Шаг квантования hкв
9 В	6 В	6 В	0 В	16	4	0,4 В

### Выводы.

В результате исследования компьютерного моделирования ЦАП создана учебная модель, позволяющая изучать порядок обработки принятой цифровой информации, формирования ошибки, обусловленных шагом квантования.

Исходя из условий наглядности, выбраны разрядности ЦАП 4 и 5. Такой выбор позволяет удобно наблюдать весь процесс работы ЦАП во всех разрядах одновременно.

Применение ЦАП с другим количеством разрядов нецелесообразно в целях демонстрации работы и обучения специалистов. ЦАП с большим разрядом неудобны для оценивания всех разрядов одновременно и также не обладают наглядностью.

Учебная компьютерная модель позволяет моделировать и изучать работу АЦП как в штатном режиме при отсутствии ошибок, так и в нештатных режимах при наличии ошибок в аналого-цифрового преобразования.

### СПИСОК ЛИТЕРАТУРЫ

1. Безуглов Д.А., Калиенко И.В. Цифровые устройства и микропроцессоры, – Ростов-на-Дону : Феникс, 2008. – 480 с.
2. Коджаспирова, Г.М. Технические средства обучения и методика их использования : учебное пособие для студентов высших учебных заведений / Г.М. Коджаспирова, К.В. Петров. – Москва : Академия, 2001. – 345с.
3. Микросхемы для бытовой радиоаппаратуры : справочник / И.В. Новиченко [и др.]. – Москва : КУБК-а, 1996. – 278 с.
4. Карлащук В.И. Электронная лаборатория на IBM PC. Программа Electronics Workbench и ее применение: - М.: Солон-Р, 2001.
5. Электротехника и электроника в экспериментах и упражнениях. Практикум по Electronics Workbench: Под ред. Д.И.Панфилова. В 2 т. - М.: Додэка, 1999 -2000.

---

Д.А. Жуковский<sup>1</sup>, С.Д. Ермакова<sup>2</sup>, С.А. Думбасар<sup>2</sup>, Д.Е. Панков<sup>2</sup>,  
Н.М. Лелик<sup>2</sup>, С.В. Константинова<sup>2</sup>

## ФИЗИКА И ПСИХОЛОГИЯ ВОСПРИЯТИЯ ЦВЕТА ПРИ РАБОТЕ НАД ПРОЕКТОМ САЙТА ИЛИ РЕКЛАМНОГО ПРОДУКТА

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Донской государственной технической университет,  
Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: оптический диапазон волн, цветовой спектр, психофизиологическое восприятие цвета, комплементарные или дополнительные цвета, гармоничные сочетания цветов.

В статье рассмотрено психофизиологическое влияние цвета на человека. Показана важность подбора графическим дизайнером гармоничного сочетания цветов при создании сайта или рекламного продукта. Приведен пример использования графического редактора CorelDRAW для создания цветового стиля разрабатываемого проекта.

D.A. Zhukovsky<sup>1</sup>, S.D. Ermakova<sup>2</sup>, S.A. Dumbasar<sup>2</sup>, D.E. Pankov<sup>2</sup>,  
N.M. Lelik<sup>2</sup>, S.V. Konstantinova<sup>2</sup>

## PHYSICS AND PSYCHOLOGY OF COLOR PERCEPTION WHEN WORKING ON A WEBSITE OR ADVERTISING PRODUCT PROJECT

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia 1  
Don State Technical University,  
Rostov-on-Don, Russia 2

Keywords: optical wave range, color spectrum, psychophysiological perception of color, complementary or complementary colors, harmonious color combinations

The article considers the psychophysiological influence of color on a person. The importance of choosing a harmonious combination of colors by a graphic designer when creating a website or advertising product is shown. An example of using the CorelDRAW graphic editor to create a color style of the project being developed is given.

При разработке сайта или красочного рекламного продукта программист- дизайнер должен продумать, какую психологическую атмосферу будет создавать продукт его труда. Ведь за счет умело продуманного воздействия цветовой гаммы на пользователя, просматривающего интернет страницы или листающего рекламный буклет, будет зависеть успех всего дизайнерского проекта.

Цвет возбуждает в потребителе различные эмоции и притягивает или отталкивает его от предлагаемого ему продукта или сервиса. Если правильно и достаточно эффективно использовать цвет в процессе создания дизайна сайта или рекламного продукта, то в перспективе создатели проекта смогут от этого получить добавочную стоимость.

Что же такое цвет? На самом деле цвет – это те цветовые ощущения, которые формируются в мозгу человека. Очевидно, что эти ощущения будут разными, например, если источник света будет красным, синим или зеленым и полностью будут отсутствовать при отсутствии источника света.

Таким образом, свет – это сумма излучений видимого человеком диапазона, излучаемых источником света электромагнитных волн. Область электромагнитного

---

спектра, видимая человеческим глазом, составляет диапазон примерно от 400 до 700 нанометров.

Направив луч солнечного или белого источника света через призму, как показано на рисунке 1, можно разделить его на составляющие и таким образом увидеть, как человеческий глаз реагирует на каждую отдельную длину волны. Таким образом, волны разной длины интерпретируются человеком как разные цвета.

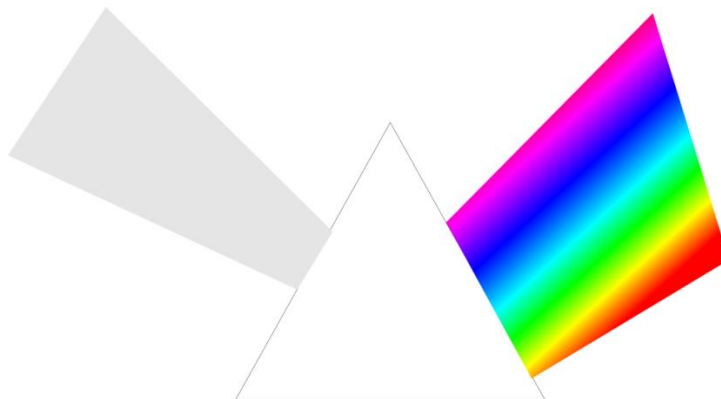


Рисунок 1. Разделение спектра белого света на составляющие

Следует отметить, что речь идет именно о восприятии цвета человеческим сенсором – глазом. Многие животные могут вообще не воспринимать цвет или видеть окружающий мир в другом оптическом диапазоне волн, включая ультрафиолетовую и инфракрасную области спектра.

Ниже приведены цвета излучений, которые сопоставлены с занимаемыми ими спектральными интервалами:

- Красный 620-700 нм;
- Оранжевый 580-620 нм;
- Желтый 565-580 нм;
- Зеленый 510-565 нм;
- Голубой 480-510 нм;
- Синий 450-480 нм;
- Фиолетовый 400-450 нм.

Действие на органы зрения излучений, с длинами волн в диапазоне 390-710 нм, приводит к цветовым ощущениям. Эти ощущения различаются качественно и количественно. Их качественная характеристика называется цветностью, а количественная – светлотой.

Еще в древности было замечено, что различные цвета по-разному воздействуют на психику человека. Рассмотрим в качестве примера 7 основных цветов – красный, оранжевый, желтый, зеленый, голубой, синий, фиолетовый, как показано на рисунке 2, и 3 монохромных – белый, серый и черный.

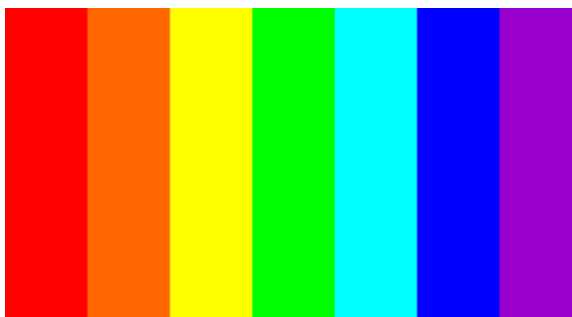


Рисунок 2. Основные цвета видимого оптического спектра

---

Красный – цвет действия, динамичности, энергии и лидерства, но в тоже время может ассоциироваться с опасностью, тревогой и запретами.

Оранжевый цвет является радостным и возбуждающим. Вспомним веселую детскую песенку: «Оранжевое небо, Оранжевое море, Оранжевая зелень, Оранжевый верблюд...». Оранжевый цвет имеет благотворное влияние и способствует хорошему настроению.

Ассоциация желтого цвета с солнцем делает его теплым, лучезарным, располагающим. Его характеристики: радость жизни, честность, веселье, радость и свобода. Однако считается, что он цвет сплетен, сарказма, рассеяности и критичности.

Зеленый цвет является наиболее спокойным цветом из всех остальных. Зеленый выражает обязательность, стабильность, выдержку, прогресс и настойчивость. Отрицательные качества зеленого – ревность, эгоизм, скука, замедление реакций.

Голубой цвет расширяет пространство, комфортен, успокаивает и позволяет сдерживать эмоции.

Синий цвет способствует спокойствию и умиротворенности, дает ощущение безмятежности и вызывает меланхолию. Цвет строгости и сохранения дистанции.

Фиолетовый цвет является самым тяжелым цветом, массивным, угнетающим и пассивным. Фиолетовый ассоциируется со скромностью, грустной задумчивостью, страданием.

Белый цвет вызывает чувства открытости, полноты, легкости, единства, чистоты и невинности. В то же время белый цвет характеризуется следующими ощущениями: бесплодностью, изоляцией, разочарованием, скукой и отрешенностью. Интересное качество белого цвета – уравновешенность (равенство), так как он заключает в себе все цвета, которые в сумме и формируют белый.

Черный – отсутствие или уничтожение всех цветов. Отсюда можно сделать вывод о чувственных ощущениях, вызываемых черным цветом. Этот цвет угнетает, вводит в оцепенение, отражает конфликт и безверие.

Серый цвет не является ни темным, ни светлым, ни цветным. Он не вызывает никакого ощущения. Этот цвет характеризует единство противоположностей, здравомыслие, уравновешенность. К негативным ощущениям от серого относятся: депрессия, печаль, меланхолия, одиночество.

Очевидно, что все разнообразие цветовой гаммы значительно шире и психологическое восприятие цветов у разных народов и даже у лиц различной возрастной категории может быть не только не соответствовать изложенным психологическим ощущениям, но и даже быть противоположными.

В данном случае авторы приводят наиболее устоявшиеся психо-физиологические ощущения, исходя из множества источников, которые приведены в [1-4].

При создании сайта или рекламного продукта использовать цвета, нужно очень осторожным. Не рекомендуется использовать слишком много цветов. Но и при использовании небольшого количества цветов существуют определенные правила.

Например, в качестве используемых сочетаний применяются следующие:

- использование одного цвета разной степени насыщенности;
- использования природных сочетаний цветов;
- использования противоположных цветов, контрастность;
- использования близлежащих цветов;

Очевидно, что при использовании программистом-дизайнером нескольких цветов в сайте или рекламном продукте могут возникнуть гармоничные (притягивающие к себе) и негармоничные (контрастные и тревожные сочетания), что в значительной степени будет сказываться на восприятии группы пользователей. Например, одним из природных сочетаний цветов является сочетание красного и черного или желтого и черного, которое часто используется для окраса ядовитых насекомых. Применение на сайте таких контрастных сочетаний будет далеко не гармоничным.

---

Для определения гармоничных (приятных для восприятия человеком) цветовых сочетаний используется цветовой круг, представленный на рисунке 3 [6].

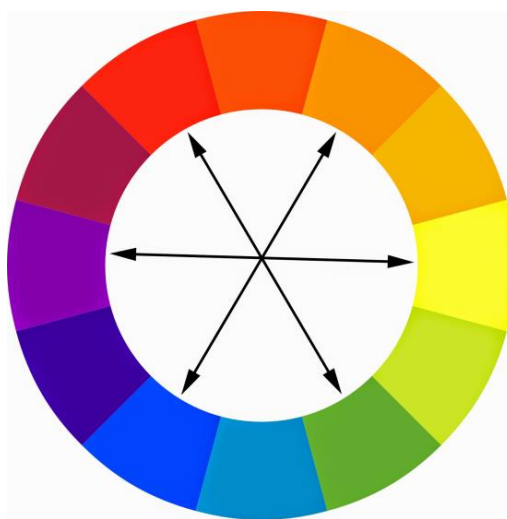


Рисунок 3. Цветовой круг

Цветовой круг представляет собой графический способ распределения цветов видимого спектра. При этом в цветовой круг добавлен не существующий в спектре цвет – пурпурный для связки двух крайних цветов в спектре – красного и фиолетового. Существует множество цветовых кругов, которые являются производными от различных цветовых моделей, рассмотрение которых ограничено рамками данной статьи.

Цвета, расположенные в круге напротив друг друга называются комплементарными или дополнительными. Смесь таких цветов теряет цветность. В зависимости от цветовой модели, результирующим цветом смеси являются: белый, черный или серый. Можно сказать, что противоположные цвета в цветовом круге уничтожают друг друга.

Таким образом, при использовании дополнительных цветов возникает сильный цветовой контраст, который, возможно, сначала привлечет внимание пользователя к сайту, но долго на нем не удержится из-за раздражающего воздействия.

Различные психологические эксперименты, связанные с влиянием цвета, проводимые в разное время учеными и философами, позволили сделать вывод о гармоничном сочетании цветовых составляющих. Сочетания цветов, ощущение от которых человеку приятно, называются гармоничными. В книге [3] в результате глубоких обоснований предлагается считать гармоничными те цвета, которые вписаны в цветовой круг в виде равносторонних или равнобедренных треугольников. Также гармоничными будут считаться цвета, которые получаются в результате вписывания в цветовой круг равностороннего пятиугольника.

Если дизайнеру необходимо привлечь внимание потребителя к своему продукту, он может использовать контрастные сочетания цветов, когда в цветовой круг вписан квадрат или прямоугольник. При этом следует учесть, что такое сочетание не будет гармоничным и, возможно, будет вызывать у потребителя продукта не понятное для него раздражение.

Современные графические редакторы позволяют формировать приведенные выше сочетания в различных пропорциях. Например, редактор векторной графики CorelDRAW при выборе в меню программы: «Инструменты»/ «Цветовые стили»/ «Создать цветовой стиль»/ «Краскосмесители» выводит на экран цветовой круг с возможностью вписывания в него от линии до пятиугольника, как показано на рисунке 4 [7].



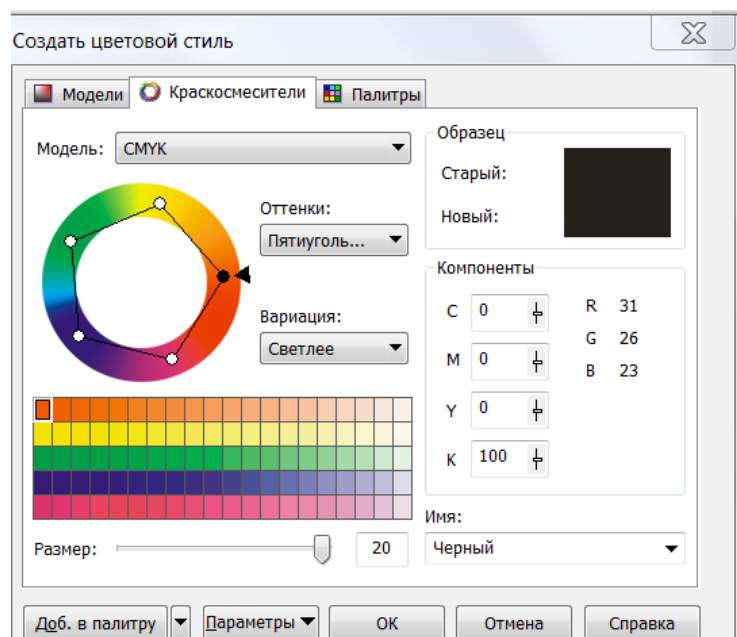


Рисунок 4. Использование инструмента «Создать цветовой стиль»

Используя возможности редактора модно получать любые гармоничные или контрастные сочетания цветов, как показано на рисунке 5.

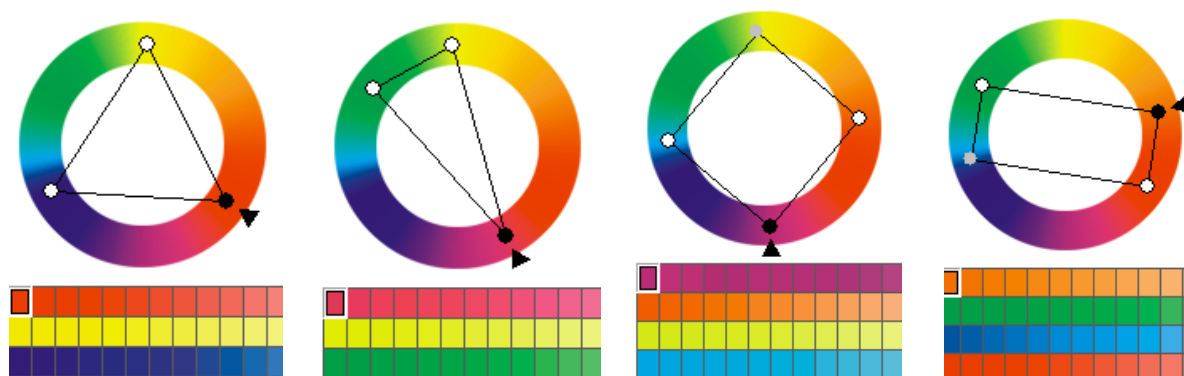


Рисунок 5. Примеры получения различных цветовых сочетаний

Следует отметить, что вписанную в цветовой круг фигуру можно вращать и изменять в ней соотношение сторон. Это позволяет дизайнеру использовать бесконечно большое количество комбинаций цветовой гаммы при построении сайта или рекламного продукта.

В данной статье авторы преследовали цель показать важность использования психофизиологического воздействия цвета на человека при создании графическим дизайнером сайта, интернет-портала или рекламного продукта. Показано, как можно использовать графический редактор CorelDRAW для создания цветového стиля при формировании гармоничного (приятного для человека) или контрастного (привлекающего внимание) сочетания цветов.

#### СПИСОК ИСТОЧНИКОВ

1. Волкова Ю.А. Психология восприятия цвета человеком. Северный (Арктический) федеральный университет. NovaInfo 57, с.534-540, Опубликовано 23 декабря 2016. <https://novainfo.ru/article/9819?ysclid=loajffqncg190281020> (дата доступа 20.10.2023)

2. М. Малоухова. Психология цвета: как цвет влияет на потребителей. <https://netology.ru/blog/10-2023-color-psychology?ysclid=loajkcwid2864017694> (дата доступа 20.10.2023)
3. Иоханес Иттен. Основы цвета. [http://soul-foto.ru/photo\\_books/Иттен%20Иоханес.%20Основы%20цвета.pdf?ysclid=loajnd5vq9656201474](http://soul-foto.ru/photo_books/Иттен%20Иоханес.%20Основы%20цвета.pdf?ysclid=loajnd5vq9656201474) (дата доступа 20.10.2023)
4. Буренкова О.А. Влияние цвета на психофизиологическое состояние личности. Журнал «Успехи современного естествознания». – 2013. – № 10 – С. 153-154. <https://natural-sciences.ru/ru/article/view?id=33038&ysclid=loajv6r7oe550496889> (дата доступа 20.10.2023)
5. Ж. Агостон. Теория цвета и её применение в дизайне. М.: «Мир» 1982. – 184 с.
6. Цветовой круг. [https://ru.wikipedia.org/wiki/Цветовой\\_круг](https://ru.wikipedia.org/wiki/Цветовой_круг) (дата доступа 20.10.2023)
7. Официальный сайт компании COREL. <https://www.corel.com/en/all-products/> (дата доступа 20.10.2023)

**А.Г. Жуковский<sup>1</sup>, Д.А. Жуковский<sup>1</sup>, С.А. Швидченко<sup>1</sup>,  
Д.Е. Панков<sup>2</sup>, А.Р.Балановская<sup>1</sup>**

**ОСОБЕННОСТИ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПО  
ДИСЦИПЛИНАМ, ТРЕБУЮЩИМ ИЗМЕНЕНИЙ ПРОГРАММНО-АППАРАТНОЙ  
КОНФИГУРАЦИИ КОМПЬЮТЕРОВ В УСЛОВИЯХ ОБЕСПЕЧЕНИЯ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>1</sup>  
Донской государственный технический университет, Ростов-на-Дону, Россия<sup>2</sup>

Ключевые слова: политика безопасности, иерархическая структура компьютерной сети, домены, идентификация и аутентификация, учебные дисциплины.

В статье рассмотрены ограничения, возникающие при проведении практических и лабораторных занятий по дисциплинам, требующим изменений программно-аппаратной конфигурации компьютеров. Приведены предложения по повышению эффективности проведения занятий при соблюдении политики безопасности вуза.

**A.G. Zhukovsky<sup>1</sup>, D.A. Zhukovsky<sup>1</sup>, S.A. Shvidchenko<sup>1</sup>,  
D.E. Pankov<sup>2</sup>, A.R. Balanovskaya<sup>1</sup>**

**FEATURES OF CONDUCTING PRACTICAL CLASSES IN DISCIPLINES  
REQUIRING CHANGES IN THE SOFTWARE AND HARDWARE CONFIGURATION  
OF COMPUTERS IN THE CONDITIONS OF INFORMATION SECURITY**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>1</sup>  
Don State Technical University, Rostov-on-Don, Russia<sup>2</sup>

Keywords: security policy, hierarchical structure of a computer network, domains, identification and authentication, academic disciplines.

---

The article discusses the limitations that arise when conducting practical and laboratory classes in disciplines that require changes in the hardware and software configuration of computers. The proposals for improving the effectiveness of classes in compliance with the security policy of the university are given.

В Северо-Кавказском филиале Московского технического университета связи и информатики (далее в Филиале) преподается большое количество дисциплин, связанных с изучением программного и аппаратного состава компьютерных информационных систем. Такими дисциплинами, например, являются: «Архитектура информационных систем», «Операционные системы», «Основы информационной безопасности», «Сетевые программные технологии», «Методы отладки и тестирования программных продуктов», «Мультимедиа технологии и протоколы», «Управление и администрирование в информационных системах», «Методы и средства защиты компьютерной информации», «Проектирование клиент-серверных приложений», «Учебная практика» и другие. При этом приведенный перечень далеко не полный и ограничен рамками статьи.

При проведении практических и лабораторных занятий по приведенным выше дисциплинам требуется установка, деинсталляция и настройка прикладного и системного программного обеспечения, изменение сетевой конфигурации, замена или установка аппаратных средств с инсталляцией соответствующих драйверов.

Например, при изучении дисциплины «Основы информационных систем и сетей» проводится лабораторная работа по теме: «Исследование характеристик и возможностей программ по восстановлению потерянных данных». Целью работы является изучение возможностей специализированного программного обеспечения по восстановлению потерянных или удаленных данных. В работе требуется выяснить, какие из утилит наиболее эффективны.

Для этого предлагается перечень из 16 различных специализированных программ по восстановлению информации. Студент должен выбрать из предложенного списка, опираясь на анализ функционала данных программ сайте производителя данного программного обеспечения или из других источников, три из них, проинсталлировать их на компьютер и исследовать возможности данных программ, удалив ряд файлов и папок на компьютере и на USB-флэш накопителе.

Примерно аналогичными по порядку выполнения являются лабораторные работы: «Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок», «Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии», «Исследование характеристик и возможностей антивирусного ПО», «Исследование характеристик и возможностей программ по организации резервного копирования».

Очевидно, что для выполнения заданий на лабораторную работу необходимо не только многократно устанавливать и удалять специальное ПО, но также удалять файлы и папки, что в настоящих условиях является невозможным. Это связано с тем, что компьютеры, находящиеся в учебных лабораторных аудиториях входят в клиент-серверную архитектуру, в которой задачи распределены между клиентами и серверами. В такой архитектуре клиент, обычно являющийся пользователем или программой, запрашивает услуги или ресурсы у сервера, который отвечает на запросы, предоставляя необходимые данные или обеспечивая определенную функциональность. При этом клиентские компьютеры сильно ограничены в правах за счет реализации политики информационной безопасности Филиала. Комплекс мер политики по обеспечению информационной безопасности при проведении учебного процесса обычно предусматривает:

- защиту информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации документов;

- 
- минимально необходимый, гарантированный доступ обучающегося только к тем информационным ресурсам, которые необходимы ему для усвоения материала;
  - контроль исполнения установленной технологии подготовки, обработки, передачи и хранения информации;
  - аутентификацию обрабатываемой информации;
  - снижение уровня рисков и угроз информационной безопасности до приемлемого уровня, позволяющего осуществлять устойчивое цифровое развитие Филиала и др.

Таким образом, любые попытки внесения изменений в программно-аппаратную часть компьютеров учебных лабораторных аудиторий будут определяться, как попытки нарушения информационной безопасности и потребуют применения соответствующего административного воздействия к нарушителям.

В этом случае практическое занятие проводится путем анализа в сети Интернет информации о функциональных возможностях изучаемой программы, ее положительных и отрицательных качествах, без установки требуемого программного обеспечения на компьютеры рабочих станций. Такой подход к проведению занятия в значительной степени снижает его эффективность.

В некоторой степени решить представленную выше проблему поможет использование виртуальной машины, например, свободно распространяемой компанией Oracle программы VirtualBox – эмулятора операционной системы, поддерживающий различные версии Windows, Linux, MacOS и Solaris.

Среди аналогов, распространяющихся по лицензии OpenSource, VirtualBox является одним из самых стабильных и удобных эмуляторов. Эмулятор создает среду, в которую можно установить операционную систему, не удаляя уже установленную. Вместо физического жесткого диска используется логический раздел HDD. В среде, которую эмулирует Virtual Box, имеется оперативная память, процессор, видеокарта и другие аппаратные устройства, которые на самом деле являются виртуальными.

Однако при применении виртуальной машины также возникают сложности. Прежде всего, это связано с очень высокими требованиями к аппаратной части хост-компьютера, т.е. компьютера, на который устанавливается виртуальная машина. Например, при установке виртуальной гостевой машины с операционной системой Windows 10 на хост компьютер с операционной системой Windows 7 (заметим, не ресурсоемкой) и оперативной памятью 8 Гб, загружается 83% оперативной памяти или 6,58 Гб, как показано на рисунке 1.

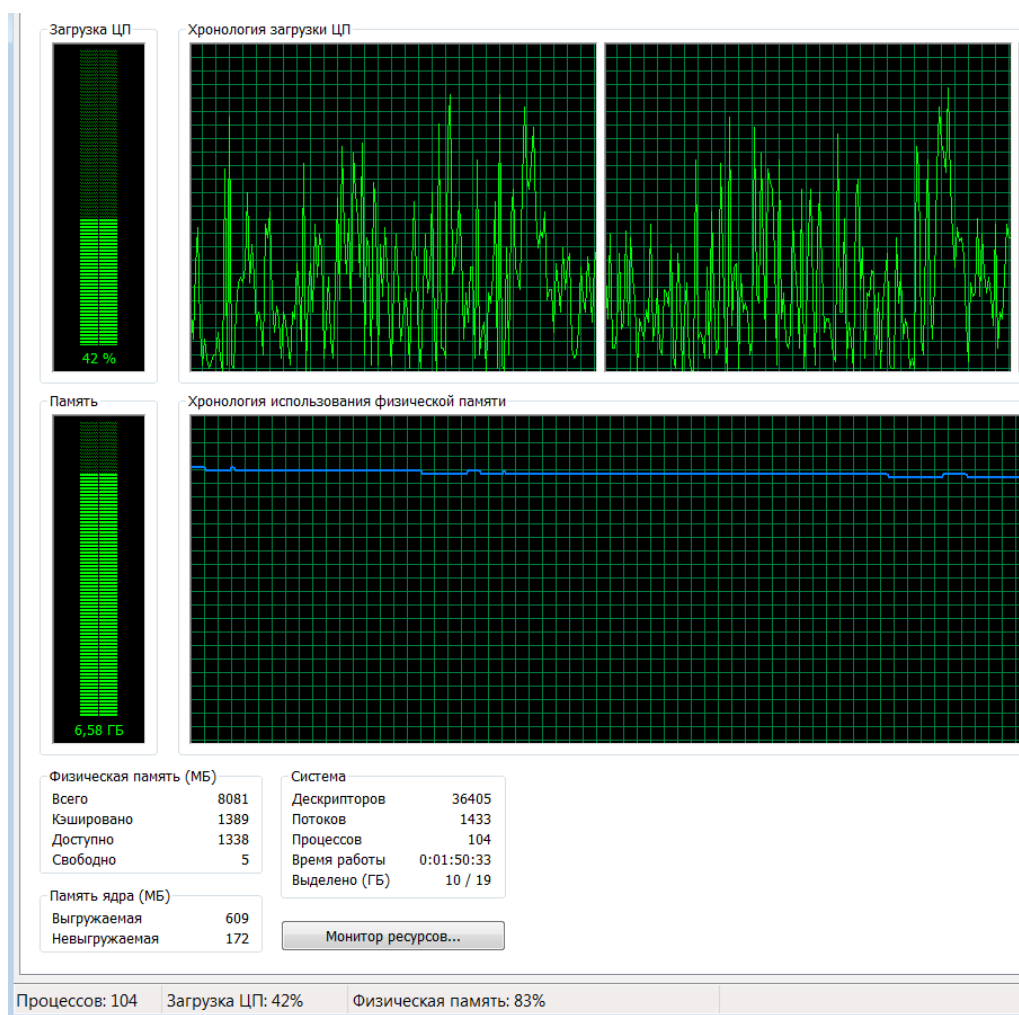


Рисунок 1. Загрузка аппаратных ресурсов компьютера при запуске виртуальной машины с операционной системой Windows 10

Таким образом, с учетом того, что в подавляющем большинстве рабочих станций в учебных лабораторных аудиториях установлена оперативная память объемом 4Гб, следует сделать вывод, что при использовании современных операционных систем, в худшем случае работать будет невозможно, а в лучшем случае – некомфортно из-за резкого снижения времени выполнения команд.

Следует отметить, что использование виртуальной машины может разрешить изложенную выше проблему, только если изменения вносятся в программную часть информационной системы. В случае изменения аппаратной части информационной системы, например, замена жесткого диска, подключение не поддерживаемых виртуальной машиной устройств, конфигурирование сетевой структуры информационной системы и др., виртуальная машина окажется бесполезной.

Для разрешения проблемы проведения занятий по дисциплинам, требующим внесения изменений в программно-аппаратный состав компьютеров, авторами предложен следующий подход.

Предлагается создать 1-2 учебных лабораторных аудиторий, в которых будут установлены компьютеры, сформированные в одноранговую локальную сеть по топологии «звезда» с использованием 16-ти или 24 портового коммутатора. При этом сеть не должна быть включена в домен с соответствующими ограничениями. Через один из портов коммутатора вся сеть может иметь доступ к интернету.

При этом компьютеры могут быть устаревшими (но работоспособными) и иметь различный аппаратный состав. Этот факт, конечно, в некоторой степени осложнит работу должностных лиц учебной лаборатории, но в значительной степени увеличит

---

эффективность проведения занятий, т.к. обучающийся будет работать на реальной системе с реальным «софтом» и «хардом».

При использовании предложенного подхода могут возникнуть следующие наиболее неприятные проблемы:

- на рабочую станцию может проникнуть вирус;
- при инсталляции новой программы или установке драйверов может произойти крах операционной системы;
- при использовании USB-флэш накопителя, он может быть заражен вирусом;
- при изменении конфигурационных параметров рабочей станции, ее нормальная работоспособность может быть нарушена;
- компьютер рабочей станции может выйти из строя.

Конечно, эти проблемы будут регулярно возникать. Решение проблем простое – иметь в учебной лаборатории программные «образы» каждой из рабочих станций и регулярно, в идеальном случае после очередного учебного дня, заново устанавливать образ системы на компьютер с USB-флэш накопителя.

Если во время занятия обучающие использовали USB-флэш накопители, то рекомендуется в конце занятия провести их сканирование на защищенном компьютере преподавателя на предмет заражения вирусом.

Что касается выходом из строя компьютера рабочей станции, то авторами предлагается в таких экспериментальных аудиториях использовать списанные, но работоспособные компьютеры или достаточно устаревшие, выход из строя которых можно считать в большей степени естественным процессом завершения жизненного цикла, чем воздействием извне.

#### **Вывод.**

По мнению авторов, имеющих большой педагогический опыт, с изложенной выше проблемой сталкивается большинство вузов. Поэтому предложения, представленные в данной статье, на наш взгляд являются актуальными и полезными и могут быть внедрены в любом вузе, на основе парка устаревших компьютеров.

#### **СПИСОК ИСТОЧНИКОВ**

1. Жуковский А.Г., Жуковский Д.А., Швидченко С.А. Основы информационной безопасности сетей и систем. Учебное пособие. – Ростов-на-Дону: СКФ МТУСИ, 2020. – 52 с.
2. Жуковский А.Г., Жуковский Д.А., Швидченко С.А. Мониторинг и конфигурация Wi-Fi сетей. Учебно-методическое пособие. Ростов-на-Дону: СКФ МТУСИ, 2021. – 59 с.
3. Кенин А. М. Практическое руководство системного администратора. — СПб.: БХВ-Петербург, 2010. — 464 с.: ил. — (Системный администратор)
4. Михайлов, В. В. Администрирование информационных систем: конспект лекций: учебное пособие / В. В. Михайлов. – Белгород: Изд-во БГТУ, 2017. – 112 с.
5. Кенин, А. М. Самоучитель системного администратора / А. М. Кенин, Д. Н. Колисниченко. — 5-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2019. — 608 с.: ил. — (Системный администратор)
6. Официальный сайт корпорации ORACLE. Программа Oracle VM VirtualBox <https://www.oracle.com/virtualization/virtualbox/> (Дата доступа 16.10.2023)
7. Долженко А.М., Жуковский А.Г. Сети ЭВМ и телекоммуникации. Методические указания к выполнению курсового проекта /РИС ЮРГУЭС Ростов-на-Дону, 2009.
8. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. — СПб.: Питер, 2022. — 1008 с.

## ЦИФРОВАЯ ЭКОНОМИКА В УПРАВЛЕНИИ ОБРАЗОВАНИЕМ И НАУКОЙ

Волгоградский государственный университет, Волгоград, Россия<sup>1</sup>

Южный Федеральный Университет, Ростов-на-Дону, Россия<sup>2</sup>

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>3</sup>

Ключевые слова: цифровая экономика, цифровая трансформация, цифровизация науки и образования, «Стратегия цифровой трансформации отрасли науки и высшего образования», цифровая зрелость.

В данной статье авторы приводят определения цифровой экономики, цифровизации образования и цифровой трансформации, раскрывают суть данных категорий и процессов. Рассматривают стратегию «Цифровой трансформации отрасли науки и высшего образования», выделяют основные её направления до 2030 года, а также анализируют главные проекты в рамках этих направлений и выделяют приоритетные их задачи.

A.A. Dzhikiya<sup>1</sup>, V.V. Mavrina<sup>2</sup>, V.I. Yukhnov<sup>3</sup>

## DIGITAL ECONOMY IN EDUCATION AND SCIENCE MANAGEMENT

Volgograd State University, Volgograd, Russia<sup>1</sup>

Southern Federal University, Rostov-on-Don, Russia<sup>2</sup>

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>3</sup>

Keywords: digital economy, digital transformation, digitalization of science and education, "Strategy of digital transformation of the branch of science and higher education", digital maturity.

In this article, the authors provide definitions of the digital economy, digitalization of education and digital transformation, reveal the essence of these categories and processes. They consider the strategy of "Digital transformation of the science and higher education industry", identify its main directions until 2030, as well as analyze the main projects within these areas and highlight their priority tasks.

Цифровая экономика – это не какая-то определённая сфера жизни деятельности людей или отрасль, а целая система и основа построения экономических моделей, которые позволяют трансформировать окружающий мир. Цифровая экономика – это большой шаг вперёд, а также упрощение многих процессов и взаимодействий, их вывод на новый уровень. В связи с этим, в современном мире происходят радикальные преобразования, которые затрагивают все стороны жизни людей. И сфера образования не является исключением.

Стоит отметить, что цифровая трансформация образования и дистанционное онлайн-образование с помощью различных цифровых платформ, к примеру, таких, как Moodle, Microsoft Teams, Discord, Coursera и др., являются абсолютно разными процессами. Понятие цифровой трансформации гораздо шире и включает в себя трансформацию не только непосредственно самого учебного процесса, но и организационных, появление принципиально новых продуктов.

Цифровизация образования стала особо заметна и ощутима после пандемии COVID-19, когда это стало вынужденной мерой. Однако процессы цифровизации данной

---

сферы начались гораздо раньше и являются достаточно масштабными, о чём свидетельствует размер рынка образовательных технологий (EdTech). По оценке Всемирного экономического форума, к 2025 году он достигнет 342 млрд долларов США. Только на одной платформе Coursera в прошлом году училось онлайн 100 миллионов слушателей.

Специалисты Высшей школы экономики выделили несколько этапов внедрения и использования информационных технологий в образовании. И каждый из них включал в себя разные процессы.

В рамках первой волны (автоматизации) активно появляются новые компьютерные классы разного уровня, которые способствуют формированию и развитию цифровой грамотности у молодёжи. Данная волна охватывает период с середины восьмидесятых по начало девяностых годов.

Вторая волна (цифровизация) характеризуется развитием уже более сложных процессов, а именно широким использованием информационно-коммуникационных технологий и их внедрением в учебный процесс. Теперь цифровые устройства и интерактивные формы начинают использоваться не только на занятиях по информатике, но на занятиях по другим областям.

Третья волна, собственно, цифровая трансформация, стартовала в 2018 году и продолжается до сих пор, являясь современным этапом и здесь уже идёт речь о полной цифровой трансформации образования, то есть об использовании цифровых технологий и средств во всех процессах образования, значительного снижения издержек в связи с внедрением цифровых технологий, появлении новых продуктов и услуг.

Для того, чтобы цифровая трансформация образования была действительно эффективной и результативной должно обновляться всё:

- образовательные стандарты и содержание образования;
- планируемые образовательные результаты;
- развиваемые компетенции обучающихся;
- педагогические методы;
- технологии обучения;
- средства и методы обучения;
- организация учебного процесса;
- организация процессов, сопровождающих обучение и др.

14 июля 2021 года на сайте Министерства науки и высшего образования появилась «Стратегия цифровой трансформации отрасли науки и высшего образования» – документ более чем на 260 страниц. Согласно ему, в России возникнет целый ряд собственных цифровых систем для научных организаций и университетов.

Документ охватывает период до 2030 года и предполагает работы сразу по пяти направлениям (трекам) цифровой трансформации. Каждое направление – глубоко проблемное для российских университетов и научных организаций:

### **1. Архитектура цифровой трансформации.**

Главной задачей данного направления является создание неких единых информационных базы и подхода к вопросу цифровой трансформации отраслей науки и образования, опираясь на которые вузы и научные организации смогут реализовывать собственные стратегии модернизации и трансформации, поскольку ранее созданные информационные системы относятся к разным промежуткам времени и плохо связаны между собой.

**2. Развитие цифровых сервисов.** Рынок, на котором они представлены достаточно объёмен и продолжает расти до сих пор. Но при этом вузы всё равно до сих пор внедряют новые технологии формально. Кроме того, доступ «к цифре» у всех различен. Министерство ставит своей задачей создание различных сервисов, которые позволят трансформировать все стороны деятельности научных и образовательных организаций.



---

**3. Управление данными.** На данный момент Минобрнауки активно использует различные Excel- и Google-формы для сбора и обработки информации, которые постоянно рассылает и пересылает вузам, что является достаточно небезопасным и некачественным, с точки зрения дальнейшей обработки данных и информации. В связи с этим, предполагается постепенный уход от данной системы и создание абсолютно новой, которая позволит принимать данные постоянно и автоматически и формировать на их основе предиктивную аналитику.

**4. Модернизация инфраструктуры.** Одним из сдерживающих факторов цифровой трансформации отраслей науки и образование является устаревшее оборудование или вовсе его нехватка. Поэтому в рамках данного трека, основной задачей для себя Министерство видит замену всего как морально, так и фактически устаревшего оборудования и обеспечение своевременной замены инфраструктуры вузов и научных центров в соответствии с современными техническими требованиями.

**5. Управление кадровым потенциалом.** Как говорилось ранее, чтобы цифровая трансформация была эффективной, должно обновляться и совершенствоваться всё. И подготовка кадров не является исключением. В результате реализации стратегии 100% преподавателей и административных сотрудников в вузах должны обладать цифровыми компетенциями. Сейчас этот показатель оценивается довольно низко.

«Стратегия цифровой трансформации отрасли науки и высшего образования» включает семь проектов, каждый из которых должен обеспечить продвижение к «цифровой зрелости» по одному или сразу по нескольким из пяти названных выше направлений. Прототипы или базовые версии сервисов по каждому из проектов должны заработать уже к 2024 году или раньше.

**1. Датахаб.** Представляет собой создание системы управления данными, которая упростит обмен данными между вузами и научными организациями с Минобрнауки и позволит давать доступ к этой информации внешним организациям и аудиториям. Предполагается бесшовный доступ бизнеса к результатам исследований и сервисы для граждан на основе этих данных.

**2. Архитектура цифровой трансформации.** Продуктом этого проекта будет являться VI-система, которая будет сопровождать образовательные и научные организации на их пути цифровой трансформации. Так же она позволит Минобрнауки отслеживать изменения в паспортах «цифровой зрелости» вузов. Кроме того, часть информации из этого паспорта будет находиться в открытом, публичном доступе.

**3. Цифровой университет.** Представляет собой достаточно масштабный проект, охватывающий создание и развитие сервисов для всех бизнес-процессов в сфере науки и высшего образования. Цифровой университет включает в себя не только онлайн-занятия и управление расписанием, но и мониторинг посещаемости, успеваемости, научной и публикационной активности, управление организационными, финансовыми, административными и другими процессами. Некоторые российские университеты уже внедряют собственные цифровые сервисы во многие направления. Однако стратегия предполагает создание некой общей модели для всех подведомственных Минобрнауки вузов. Также, согласно стратегии, данная модель должна быть внедрена не менее, чем в 50% таких вузов к концу 2024 года. Кроме того, столько же университетов к этому же времени должны реализовывать образовательные программы с построением индивидуальных образовательных траекторий.

**4. Единая сервисная платформа науки.** Основной задачей данной платформы является обеспечение возможности создания в России «виртуального ассистента учёного» посредством формирования единой экосистемы сервисов и услуг, которая позволит учёным проводить совместные исследования и предоставит доступ к международным базам данных и существующим мерам поддержки.

**5. Маркетплейс программного обеспечения и оборудования.** Данный проект представляет собой создание специальной платформы, с помощью которой научные и

---

образовательные организации смогут выбирать и заказывать современное оборудование и программное обеспечение напрямую от самих поставщиков, что в последствии даст возможность Минобрнауки полностью обновить инфраструктуру научных и образовательных организаций. Стратегия предполагает, что к 2024 году подведомственные Министерству вузы должны будут проводить в онлайн режиме не менее 75% закупок оборудования и программного обеспечения.

**6. Цифровое образование.** Задачей данного проекта является развитие цифровых компетенций как непосредственно у самих студентов, так и у научных, педагогических, преподавательских составов. Для реализации данного проекта были определены шаги, первым из которых является создание и обучение команд по цифровой трансформации в каждом вузе, подведомственном Минобрнауки. В некоторых вузах уже введена должность проректора по цифровой трансформации, также постепенно разрабатываются программы для обучения их команд. Все сотрудники, включая административный персонал, научных работников, преподавательский состав, и студенты, подведомственных Минобрнауки образовательных учреждений к 2030 году должны пройти программу по повышению цифровых компетенций.

**7. Сервис хаб.** Целью этого проекта является создание отдельной информационной системы, которая позволит систематизировать и регламентировать бизнес-процессы в вузах и в Министерстве науки и высшего образования. Доступ к этой системе должен быть обеспечен через мобильное приложение или веб-интерфейс, с помощью которого любой пользователь сможет заказать услугу и получить результат.

Таким образом, основной задачей «Стратегии цифровой трансформации отрасли науки и высшего образования» является создание «цифрового единства». Все сервисы, упомянутые в документе и рассмотренные в данной статье должны быть не просто связаны друг с другом, но и взаимодействовать между собой и функционировать на территории всей страны. Кроме того, документ называет ряд показателей, с помощью которых возможно будет определить, достигла ли сфера науки и образования «цифровой зрелости», и которые предполагают, что к 2030 году все подведомственные Минобрнауки вузы:

- внедрят единую модель цифрового университета;
- достигнут базового уровня цифровой зрелости;
- будут реализовывать образовательные программы с построением индивидуальных образовательных траекторий обучающихся;
- будут использовать «Сервис хаб» для создания и управления сервисами.

Кроме того, к 2030 году вузы должны взаимодействовать между собой по интеграции сервисов и содержанию образовательных программ и процессов посредством межведомственного сетевого механизма.

## СПИСОК ЛИТЕРАТУРЫ

1. Дышекова А. А. Цифровая экономика в образовании. Режим доступа URL: <https://kbgau.ru/riu/vypuski/arkhiv-nomerov/2021/2021-3/23.pdf> (Дата обращения: 17.10.2023).
2. Стратегия цифровой трансформации науки и высшего образования: к чему готовиться? Режим доступа URL: <https://skillbox.ru/media/education/opublikovana-strategiya-tsifrovoy-transformatsii-nauki/?ysclid=lnuphiynq6719307731> (Дата обращения: 18.10.2023).
3. Стратегия цифровой трансформации отрасли науки и высшего образования. Режим доступа URL: <https://minobrnauki.gov.ru/upload/iblock/e16/dv6edzmr0og5dm57dtm0wyllr6uwtujw.pdf> (Дата обращения: 18.10.2023).

- 
4. Что такое цифровизация образования и зачем она нужна. Режим доступа URL: <https://skillbox.ru/media/education/что-такое-цифровизация-образования-и-зачем-она-нужна/> (Дата обращения: 17.10.2023).

**Л.А. Гаевская**

## **ЗНАЧЕНИЕ ФИЗИЧЕСКОЙ КУЛЬТУРЫ В ЖИЗНИ СОВРЕМЕННОГО СТУДЕНТА**

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: физическая культура, опрос, студенты, современный мир.

В данной статье рассматривается значение физической культуры для студентов в современном мире. Основные заболевания, которые присутствуют у современной молодежи, а также образ жизни. Приоритет занятий физической культуры, как одно из средств решения проблем со здоровьем современной молодежи.

**L.A. Gayevskaya**

## **THE IMPORTANCE OF PHYSICAL CULTURE IN LIFE A MODERN STUDENT**

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: physical culture, survey, students, modern world.

This article examines the importance of physical culture for students in the modern world. The main diseases that are present in modern youth, as well as lifestyle. The priority of physical education classes as one of the means of solving health problems of modern youth.

Современный ритм жизни ставит перед молодым поколением множество вызовов: быстрый темп, стресс, не всегда здоровое питание и недостаток физической активности. В таких условиях физическая культура становится одним из ключевых элементов здорового образа жизни.

Физическое здоровье. Поддержание физической формы — это не только красивое тело, но и здоровые органы и системы. Регулярные физические нагрузки укрепляют сердце, сосуды, улучшают работу легких и повышают общий иммунитет.

Психоэмоциональное состояние. Физическая активность стимулирует выработку эндорфинов — "гормонов счастья". Это помогает бороться со стрессом, депрессией и улучшает настроение. Спорт также улучшает качество сна, делая его более глубоким и расслабляющим.

Социальные аспекты. Физическая культура часто подразумевает командные виды спорта, что помогает укреплять социальные связи, развивать коммуникативные навыки и учиться работать в команде.

Развитие личности. Через спорт молодой человек учится дисциплине, находит мотивацию для достижения целей и ставит перед собой новые вызовы.

Профилактика заболеваний. В эпоху сидячего образа жизни и компьютерной зависимости риск развития многих заболеваний, таких как ожирение, диабет, проблемы с

---

позвоночником, значительно возрастает. Регулярные занятия физкультурой являются лучшей профилактикой.

Улучшение качества жизни. Занятия спортом делают человека более активным, энергичным и жизнерадостным. Это открывает перед молодым человеком новые горизонты и возможности.

Физическая культура играет значительную роль в жизни современного студента, оказывая влияние на физическое, психологическое и социальное состояние молодого человека. Вот некоторые из основных аспектов влияния:

1. Физическое состояние: Регулярные физические упражнения помогают студентам поддерживать свою физическую форму, улучшают работу сердца, легких и других важных систем организма. Это также помогает укрепить иммунную систему и снизить риск различных заболеваний.
2. Психологическое состояние: Физическая активность стимулирует выработку эндорфинов – "гормонов счастья", что помогает бороться со стрессом, улучшает настроение и снижает риск развития депрессии. Для студентов, сталкивающихся с давлением экзаменов и академической нагрузкой, это особенно важно.
3. Концентрация и память: Некоторые исследования показали, что регулярная физическая активность может улучшать когнитивные функции, включая концентрацию, память и способность к обучению.
4. Социальные связи: Занятия спортом и командными играми помогают студентам налаживать социальные связи, учат работать в команде, развивают лидерские качества и умение общаться.
5. Дисциплина и самоорганизация: Постоянная тренировка и занятия физической культурой требуют дисциплины и планирования, что может переноситься и на другие аспекты жизни студента, такие как учеба или работа.
6. Сон: Физическая активность помогает улучшить качество сна, что особенно важно для студентов, чье образование и благополучие зависят от отдыха и восстановления.
7. Самооценка: Регулярное занятие спортом может повысить самооценку и уверенность в себе у студентов, улучшая их социальное взаимодействие и академические достижения.

В целом, физическая культура является интегральной частью благополучия и развития современного студента. Она может помочь молодым людям не только поддерживать здоровье, но и справляться с академическими и социальными вызовами.

Физическая культура является главным компонентом в здоровье человека. Необходимо придерживаться активного образа жизни для развития выносливости, иммунитета, и поддержания многих систем жизнедеятельности. Если бы физической культуры как дисциплины не было в университетах, то здоровье студентов было бы на очень низком уровне!

Физическая культура играет важную роль в жизни современного молодого человека, предоставляя инструменты для поддержания физического и психоэмоционального здоровья. В мире, где забота о себе становится все более актуальной, не стоит забывать о важности регулярных физических нагрузок. Поэтому значение физической культуры в развитии здорового образа жизни огромно.

## СПИСОК ЛИТЕРАТУРЫ

1. World Health Organization. Regional Office for Europe. Health literacy. Convincing facts. 2018. [http://www.euro.who.int/\\_\\_data/assets/pdf\\_file/0010/254377/Health\\_Literacy\\_RU\\_web.pdf](http://www.euro.who.int/__data/assets/pdf_file/0010/254377/Health_Literacy_RU_web.pdf)

- 
2. Birzhakov M.B. Introduction to tourism. M. – SPb., 2011.
  3. Vasilyeva O.S., Pravdina L.R., Litvinenko S.N. The book about new physical culture (health-improving possibilities of physical culture). Rostov-on-Don, 2010.
  4. Maslyakov V.A., Matyazhev V.S. Mass physical culture at the university. M., 1991.

**П.С. Шевчук<sup>1,2</sup>, О.А. Решетникова<sup>1,3</sup>**

**ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ МЕЖВЕДОМСТВЕННОГО  
ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ В КОНТЕКСТЕ РЕАЛИЗАЦИИ  
КОНЦЕПЦИИ «ЕДИНОГО ОКНА»**

Ростовский филиал Российской таможенной академии, Ростов-на-Дону, Россия<sup>1</sup>  
Донской государственный технический университет, Ростов-на-Дону, Россия<sup>2</sup>  
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО  
«Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия<sup>3</sup>

Ключевые слова: система межведомственного электронного взаимодействия, федеральные органы исполнительной власти, национальный механизм «единого окна», электронный документооборот, технологии «блокчейн».

В статье рассмотрены проблемы и актуальные тенденции развития системы межведомственного электронного взаимодействия (СМЭВ) в контексте реализации концепции «единого окна», представлены механизмы прослеживаемости товаров при информационном взаимодействии таможенных и налоговых органов на основе технологии «блокчейн», что позволит сократить время и повысить эффективность проведения таможенного контроля после выпуска товаров (ТКПВТ) и объективно приведет к снижению нагрузки на таможенные органы.

**P.S. Shevchuk<sup>1,2</sup>, O.A. Reshetnikova<sup>1,3</sup>**

**IMPROVING THE EFFICIENCY OF THE SYSTEM OF INTERDEPARTMENTAL  
ELECTRONIC INTERACTION IN THE CONTEXT OF THE IMPLEMENTATION OF  
THE "SINGLE WINDOW" CONCEPT**

Rostov Branch of the Russian Customs Academy, Rostov-on-Don, Russia<sup>1</sup>  
Don State Technical University, Rostov-on-Don, Russia<sup>2</sup>  
North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia<sup>3</sup>

Keywords: system of interdepartmental electronic interaction, federal executive authorities, national single window mechanism, electronic document management, blockchain technologies.

The article discusses the problems and current trends in the development of the system of interdepartmental electronic interaction in the context of the implementation of the concept of "single window", presents the mechanisms of traceability of goods in the information interaction of customs and tax authorities based on the technology "blockchain", which will reduce the time and improve the efficiency of customs control after the release of goods (TKPVT) and objectively lead to a decrease in the burden on the customs authorities.

## **1. Введение.**

Современные информационные таможенные технологии, реализация которых осуществляется в рамках системы межведомственного электронного взаимодействия (СМЭВ) активно применяются в Федеральной таможенной службе России (ФТС России). Как один из ключевых контролирующих федеральных органов исполнительной власти (ФОИВ), ФТС России обладает большим потенциалом развития технологий на основе принципов межведомственного взаимодействия, «одного окна», автоматизации и интеллектуализации процессов, реализация которых – важная составляющая целевого ориентира № 1 «полномасштабная цифровизация и автоматизация деятельности таможенных органов» и таких стратегических направлений, представленных в Стратегии развития таможенной службы Российской Федерации до 2030 года (Стратегия 2030), как «совершенствование таможенного администрирования», «современные технологии обеспечения соблюдения запретов и ограничений, соблюдения валютного законодательства, защиты прав на объекты интеллектуальной собственности в условиях развития интегрированных информационных цифровых систем», «совершенствование информационно-технического обеспечения таможенных органов и информационной безопасности». В реализации данных стратегических направлений особое место занимает развитие СМЭВ [1].

Таким образом, актуальность исследования заключается в том, что межведомственное электронное взаимодействие ФТС России с иными ФОИВ является важным условием автоматизации и интеллектуализации системы таможенного администрирования. Дальнейшее развитие СМЭВ обеспечит эффективное взаимодействие ФОИВ и всех заинтересованных лиц.

Цель настоящей статьи – определить проблемы межведомственного взаимодействия ФТС России с иными ФОИВ и пути их решения в условиях цифровизации и интеллектуализации системы таможенного администрирования.

## **2. Развитие системы межведомственного электронного взаимодействия.**

На сегодняшнем этапе развития в рамках Евразийского экономического союза (ЕАЭС) разработаны основные документы по развитию механизма «единого окна» в странах ЕАЭС:

1. Описание эталонной модели национального механизма «единого окна» в системе регулирования внешнеэкономической деятельности [2].
2. Основные направления развития механизма «единого окна» в системе регулирования внешнеэкономической деятельности (ВЭД) [3].

В 2015 году Высший Евразийский экономический совет утвердил эталонную модель национального механизма «единого окна», которая предполагает взаимодействие по трем основным направлениям: бизнес – бизнес (B2B), бизнес – государство (B2G/G2B), государство – государство (G2G).

Цель реализации эталонной модели является создание инновационного трансграничного интеллектуального механизма, позволяющего реализовать получение заинтересованными лицами комплекса государственных услуг при совершении внешнеторговых операций в процессе взаимодействия с контролирующими органами и (или) уполномоченными организациями стран ЕАЭС.

Эталонная модель национального механизма «единого окна» является инструментом упрощения внешнеторговых процедур в целях оптимизации административных процедур, связанных с реализацией ВЭД, и создания условий для осуществления электронных операций, и электронной коммерции. В этой связи на рис. 1 отражены преимущества эталонной модели механизма «единого окна».



Рисунок 1. Преимущества эталонной модели механизма «единого окна»

Внедрение системы «единого окна» – глобальный и достаточно сложный процесс, который обусловлен трудностями, финансового, технического и субъективного характера. Однако полномасштабное внедрение данной системы позволит вывести механизм предоставления государственных, в том числе таможенных услуг – на качественный новый уровень.

Обобщим основные проблемы развития СМЭВ в контексте реализации механизма «единого окна» в системе таможенного администрирования:

- недостаточная унификация законодательства в области применения информационных систем и технологий;
- слабая координация участников, вовлеченных в процесс;
- разный уровень технической оснащенности информационных систем государственных органов;
- отсутствует единый орган;
- отсутствует единый набор данных и единый пропускной канал;
- отсутствует межведомственная СУР;
- сохраняются требования о предоставлении бумажных документов.

### **3. Интеллектуальный механизм «единого окна».**

Создаваемый интеллектуальный механизм «единого окна» должен охватывать экспортные, импортные и транзитные операции. В отношении импорта товаров ФТС России большинство таможенных операций переведено в электронный вид. В части транзитного компонента будет создана межотраслевая территориально-распределительная цифровая платформа для поддержки международных транспортных коридоров. В соответствии с Указом Президента Российской Федерации от 7 мая 2018 г. № 204 в первую очередь будет реализовываться экспортный сегмент механизма «единого окна» в формате федерального проекта «Системные меры развития международной кооперации и экспорта» национальной программы по международной кооперации и экспорту [4]. Так, с конца 2020 г. была запущена система в режиме «одного окна» для компаний, занимающихся экспортом продукции, которая позволяет предпринимателям в формате «онлайн» оформлять документы по ВЭД путем единого обращения в различные ведомства. Такая цифровая платформа нацелена на последующее объединение всех государственных сервисов в сфере экспорта. Данный механизм осуществляется на базе

---

государственного института поддержки несырьевого неэнергетического экспорта – Российского экспортного центра. Основным преимуществом платформы, безусловно, является сокращение временных и трудовых ресурсов компаний-экспортёров, поскольку оформление подачи заявления занимает несколько минут, что существенно меньше ручного сбора и обработки документов.

В системе «Одно окно» в цифровом виде представлены услуги и сервисы, необходимые компании-экспортеру для решения основных задач бизнеса на каждом этапе экспортного цикла. Для взаимодействия с различными ведомствами экспортеру достаточно один раз ввести в систему необходимые данные, а затем получать необходимые услуги.

Услуги, которые можно получить через данный сервис, регламентированы Распоряжением Правительства РФ от 8 июля 2020 г. № 1776-р [5]. Среди услуг, непосредственно связанных с налогообложением экспортной деятельности – это проверка обоснованности применения налоговой ставки 0 процентов по НДС в отношении операций по реализации товаров, вывезенных в таможенной процедуре экспорт. Данную функцию выполняет ФНС России, основной направленностью которой является:

- формирование пакета документов (информации, сведений) для подачи в налоговый орган;
- проведение предварительной проверки правильности заполнения налоговой декларации (форматно-логический контроль), сверка подтверждающих документов (информации, сведений) с базами данных таможенных органов;
- получение информации о результатах предварительной проверки;
- подача пакета документов (информации, сведений) в налоговый орган по телекоммуникационным каналам связи через оператора электронного документооборота;
- обмен информацией (документами) в рамках камеральной проверки с использованием телекоммуникационных каналов связи оператора электронного документооборота;
- формирование заявления о возврате суммы НДС и его направление в адрес налогового органа по телекоммуникационным каналам связи через оператора электронного документооборота.

Переход от традиционного НДС к цифровому на основе smart-систем позволит создать систему универсального взимания косвенного налога и возможности его возмещения без вмешательства человеческого фактора. В этом направлении особую актуальность приобретает внедрение проактивного режима оказания государственной услуги по возврату НДС при экспорте товаров, заключающегося в беззаявительном характере предоставления услуге: получателю такая услуга предоставляется по умолчанию при соблюдении всех необходимых условий. В этой связи требуется интеграция баз данных ФТС и ФНС России с развитым механизмом автоматизации получения необходимой информации [6 - 8].

В развитии проактивного режима предоставления государственных услуг у ФТС России уже есть практический опыт. Так, развитие информационных таможенных технологий позволило перевести уплату таможенных платежей в цифровую плоскость. Переход на единые лицевые счета позволил при распоряжении денежными средствами не указывать в ЭДТ платежные документы. Распоряжением на уплату таможенных платежей являлось указание в таможенном документе ИНН. Перевод сведений о движении денежных средств в электронный вид дал возможность реализовать информационные сервисы личного кабинета участника ВЭД, которые позволяют автоматически получать справочную информацию об остатках денежных средств, а также об их поступлении и расходовании. На сегодняшний день таможенные органы имеют возможность в проактивном режиме направлять в личный кабинет участника ВЭД информацию о зачете



---

излишне уплаченных (взысканных) таможенных платежей в авансовые платежи, а также при начислении процентов.

Большой потенциал развития СМЭВ в контексте реализации концепции «единого окна» видится по направлению информационного взаимодействия таможенных органов и иных ФОИВ в пункте пропуска, в рамках которого важным является внедрение инструментов «интеллектуального» пункта пропуска, а именно:

1. Сочетание различных субтехнологий сквозных цифровых технологий, создаваемых в рамках национального проекта «Цифровая экономика, при проектировании «интеллектуального» пункта пропуска.

2. Формирование единой отраслевой цифровой платформы проведения таможенного контроля на базе ГЦОД ФТС России, представляющей собой механизм «единого окна», позволяющий реализовать однократное представление сведений в виде предварительной ЭДТ, объединить физические сигналы различных источников информации от технических средств таможенного контроля, таких как системы радиационного и весогабаритного контроля, инспекционно-досмотровые комплексы, и информационные источники (базы данных) контролирующих органов, обеспечить применение межведомственной системы управления рисками (СУР) [9]. Данная цифровая платформа позволит повысить степень автоматизации процессов совершения таможенных операций и таможенного контроля в пункте пропуска.

3. Для последующего совершенствования бизнес-процессов в «интеллектуальном» пункте пропуска, моделирования новых процессов и задач необходимо создание на отраслевой цифровой платформы Главного центра обработки данных (ГЦОД) ФТС России виртуальной модели «интеллектуального» пункта пропуска, являющейся его «цифровым двойником».

В рамках развития национальных механизма «единого окна» в системе таможенного администрирования необходимо:

- усилить координацию между ФОИВ и иными уполномоченными организациями;
- усилить интеграцию баз данных ФОИВ;
- унифицировать структуру информации в рамках информационного обмена;
- интегрировать отдельные механизмы «единого окна»;
- обеспечить информационную безопасность механизма «единого окна» на основе технологии «блокчейн» в рамках осуществления документальной проверки, которая может производиться через шифрование электронных сертификатов и размещения их в блокчейн ФОИВ, после чего производится сверка в системе, сертификаты хешируются, сверяются и в случае совпадения хэш-кодов считывается информация, необходимая для осуществления контроля по прослеживаемости товаров.

Сопряжение национальных механизмов «единого окна» в рамках ЕАЭС с последующим формированием наднационального механизма «единого окна» требует [10 - 12]:

- унификацию законодательств стран ЕАЭС в области применения информационных системы и технологий;
- полномасштабный переход на электронное представление документов и сведений в странах ЕАЭС;
- реализацию совершенной системы выборочного контроля на основе применения «интеллектуальной» СУР;
- утверждение оператора наднационального механизма «единого окна» с целью обеспечения его бесперебойной работы;
- обеспечения корректного функционирования системы документооборота и межведомственного взаимодействия с иными государственными органами и др.

### **Заключение.**

Таким образом, реализация СМЭВ в рамках концепции «единого окна» требует определенных практических решений, связанных усилением взаимодействия ФТС и ФНС России, а также иных ведомств, что позволит повысить качество предоставления государственных услуг, в том числе за счет внедрения и расширения практики применения проактивного режима оказания услуг в системе таможенного администрирования. Большую роль в развитии СМЭВ на принципах однократного представления сведений играет внедрение единой отраслевой цифровой платформы проведения таможенного контроля, представляющей собой механизм «единого окна» в пункте пропуска и позволяющей автоматизировать большую часть бизнес-процессов. Дальнейшее развитие национального механизма «единого окна» должно быть обеспечено усилением координации ФОИВ, последующей интеграцией баз данных контролирующих органов, унификацией структуры запрашиваемой информации, информационной безопасностью системы на основе технологии «блокчейн». Формирование наднационального механизма «единого окна» должно быть обеспечено унификацией законодательств стран ЕАЭС, полномасштабным переходом на электронный документооборот, усилением координации ведомств по сопряжению национальных механизмов «единого окна».

Реализация СМЭВ в рамках концепции «единого окна» требует определенных практических решений, связанных усилением взаимодействия ФТС и ФНС России, а также иных ведомств, что позволит повысить качество предоставления государственных услуг, в том числе за счет внедрения и расширения практики применения проактивного режима оказания услуг в системе таможенного администрирования. Большую роль в развитии СМЭВ на принципах однократного представления сведений играет внедрение единой отраслевой цифровой платформы проведения таможенного контроля, представляющей собой механизм «единого окна» в пункте пропуска и позволяющей автоматизировать большую часть бизнес-процессов. Дальнейшее развитие национального механизма «единого окна» должно быть обеспечено усилением координации ФОИВ, последующей интеграцией баз данных контролирующих органов, унификацией структуры запрашиваемой информации, информационной безопасностью системы на основе технологии «блокчейн». Формирование наднационального механизма «единого окна» должно быть обеспечено унификацией законодательств стран ЕАЭС, полномасштабным переходом на электронный документооборот, усилением координации ведомств по сопряжению национальных механизмов «единого окна».

### **СПИСОК ЛИТЕРАТУРЫ**

1. Стратегия развития таможенной службы Российской Федерации до 2030 года. [Электронный ресурс] // <http://government.ru/docs/all/128068>.
2. Решение Евразийского межправительственного совета от 30.04.2019 № 6 «Об Описании эталонной модели национального механизма «единого окна» в системе регулирования внешнеэкономической деятельности» [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>.
3. Решение Высшего совета ЕАЭС от 08.05.2015 № 19 «О плане мероприятий по реализации Основных направлений развития механизма «единого окна» в системе регулирования внешнеэкономической деятельности» [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>.
4. Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024

- 
- года» (ред. от 21.07.2020) [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>.
5. Распоряжение Правительства Российской Федерации от 08.07.2020 № 1776-р «Об утверждении перечня государственных и иных услуг (функций), административных и иных процедур в сфере внешнеэкономической деятельности, предоставление (исполнение) которых может осуществляться в электронной форме по принципу «одного окна» с использованием информационной системы «Одно окно», созданной акционерным обществом «Российский экспортный центр»» (ред. от 15.12.2022) [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>.
  6. Кацмарчук А.И., Шевчук П.С. Взаимодействие таможенных и налоговых органов при проведении таможенной проверки. В сборнике: Актуальные проблемы науки и техники. Сборник трудов по материалам XIII Международного конкурса научно-исследовательских работ. Уфа, 2023. С. 35-41.
  7. Черноусова В.Р., Шевчук П.С. Взаимодействие таможенных и налоговых органов при проведении таможенной проверки. В сборнике: Фундаментальные и прикладные аспекты развития современной науки. Сборник трудов по материалам XIII Международного конкурса научно-исследовательских работ. Уфа, 2023. С. 97-104.
  8. Беляева Е.Е., Шевчук П.С. Порядок проведения контроля таможенной стоимости после выпуска товаров. В сборнике: Фундаментальные и прикладные аспекты развития современной науки. Сборник трудов по материалам XIII Международного конкурса научно-исследовательских работ. Уфа, 2023. С. 105-110.
  9. Карелидзе Н.Х., Айтиев Б.Н., Шевчук П.С. Особенности применения системы управления рисками при проведении таможенного контроля после выпуска товаров. В сборнике: Актуальные проблемы науки и техники. Сборник трудов по материалам XIII Международного конкурса научно-исследовательских работ. Уфа, 2023. С. 29-34.
  10. Репина А.Д., Сатаров М.М., Шевчук П.С. Место таможенного контроля после выпуска товаров и направления его развития в РОССИЙСКОЙ ФЕДЕРАЦИИ. В сборнике: Актуальные проблемы науки и техники. сборник трудов по материалам VIII Международного конкурса научно-исследовательских работ. Уфа, 2022. С. 116-122.
  11. Логачева Ю.С., Шевчук П.С. Направления совершенствования таможенного контроля после выпуска товаров. В сборнике: Инновационные научные исследования в современном мире. сборник трудов по материалам VIII Всероссийского конкурса научно-исследовательских работ. Уфа, 2022. С. 32-36.
  12. Сигида Д.А., Шевчук А.П. Актуальные проблемы таможенного контроля после выпуска товаров и способы их решения. В сборнике: Инновационные подходы в решении научных проблем. Сборник трудов по материалам VIII Международного конкурса научно-исследовательских работ. Уфа, 2022. С. 54-60.

## ПРОБЛЕМЫ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАНИЕ

Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Ключевые слова: искусственный интеллект, образование, проблемы и преимущества, эффективный учебный процесс.

В работе рассмотрены возможности применения искусственного интеллекта (ИИ) в учебном процессе вуза, а также связанные с этим проблемы. Исследуются преимущества и недостатки внедрения образовательных инструментов, основанных на искусственном интеллекте. Результат исследования показывает, что с интеграцией ИИ в образование преподаватели получают не только новые возможности и инструменты работы, но и столкнутся с определенными трудностями. В работе приводятся некоторые предложения по преодолению потенциальных рисков, связанных с введением ИИ в учебный процесс.

N.O. Svetlichnaya, B.B. Konkin, L.A. Gayevskaya, A.M. Korshun

## PROBLEMS OF INTRODUCING ARTIFICIAL INTELLIGENCE IN THE EDUCATION

North Caucasus branch of Moscow Technical University  
of Communications and Informatics, Rostov-on-Don, Russia

Keywords: Artificial intelligence; education; advantages and problems, effective studying.

The paper examines the possibilities of using artificial intelligence (AI) in the educational process of a university, as well as related problems. Some advantages and disadvantages of introducing educational artificial intelligence-based tools are explored. The result of the study shows that teachers will receive new opportunities and work tools, and also face certain difficulties with the integration of AI in education. The paper provides some suggestions for preventing the potential risks related to the introduction of AI into the educational process.

Использование искусственного интеллекта (ИИ) в образовании — это инновационный способ создания персонализированного опыта обучения для учащихся. Кроме этого, ИИ полезен для преподавателей, поскольку открывает новые возможности в профессии, предоставляя ценные данные и средства обучения.

Внедрение технологий искусственного интеллекта в образование вызывает множество вопросов и споров. Некоторые пользователи обеспокоены потенциальными опасностями, которые ИИ представляет для молодежи и общества в целом, в то время как другие воодушевлены его возможностями для инноваций в образовании.

Помимо очевидных преимуществ ИИ в образовании, а именно адаптивное и персонализированное обучение, применение интеллектуальной игровой среды обучения, оценка решения задач в режиме реального времени, ИИ предлагает преподавателям новые инструменты ведения дисциплин. Использование искусственного интеллекта в образовании целесообразно благодаря его следующим инновационным возможностям:

**1. Иммерсивное обучение.** Данный метод обучения заключается в погружении в реальный контекст, где учащимся предлагается работать в симуляции реальной среды. Такой подход позволяет студентам повысить вовлеченность в процесс обучения, лучше контролировать свои результаты и получить реальный жизненный опыт. Иммерсивный

---

способ обучения позволяет устранить отвлекающие факторы и избавляет процесс обучения от монотонности за счет стимулирующей визуализации.

**2. Интеллектуальные системы обучения (ИСО).** ИСО используют компьютерную среду обучения, чтобы помочь учащимся учиться, практиковать или овладевать новыми навыками, предоставляя индивидуальное обучение в зависимости от их уровня владения определенной темой или набором навыков.

Доказано, что ИСО эффективно помогает учащимся улучшить свое понимание учебного материала посредством персонализированной обратной связи, которая предоставляет им немедленную информацию о том, насколько хорошо они понимают тему, изучаемую во время занятия, по сравнению с другими студентами, которые выполняют те же функции в искусственном пространстве, например, в виртуальной лаборатории.

**3. Формирование адаптивной группы.** Применение ИИ позволяет создавать адаптивные группы, в которых учащихся можно объединять в зависимости от их уровня подготовленности или сформированности навыков, тем самым давая им возможность учиться лучше и эффективнее.

Создание адаптивных групп дает одним студентам дополнительное время и возможность работать над освоением материала, а другим – двигаться в своем собственном темпе, не замедляя чью-либо работу. Это достигается путем назначения каждому учащемуся уникального плана обучения, основанного на его прогрессе и способностях. Это позволяет каждому студенту в одной и той же группе получать разные инструкции в зависимости от того, как он справляется с конкретными навыками или материалами.

**4. Интеллектуальная модерация.** Технология модерации предполагает применение активных методов обучения, что делает ее применение особенно актуальным в условиях реализации ФГОС, основанного на компетентностно-деятельностном подходе. Интеллектуальная модерация – это техника организации интерактивного общения, благодаря которой групповая работа становится более целенаправленной и структурированной. Данная технология может быть реализована в качестве интеллектуальных инструментов модерации онлайн-классов и курсов, которые обеспечат соответствующее вовлечение учащихся в учебный материал и при этом сведут к минимуму показатели отсева студентов из-за неуспеваемости.

**5. Обучение с использованием виртуальной реальности (VR).** ИИ делает возможными практические занятия в виртуальной реальности, которые позволяют студентам учиться, чувствуя себя погруженными в определенную среду или сценарий. Благодаря данной технологии, учащиеся получают захватывающую связь с учебным материалом и оказываются вовлеченными в процесс обучения. Например, применение VR на занятиях иностранного языка может иметь следующую форму: после видеолекции учащемуся предлагается применить полученные знания на практике. Надев шлем, он оказывается на типичном профессиональном мероприятии, где может поговорить последовательно с каждым из коллег. После завершения диалога система оценивает степень поддержки визуального контакта и предлагает мини-тест по услышанному материалу.

**6. Улучшение качества курса.** ИИ предлагает инновационный способ сделать образовательные курсы на всех уровнях более интересными. Искусственный интеллект может изменять содержание курса дисциплины, обеспечивать мгновенную обратную связь и оценивать интерес учащихся с помощью методов интерактивного обучения, которые в настоящее время недоступны в образовательных учреждениях. Искусственный интеллект способен улучшить существующие способы обучения, предоставляя учащимся другой опыт, чем они могли бы получить при традиционном методе обучения.

Искусственный интеллект уверенно входит в нашу жизнь, его использование в качестве образовательного инструмента имеет множество преимуществ. Вместе с тем

---

внедрение этих технологий ИИ сопряжено с рядом проблем. Среди них оснащение аудиторий соответствующим аппаратным и программным обеспечением и колоссальный объем подготовительной работы со стороны преподавателя по разработке тематики преподаваемой дисциплины с внедрением инструмента ИИ. Кроме этого, отмечаются определенные слабые стороны искусственного интеллекта в образовании. Некоторые из основных его недостатков перечислены ниже.

**1. Финансовые проблемы.** Одним из главных недостатков внедрения ИИ в образование являются финансовые проблемы. Потребуется покрыть весомые расходы на приобретение оборудования и программного обеспечения, которые могут поддерживать возможности ИИ, такие как инструменты распознавания лиц или обработки естественного языка, оборудование виртуальной реальности.

**2. Снижение человеческого взаимодействия, коммуникационный барьер и недостаток эмоционального интеллекта.** Использование ИИ приводит к тому, что во время занятий учащиеся теряют возможность практиковать и изучать социальные навыки, возможные лишь в условиях контакта с реальными людьми. В результате могут возникнуть языковые барьеры при общении с людьми, потому что машины не могут понять нас со всеми особенностями человеческого общения: использовать не только слова, но и жесты, мимику, которые обеспечивают контекст, подсказки относительно намерений собеседника, не требуя от него каких-либо конкретных объяснений, почему он сделал то или иное во время разговора.

Применение ИИ как образовательного инструмента может полностью исключить потребность в преподавателе и живом общении с ним. Однако в этой возможности кроется главный недостаток ИИ - отсутствие эмоционального интеллекта, а вместе с ним и социальные навыки, такие как эмпатия и коммуникативные навыки, проявляющиеся при взаимодействии с другим человеком при непосредственном контакте. Хочется надеяться, что новые технологии не смогут полностью заменить преподавателей, поскольку живое общение приносит нечто большее, чем просто знания, что невозможно реализовать средствами ИИ.

**3. Зависимость от искусственного интеллекта.** Искусственный интеллект может вызвать привыкание. Студенты могут потерять интерес к обучению, поскольку их больше интересуют устройства искусственного интеллекта, что является недостатком его использования в образовательных целях.

**4. Проблемы с данными искусственного интеллекта.** Невозможно предусмотреть все способы обучения учащихся, а преподавателям сложно найти единый алгоритм, удовлетворяющий потребности каждого студента. ИИ нуждается в большом количестве информации, чтобы компьютерная программа могла правильно обучаться, а этот процесс сопряжен с множеством проблем. Главная из них заключается в сборе качественных данных, так как обучающиеся могут неточно или неправильно отмечать ответы во время опросов. В дальнейшем для ИИ это предполагает серьезные проблемы по сбору данных.

**5. Снижение мыслительной способности студентов.** Использование инструментов ИИ приводит к тому, что лишает учащихся развития мыслительных способностей и делает их более зависимыми от технологий, что тормозит или полностью исключает формирование самостоятельности.

В попытках преодолеть перечисленные недостатки ИИ по отношению к учебной деятельности предлагаются следующие рекомендации:

- осуществлять образовательный процесс на основе проработанной и проанализированной обучающей системы;
- отслеживать влияние продуктов ИИ на самостоятельность обучающихся, их мыслительные способности, чтобы корректировать частоту и способ применения данных инструментов;
- учитывать влияние ИИ на психологическое состояние студентов;

- 
- комбинировать традиционное обучение с использованием ИИ, с целью разнообразить учебный процесс, обеспечить дополнительную мотивацию и вовлеченность в учебную деятельность.

Таким образом, искусственный интеллект предоставляет широкие возможности для образовательных процессов. Его применение позволяет значительно повысить результативность и качество образовательного процесса, а также профессионализм преподавателей. Однако необходимо осмотрительно подходить к внедрению ИИ в образование в целом и в учебный процесс каждого обучающегося, учитывая положительные стороны и потенциальные риски этих технологий. Баланс между инновациями и традиционными методами обучения – ключевой фактор для успешного влияния ИИ на процесс обучения и обеспечения лучшего образования для каждого студента, учитывая его индивидуальные возможности.

#### СПИСОК ЛИТЕРАТУРЫ

1. U.S. Department of Education, Office of Educational Technology, Artificial Intelligence and Future of Teaching and Learning: Insights and Recommendations, Washington, DC, 2023. <https://tech.ed.gov>
2. Research on Education and Media. Vol. 12, N. 1, Year 2020 - ISSN: 2037-0830 Artificial Intelligence in Education and Schools.
3. Искусственный интеллект в образовании. Бластим, 2023. <https://habr.com/ru/articles/740730/>