МЕЖДУНАРОДНЫЙ ЦЕНТР НАУЧНОГО СОТРУДНИЧЕСТВА
«НАУКА И ПРОСВЕЩЕНИЕ»

SCIENCE and EDUCATION
INTERNATIONAL CENTRE FOR SCIENTIFIC COOPERATION

WORLD SCIENCE: PROBLEMS AND INNOVATIONS

СБОРНИК СТАТЕЙ LXXXIII МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ
«WORLD SCIENCE: PROBLEMS AND INNOVATIONS»,
СОСТОЯВШЕЙСЯ 30 МАЯ 2025 Г. В Г. ПЕНЗА

ПЕНЗА
МЦНС «НАУКА И ПРОСВЕЩЕНИЕ»
2025

УДК 001.1
ББК 60
В75

Ответственный редактор:
Гуляев Герман Юрьевич, кандидат экономических наук

В75

WORLD SCIENCE: PROBLEMS AND INNOVATIONS: сборник статей LXXXIII Международной научно-практической конференции. – Пенза: МЦНС «Наука и Просвещение». – 2025. – 330 с.

ISBN 978-5-00236-936-2

Настоящий сборник составлен по материалам LXXXIII Международной научно-практической конференции «**WORLD SCIENCE: PROBLEMS AND INNOVATIONS**», состоявшейся 30 мая 2025 г. в г. Пенза. В сборнике научных трудов рассматриваются современные проблемы науки и практики применения результатов научных исследований.

Сборник предназначен для научных работников, преподавателей, аспирантов, магистрантов, студентов с целью использования в научной работе и учебной деятельности.

Ответственность за аутентичность и точность цитат, имен, названий и иных сведений, а также за соблюдение законодательства об интеллектуальной собственности несут авторы публикуемых материалов.

Полные тексты статей в открытом доступе размещены в Научной электронной библиотеке **Elibrary.ru** в соответствии с Договором №1096-04/2016К от 26.04.2016 г.

УДК 001.1
ББК 60

ISBN 978-5-00236-936-2

СОДЕРЖАНИЕ

ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ 10

КВАНТОВЫЕ АЛГОРИТМЫ: АЛГОРИТМ ШОРА, АЛГОРИТМ ГРОВЕРА И ИХ ЗНАЧЕНИЕ
МАКСИМОВ ИГОРЬ ВИТАЛЬЕВИЧ, ФАЙЗУЛЛИН КАМИЛЬ РАМИЛЕВИЧ 11

РОЛЬ МАТЕМАТИКИ В РАЗВИТИИ СОВРЕМЕННОЙ СОЦИОЛОГИИ
СЕРЕДА НАТАЛЬЯ ВЛАДИМИРОВНА, СЕРЕДА ДАНИИЛ ВАДИМОВИЧ 14

ТЕХНИЧЕСКИЕ НАУКИ 18

СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА НЕРАЗРУШАЮЩЕГО КОНТРОЛЯ В СТРОИТЕЛЬСТВЕ
ЗАХАРЫЧЕВ НИКИТА АЛЕКСАНДРОВИЧ 19

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЕКТА ДЛЯ АНАЛИЗА ТЕХНИК ДВИЖЕНИЙ В СПОРТЕ
ЗУБКОВА ВИКТОРИЯ МИХАЙЛОВНА 23

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ЗАЩИТЫ ПРОМЫШЛЕННЫХ IOT-УСТРОЙСТВ
КОВАЛЕРОВ ЯРОСЛАВ ДМИТРИЕВИЧ, КОЛЮЧКИН АНТОН АЛЕКСАНДРОВИЧ,
КУДРЯВЦЕВ ДАНИИЛ ПАВЛОВИЧ 27

РАЗРАБОТКА СТРУКТУРНОЙ И ПРИНЦИПИАЛЬНОЙ ЭЛЕКТРИЧЕСКИХ СХЕМ ИМПУЛЬСНЫЙ ПРЕОБРАЗОВАТЕЛЬ ПОСТОЯННОГО НАПРЯЖЕНИЯ ПОНИЖАЮЩЕГО ТИПА
ХАНМАГОМЕДОВ АНДРЕЙ ХАНМАГОМЕДОВИЧ, ВАСИЛЬЕВ ВЯЧЕСЛАВ ВАСИЛЬЕВИЧ,
ДОЕВ РОМАН ГЕННАДЬЕВИЧ, КАЛАГОВА СВЕТЛАНА КАЗБЕКОВНА 30

ВЗАИМНАЯ СИНХРОНИЗАЦИЯ СВЧ АВТОГЕНЕРАТОРОВ ДЛЯ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ЭНЕРГИИ
АНЬ ХА КУОК, КИ ФАМ 34

ПРАВИЛА ДОРОЖНОГО ДВИЖЕНИЯ В ДРЕВНЕМ КИТАЕ
ГУ ЧЭНЬФЭН, БИ ВЭНЬЕ 38

ЦИФРОВЫЕ ДВОЙНИКИ В ЭЛЕКТРОЭНЕРГЕТИКЕ: НЕЙРОСЕТЕВЫЕ МОДЕЛИ ДЛЯ МОНИТОРИНГА И ДИАГНОСТИКИ КАБЕЛЬНЫХ ЛИНИЙ
ГАЛИМЗЯНОВ ИЛСАФ ЗЯМИЛОВИЧ 42

ТИПЫ СИСТЕМ РЕГУЛИРОВАНИЯ ПОДАЧИ ТОПЛИВА В ГТУ
ТОМИНА ДИАНА АЛЕКСАНДРОВНА 46

МЕТОД ОМП НА ВЛ 6-35КВ ПО ПОКАЗАНИЯМ НАВЕДЕННОГО НАПРЯЖЕНИЯ
СТАВЦЕВ СЕРГЕЙ ПЕТРОВИЧ 49

ОБОРУДОВАНИЕ ДЛЯ ТЕРМООБРАБОТКИ ДРЕВЕСИНЫ
ОВЧИННИКОВА ТАТЬЯНА СЕРГЕЕВНА 54

АСПЕКТЫ ВНЕДРЕНИЯ АБСОРБЕНТОВ И АДСОРБЕНТОВ ПРИ ГАЗООТЧИСТКЕ
ВЯТКИНА ЯРОСЛАВА АЛЕКСЕЕВНА, ДЬЯЧУК АНАСТАСИЯ ИГОРЕВНА 61

ИССЛЕДОВАНИЕ КАТАЛИЗАТОРА ДЕГИДРИРОВАНИЯ КД-1 ИЗОАМИЛЕНОВ В ИЗОПРЕН
ЯУШЕВА ИЛЮЗА РАДИКОВНА, МУЛЮКОВА РУФИНА ФАТИХОВНА 65

АЛГОРИТМ РАЗРАБОТКИ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ ДЛЯ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ОТ КВАНТОВЫХ АТАК
ТАКСИМОВ АСКАР БОРАНБАЕВИЧ 68

ЭКСПЛУАТАЦИЯ ПОЖАРНЫХ РУКАВОВ
ИВАНОВ ИВАН АЛЕКСАНДРОВИЧ 75

РАЗВИТИЕ ГОРОДСКОГО РЕЛЬСОВОГО ТРАНСПОРТА В КИТАЕ
ЛЮ ЦЗЮНЬИ, ГУЛОМОВ РАМЗИДДИН ФАЗЛИДДИН УГЛИ,
ТИМОФЕЕВ ИЛЬЯ СЕРГЕЕВИЧ 78

ДИСТАНЦИОННОЕ ЗОНДИРОВАНИЕ ДЛЯ ОЦЕНКИ ЭВТРОФИКАЦИИ РЕКИ ВОЛГА В РАЙОНЕ УЛЬЯНОВСКА
КОЗЫРЕВ ВАЛЕРИЙ АЛЕКСАНДРОВИЧ 83

ДОБАВКИ В ПИЩЕВЫХ ПРОДУКТАХ
ДАДАШЕВ ИСА ХАСАНБЕКОВИЧ 88

СЕЛЬСКОХОЗЯЙСТВЕННЫЕ НАУКИ 96

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ДЛЯ КОНТРОЛЯ КАЧЕСТВА СЕЛЬСКОХОЗЯЙСТВЕННОЙ ПРОДУКЦИИ
ТХАЙ ВАЛЕРИЯ ДМИТРИЕВНА 97

ИСТОРИЧЕСКИЕ НАУКИ 100

СССР В ГОДЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ: МИФЫ И РЕАЛЬНОСТЬ
ХАЗИЕВА АЛСУ АЙРАТОВНА 101

ЭКОНОМИЧЕСКИЕ НАУКИ 104

ВЛИЯНИЕ ТЕКУЩЕГО УРОВНЯ УЧЕТНОЙ СТАВКИ НА ЭКОНОМИЧЕСКОЕ РАЗВИТИЕ РОССИИ
БОЙТУШ ОКСАНА АЛЕКСАНДРОВНА, РОМАНЧЕНКО МИХАИЛ ЕВГЕНЬЕВИЧ 105

ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ТЕКСТА ДЛЯ ПОДГОТОВКИ УПРАВЛЯЮЩЕЙ ИНФОРМАЦИИ
ПЕРЕЛЬМАН КАРИНА ЭДУАРДОВНА 110

ВЛИЯНИЕ ИНФЛЯЦИИ НА ПОКУПАТЕЛЬСКУЮ СПОСОБНОСТЬ НАСЕЛЕНИЯ В РОССИИ
НАДА М. А. 114

ВЛИЯНИЕ САНКЦИЙ НА КУРС РУБЛЯ
НАДА М. А. 117

СТРУКТУРНЫЕ ТРАНСФОРМАЦИИ В СОВРЕМЕННОЙ ЭКОНОМИКЕ: ВЛИЯНИЕ ЦИФРОВИЗАЦИИ, ГЛОБАЛИЗАЦИИ И УСТОЙЧИВОГО РАЗВИТИЯ НА ЭКОНОМИЧЕСКИЙ РОСТ
РАШНИКОВА ДАРЬЯ ДМИТРИЕВНА, НИГМАТЗЯНОВА ЛЕЙСАН РИНОТОВНА 120

НОВАЯ ПЕРСПЕКТИВА ИНВЕСТИЦИОННОЙ ПРИВЛЕКАТЕЛЬНОСТИ РЕГИОНА ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ДУНАЙ ДИАНА ДМИТРИЕВНА, КРИКУНОВ НИКОЛАЙ САБИРОВИЧ 125

ЦЕНТРАЛИЗОВАННЫЕ ФИНАНСЫ КАК ИНСТРУМЕНТ РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ФИНАНСОВОЙ ПОЛИТИКИ
ДУНАЙ ДИАНА ДМИТРИЕВА, ФОМЕНКО ПОЛИНА ВИКТОРОВНА 128

СОЦИАЛЬНО ОТВЕТСТВЕННЫЕ ИНВЕСТИЦИИ
ДУНАЙ ДИАНА ДМИТРИЕВНА, ШУЛЬГА ДИАНА НИКОЛАЕВНА 131

ЭВОЛЮЦИЯ УПРАВЛЕНЧЕСКОЙ МЫСЛИ: ОТ КЛАССИЧЕСКИХ ШКОЛ ДО СОВРЕМЕННЫХ ПОДХОДОВ
УРАЗБАЕВ ДАМИР АРСТАНОВИЧ 134

АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ РОССИЙСКОГО РЫНКА МУЛЬТИМЕДИЙНОГО ОБОРУДОВАНИЯ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ
КЛЯУЗОВ ДАНИЛ МИХАЙЛОВИЧ, ХОМЯКОВА МАРИЯ ВЯЧЕСЛАВОВНА 137

THE EFFECTIVENESS OF IMPORT SUBSTITUTION POLICY IN RUSSIA: ECONOMIC AND INSTITUTIONAL ASPECTS
BARDINA KRISTINA VALERIEVNA, IVANOVA ANGELINA EVGENIEVNA 140

РОЛЬ ЭКОНОМИЧЕСКОГО АНАЛИЗА В ФОРМИРОВАНИИ ТОВАРНОЙ ПОЛИТИКИ ПРЕДПРИЯТИЙ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА
АХПАШЕВА ЕЛИЗАВЕТА АНАТОЛЬЕВНА 145

ПРОБЛЕМНЫЕ АСПЕКТЫ ПРАКТИКИ УЧЕТА ФОРМИРОВАНИЯ СЕБЕСТОИМОСТИ И ПРОДАЖИ ПРОДУКЦИИ
ЗНАМЕНСКАЯ АЛЁНА ВИТАЛЬЕВНА 149

ФИЛОСОФСКИЕ НАУКИ 153

THE CORRELATION OF SCIENTIFIC AND RELIGIOUS KNOWLEDGE IN ABAI'S WORLDVIEW
KAIRATKYZY AIZAT 154

НОВЫЕ ТЕНДЕНЦИИ В КУЛЬТУРНОЙ ПОЛИТИКЕ С ТОЧКИ ЗРЕНИЯ КИТАЙСКОЙ МОДЕРНИЗАЦИИ
ЦЮЙ И 157

ПАРАДОКСЫ СВОБОДЫ СЛОВА В ЭПОХУ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ
ЮЩУК МАКСИМ ИВАНОВИЧ 162

ФИЛОЛОГИЧЕСКИЕ НАУКИ 165

COMMUNICATIVE STRATEGIES AND TACTICS IN ENGLISH-LANGUAGE POLITICAL DISCOURSE
KOLPAKOV ARTEM ALEKSANDROVICH 166

ПЕЙОРАТИВЫ МАСКИРОВКИ МАТЕРИ АЛЕКСАНДРА НЕВСКОГО
РЕПКО СЕРГЕЙ ИВАНОВИЧ 169

STUDYING CONTEMPORARY POETRY IN LITERATURE ELECTIVES AT SCHOOL
KUZINA EKATERINA ROMANOVNA 190

СЕМАНТИЧЕСКАЯ СТРУКТУРА ГЛАГОЛА ‘ТЯНУТЬ’ В ХАНТЫЙСКОМ ЯЗЫКЕ (НА ФОНЕ МАНСИЙСКОГО ЯЗЫКА)
СОЛОВАР ВАЛЕНТИНА НИКОЛАЕВНА 193

СТРУКТУРНО-ФУНКЦИОНАЛЬНЫЕ НАПРАВЛЕНИЯ ЛИНГВИСТИКИ ТЕКСТА: ГРАММАТИЧЕСКИЕ, СЕМАНТИЧЕСКИЕ, ПРАГМАТИЧЕСКИЕ И КОГНИТИВНЫЕ АСПЕКТЫ
ГЮНАЙ МИРЗАЗАДЕ ИЛЬГАР КЫЗЫ 196

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В МЕДИЦИНЕ И МЕДИЦИНСКОМ ПЕРЕВОДЕ
ХАБИБУЛЛИНА САЛИМА РИФАТОВНА 199

ЮРИДИЧЕСКИЕ НАУКИ 203

СОВЕРШЕНСТВОВАНИЕ ПРИМЕНЕНИЯ УК РФ В РАМКАХ СТРАТЕГИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И БОРЬБЫ С ЭКСТРЕМИЗМОМ В РФ
БАКШЕЕВА ЮЛИЯ ВЛАДИМИРОВНА 204

АНАЛИЗ И ОЦЕНКА ЭФФЕКТИВНОСТИ АНТИКОРРУПЦИОННОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ
МОНГУШ ДОЛУМА ОЛЕГОВНА 212

КРАТКАЯ ИСТОРИЯ УГОЛОВНОГО ПРАВА: ОТ «РУССКОЙ ПРАВДЫ» ДО УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ
БОГДАНОВА ЕЛЕНА ЕВГЕНЬЕВНА, ЛЯХОВА АНЖЕЛИКА ИВАНОВНА 217

ДИФФЕРЕНЦИАЦИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ТРУДА ЖЕНЩИН
ПОПОВА ЕЛИЗАВЕТА НИКОЛАЕВНА 220

ПИСЬМЕННЫЕ ДОКАЗАТЕЛЬСТВА КАК ОСНОВНОЕ СРЕДСТВО ДОКАЗЫВАНИЯ В МЕЖДУНАРОДНОМ АРБИТРАЖЕ
БУРЖИМСКИЙ ОЛЕГ АЛЕКСАНДРОВИЧ, ТУХВАТУЛЛИН АРТЕМ АЗАТОВИЧ 224

ЦИФРОВИЗАЦИЯ В УГОЛОВНОМ ПРОЦЕССЕ, ПЕРСПЕКТИВЫ И РИСКИ
МАСЛОВА АНАСТАСИЯ ДМИТРИЕВНА, ВАСИЛЬКОВА АЛИНА СЕРГЕЕВНА 227

ЛИНГВИСТИЧЕСКИЕ АСПЕКТЫ ПОНИМАНИЯ ОРИГИНАЛЬНЫХ ИНОЯЗЫЧНЫХ ТЕКСТОВ В ПРОЦЕССЕ ИХ ПЕРЕВОДА
АНИКИН АРТЕМ СЕРГЕЕВИЧ 230

НЕКОТОРЫЕ ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ ПОДСУДНОСТИ ПО ПОТРЕБИТЕЛЬСКИМ СПОРАМ (НА ПРИМЕРЕ ИСКОВ К ПЕРЕВОЗЧИКАМ)
ГОРДОН ЮЛИЯ АНАТОЛЬЕВНА 233

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПРАВА НЕСОВЕРШЕННОЛЕТНИХ НА ЖИЛЬЕ В РЕСПУБЛИКЕ ТЫВА
БАПАА СЕВИЛ ВЯЧЕСЛАВОВНА 238

ПЕДАГОГИЧЕСКИЕ НАУКИ 243

FORMATION AND DEVELOPMENT OF SOCIAL ACTIVITY OF SCHOOLCHILDREN THROUGH EXTRACURRICULAR ACTIVITIES
POZHIDAEV VITALIY VADIMOVICH 244

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБРАЗОВАНИИ
КИЧИБЕКОВА САБИНА ЗАУРОВНА 247

ПРОФОРИЕНТАЦИОННО-ДЕЛОВАЯ ИГРА КАК СРЕДСТВО ПОВЫШЕНИЯ РЕЧЕВОЙ АКТИВНОСТИ НА УРОКЕ АНГЛИЙСКОГО ЯЗЫКА НА СРЕДНЕЙ СТУПЕНИ ОБУЧЕНИЯ
ШАМСУДИНОВА С. Э., СУЛЕБАНОВА Н. А. 249

THE ROLE OF A PRINCIPAL IN CREATING AN EFFECTIVE TEACHER COLLABORATION SYSTEM
LEBEDEVA VIKTORIIA ALEXSANDROVNA 253

ПРОЯВЛЕНИЕ ДИСГРАФИИ У МЛАДШИХ ШКОЛЬНИКОВ
АЛАНДАРЕНКО ПОЛИНА АЛЕКСАНДРОВНА 256

ИСТОРИЯ РАЗВИТИЯ ФИЗИЧЕСКОЙ КУЛЬТУРЫ КАК ДИСЦИПЛИНЫ
СЕЛЮК ВЛАДИСЛАВА ВИТАЛЬЕВНА 259

ЗАПУСК РЕЧЕВОГО РАЗВИТИЯ. ОСНОВНЫЕ ЭТАПЫ И ОСОБЕННОСТИ КОРРЕКЦИОННО-РАЗВИВАЮЩЕЙ РАБОТЫ
СЕМЕНОВА ЕЛЕНА ВАЛЕНТИНОВНА 263

ФОРМИРОВАНИЕ ЗДОРОВЬЕСБЕРЕГАЮЩИХ КОМПЕТЕНЦИЙ У БУДУЩИХ ЛОГОПЕДОВ
КОВАЛЬ АННА НИКОЛАЕВНА 266

РАЗВИТИЕ ЗРИТЕЛЬНОГО ВОСПРИЯТИЯ У ДЕТЕЙ СТАРШЕГО ДОШКОЛЬНОГО ВОЗРАСТА С УМСТВЕННОЙ ОТСТАЛОСТЬЮ
БАТУРИНА АЛЁНА ИВАНОВНА, ЯКУБОВА ФЕРИДЕ РУСТЕМОВНА 270

ЛОГОПЕДИЧЕСКАЯ РАБОТА ПО ПРЕОДОЛЕНИЮ ДИЗОРФОГРАФИИ У МЛАДШИХ ШКОЛЬНИКОВ С ДИЗАРТРИЕЙ
ИБРАГИМОВА АЛИНА МАРАТОВНА 273

ПРЕДМЕТНАЯ СПЕЦИФИКА ФОРМИРОВАНИЯ ЦИФРОВОГО ЭТИКЕТА У МЛАДШИХ ШКОЛЬНИКОВ
НИКИТИНА ЕЛЕНА ЮРЬЕВНА, ВИНОКУРОВА СОФИЯ ВЛАДИМИРОВНА 276

ПРАВОВОЕ ПРОСВЕЩЕНИЕ ПЕДАГОГОВ, КАК ОСНОВА ПОВЫШЕНИЯ КАЧЕСТВА ОБУЧЕНИЯ В ОБЩЕОБРАЗОВАТЕЛЬНОЙ ШКОЛЕ
ШИБАНОВА ЕЛЕНА СЕРГЕЕВНА 281

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ В ПОДГОТОВКЕ ДЕФЕКТОЛОГОВ И ФОРМИРОВАНИИ ИХ ПРОФЕССИОНАЛЬНОЙ ТРАЕКТОРИИ
ПЛОХИХ МАРИЯ СЕРГЕЕВНА 284

МЕДИТАТИВНЫЙ ЭФФЕКТ ОБУЧЕНИЯ И КОНЦЕНТРАЦИЯ ВНИМАНИЯ УЧЕНИКОВ ПРИ ИЗУЧЕНИИ КИТАЙСКОЙ КАЛЛИГРАФИИ В НАЧАЛЬНОЙ ШКОЛЕ
ЯО ЮЙЛУН, ТУН СИНЬ 287

ИСТОРИЧЕСКОЕ НАСЛЕДИЕ КАК ОСНОВА ПАТРИОТИЧЕСКОГО ВОСПИТАНИЯ МОЛОДЁЖИ
ГАФИАТУЛЛИНА ЛЕЙСАН ГУМЕРОВНА, ГАФУРБАЕВ ИСЛАМ РАМИЛЕВИЧ 292

МЕДИЦИНСКИЕ НАУКИ 295

ФИБРИЛЛЯЦИЯ ПРЕДСЕРДИЙ ПРИ РАЗЛИЧНЫХ ФОРМАХ ГИПЕРТИРЕОЗА
БАБАН ЕЛИЗАВЕТА ВИТАЛЬЕВНА, СТОЛЯРОВА ДАРЬЯ СЕРГЕЕВНА 296

АРХИТЕКТУРА 299

ПОИСК РЕШЕНИЙ ОБЕСПЕЧЕНИЯ МНОГОФУНКЦИОНАЛЬНОСТИ КВАРТИРЫ ДЛЯ СРЕДНЕСРОЧНОГО ПРОЖИВАНИЯ УЧЕНЫХ
ЭЙРИХ НАТАЛЬЯ АНДРЕЕВНА 300

ЗЕЛЕНАЯ АРХИТЕКТУРА В УСЛОВИЯХ ПЛОТНОЙ ЗАСТРОЙКИ: АНАЛИЗ ПОДХОДОВ В МОСКВЕ И ЕВРОПЕЙСКИХ ГОРОДАХ
ЛЮБИН ЕГОР ДМИТРИЕВИЧ 304

ПСИХОЛОГИЧЕСКИЕ НАУКИ 310

ПСИХОЛОГИЧЕСКАЯ КОМПЕТЕНЦИЯ РУКОВОДИТЕЛЯ КАК КРИТЕРИЙ ПРОФЕССИОНАЛИЗМА
НОВОЛОКИН КОНСТАНТИН ИГОРЕВИЧ 311

ОСОБЕННОСТИ ВРЕМЕННОЙ ПЕРСПЕКТИВЫ У СОВРЕМЕННЫХ СТУДЕНТОВ РАЗНЫХ ВОЗРАСТНЫХ КАТЕГОРИЙ
БАЗОЯН ЗОЯ АЛЕКСАНДРОВНА 314

ПСИХОЛОГИЯ ЗДОРОВОГО ОБРАЗА ЖИЗНИ В ПОДРОСТКОВОЙ СРЕДЕ
ШИЛИНА АНТОНИНА ДЕНИСОВНА 317

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ КОГНИТИВНО-ПОВЕДЕНЧЕСКОЙ ТЕРАПИИ (CBT) И ТЕРАПИИ ПРИНЯТИЯ И ОТВЕТСТВЕННОСТИ (ACT) В ПОВЫШЕНИИ САМОРЕГУЛЯЦИИ СТУДЕНТОВ
ЧЕХРЕ АМИРХОССЕЙН 320

СОЦИОЛОГИЧЕСКИЕ НАУКИ 326

СПЕЦИФИКА МОТИВАЦИИ ТРУДА В МАЛОМ РОССИЙСКОМ ПРЕДПРИНИМАТЕЛЬСТВЕ
БАЯЗИТОВ СПАРТАК РИНАТОВИЧ 327

УДК 004

АЛГОРИТМ РАЗРАБОТКИ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ ДЛЯ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ОТ КВАНТОВЫХ АТАК

ТАКСИМОВ АСКАР БОРАНБАЕВИЧ
магистр наук строительства и городского проектирования в развитии,
Университетский колледж Лондона,
руководитель
Городской центр мониторинга и оперативного реагирования при акимате города Астаны

Аннотация: В статье рассматривается проблема обеспечения информационной безопасности критической инфраструктуры в условиях появления квантовых вычислений. Проведён анализ угроз, связанных с возможностью взлома существующих криптографических алгоритмов при помощи квантовых компьютеров. Представлены классы постквантовых алгоритмов, пригодных для замены традиционных схем защиты, с акцентом на решётчатые криптосистемы как наиболее сбалансированные по криптостойкости, производительности и применимости в условиях ограниченных ресурсов. Основной результат работы – авторский алгоритм LatticeCI, предназначенный для реализации квантово-устойчивого обмена ключами в информационных системах объектов критической инфраструктуры. Описана концепция алгоритма, приведён псевдокод, даны расчёты по параметрам безопасности, объёмам данных и временным затратам. Продемонстрирована возможность внедрения алгоритма в реальную среду без значительных изменений аппаратного обеспечения.
Ключевые слова: постквантовая криптография, критическая инфраструктура, квантовые атаки, решётчатая криптография, обмен ключами, защита информации, LatticeCI, устойчивость к квантовым вычислениям, NTRU, квантовая безопасность.

ALGORITHM FOR DEVELOPING POST-QUANTUM CRYPTOGRAPHY TO PROTECT CRITICAL INFRASTRUCTURE AGAINST QUANTUM ATTACKS

Taximov Askar Boranbayevich

Abstract: The article discusses the problem of providing information security of critical infrastructure in conditions of quantum computing. The analysis of threats related to the possibility of hacking existing cryptographic algorithms with quantum computers was carried out. Presented classes of post-quantum algorithms suitable for replacement of traditional protection schemes, with emphasis on lattice cryptosystems as the most balanced in terms of cryptostability, performance and applicability under conditions of limited resources. The main result of the work is the author algorithm LatticeCI, intended for implementation of quantum-stable key exchange in information systems of critical infrastructure. The concept of the algorithm is described, provided with a pseudo-code, calculations given by security parameters, data volumes and time costs. Demonstrated the possibility of implementing the algorithm in the real environment without significant changes to hardware.
Keywords: post-quantum cryptography, critical infrastructure, quantum attacks, lattice cryptography, key exchange, information protection, LatticeCI, quantum computing resistance, NTRU, quantum security.

Современная критическая информационная инфраструктура (энергетические сети, системы управления производством, телекоммуникации и др.) в значительной мере опирается на криптографию для обеспечения безопасности данных и управления. Традиционные алгоритмы с открытым ключом – такие как RSA и криптосистемы на эллиптических кривых – десятилетиями защищали конфиденциальность и аутентичность обмена информацией. Однако появление квантовых вычислительных технологий ставит под угрозу устойчивость этих схем. Алгоритм Шора показал, что достаточно мощный квантовый компьютер сможет факторизовать большие числа и решать логарифмические задачи за полиномиальное время, практически ломая RSA, Диффи–Хеллмана и ECDSA. Параллельно алгоритм Гровера ускоряет перебор ключей симметричных шифров и хеш-функций (снижая эффективную стойкость AES-128 до эквивалента ~AES-64). Хотя для реализации этих атак требуются квантовые машины с сотнями тысяч логических кубитов, прогресс в квантовых технологиях идет быстрыми темпами. Ещё в 2023 году IBM создала квантовый процессор на 433 кубита, а в текущем году планирует увеличить их число до нескольких тысяч. Появились и первые тревожные заявления: так, группа исследователей в Китае заявила о методе, теоретически позволяющем факторизовать RSA-2048 с помощью всего ~372 кубитов. Несмотря на скепсис сообщества к таким оптимистичным оценкам, очевидно одно – угроза «квантового взлома» уже не просто теоретическая абстракция, а вопрос времени [1].

Особенно остро эта проблема встает для объектов критической инфраструктуры (ОКИИ). В таких системах компрометация данных или каналов связи напрямую угрожает общественной безопасности, приводит к финансовым потерям и технологическим авариям. Более того, инфраструктурные системы обладают повышенной инерционностью – они эксплуатируются десятилетиями, часто на устаревших платформах, где обновление криптографических механизмов затруднено. Злоумышленники могут уже сейчас тайно перехватывать зашифрованный трафик с таких объектов (*«harvest now, decrypt later»* – «собери сейчас, расшифруй потом»), рассчитывая расшифровать накопленные данные, когда квантовые вычисления станут доступны. Таким образом, необходимость перехода к постквантовой криптографии (PQC) для защиты критической инфраструктуры – насущная задача, требующая как теоретической проработки, так и практических решений. В данной работе представлен обзор актуальных угроз, анализ существующих постквантовых подходов и предлагается оригинальный алгоритм постквантового шифрования, пригодный для защиты ИТ-систем критической инфраструктуры в реальных условиях [2].

Анализ текущих угроз и существующих решений

Квантовые атаки на классическую криптографию. Основная угроза квантовых вычислений для современных криптосистем связана с возможностью резко снизить сложность задач, обеспечивающих их стойкость. Протоколы обмена ключами и цифровые подписи, основанные на факторизации или дискретном логарифме (RSA, алгоритм Диффи–Хеллмана, ECDH, ECDSA и др.), считаются условно небезопасными в постквантовой эпохе. Алгоритм Шора способен решать обе эти математические задачи за полиномиальное время, а это означает взлом шифрования с открытым ключом практически мгновенно по меркам криптографии (для достаточного размера квантовой машины). В Таблице 1 суммирован эффект квантовых атак на ряд распространённых алгоритмов. Видно, что симметричные алгоритмы и хеш-функции сохраняют часть стойкости, тогда как устойчивость асимметричных схем стремится к нулю [3].

Как видно, устойчивость алгоритмов с открытым ключом оказывается под угрозой: квантовая вычислительная техника принципиально нарушает баланс между криптографами и криптоаналитиками, заложенный в современную инфраструктуру безопасности. Если сегодня для взлома RSA-2048 понадобился бы миллиарды лет даже самому мощному суперкомпьютеру, то завтра квантовая машина может справиться с этой задачей за считанные часы или дни. Сценарий, в котором государственные структуры или хакерские группировки с доступом к квантовым ресурсам выводят из строя системы энергоснабжения, транспорта или банковского сектора, расшифровывая защищённые каналы связи – перестал быть фантастикой. В свете этого мировое сообщество активизировало разработки в области постквантовой криптографии [4].

Постквантовая криптография (PQC) – направление, разрабатывающее новые алгоритмы шифрования и цифровой подписи, устойчивые к взлому как классическими компьютерами, так и потенциальным противником, обладающим квантовым компьютером. В отличие от квантовой криптографии (си-

стем распределения ключей на основе квантовой физики), PQC-наработки являются чисто программно-математическими и не требуют специального оборудования. Это делает их более практически применимыми для защиты существующих ИТ-систем, включая критическую инфраструктуру. В 2016–2022 гг. Национальный институт стандартов и технологий США (NIST) провёл масштабный открытый конкурс по отбору постквантовых алгоритмов для стандартизации. В результате в 2022–2024 гг. были объявлены первые победители – в том числе CRYSTALS-Kyber (алгоритм обмена ключами на решётках) и CRYSTALS-Dilithium (схема цифровой подписи на решётках), признанные подходящими для широкого внедрения. Параллельно отобраны и другие перспективные схемы, проходящие финальные испытания: классическая кодовая криптосистема Classic McEliece, подписи Falcon (решётки) и SPHINCS+ (хеширование), и др.

Таблица 1

Уязвимость современных алгоритмов перед квантовыми атаками

Алгоритм	Назначение	Оценка стойкости классическая	Квантовая уязвимость (атакующий алгоритм)
RSA-2048	Шифрование, ЭЦП	~112 бит (классическая сложность)	Ломается экспоненциально быстрее (Шор)
ECDH (256 бит)	Обмен ключами	~128 бит	Ломается экспоненциально быстрее (Шор)
AES-128	Симметричное шифрование	128 бит	Эффективно ~64 бит (Гровер)
SHA-256	Хеширование	256 бит (коллизия ~128)	Эффективно коллизия ~64 бит (Гровер)
ГОСТ 34.10-2012 (256)	ЭЦП на эллиптических кривых	~128 бит	Ломается экспоненциально быстрее (Шор)

Таблица 2

Примеры постквантовых алгоритмов и их параметры на уровне безопасности ~128 бит

Алгоритм (семейство)	Основа (сложная задача)	Размер открытого ключа	Шифротекст/ подпись	Примечания
CRYSTALS-Kyber (решётки)	Module-LWE (решётки)	≈800 байт	≈768 байт	Обмен ключами (KEM), высокая скорость
Dilithium (решётки)	Module-LWE (решётки)	≈1312 байт	≈2420 байт (подпись)	Цифровая подпись, быстрая проверка
Classic McEliece (коды)	Decoding (линейные коды)	≈261120 байт	128 байт	Обмен ключами, огромный открытый ключ
SPHINCS+ (хеш)	Хеширование (Merkle-дерево)	32 байта	~7856 байт	Подпись, очень большие подписи
Rainbow (многочл.)	MQ уравнения (GF)	~158000 байт	~170 байт	Подпись, взломан в 2022 (неприменим)

Фокус на критическую инфраструктуру. Индустриальные и другие критически важные системы накладывают дополнительные ограничения на применимую криптографию. Во-первых, многие узлы (контроллеры, датчики, реле и т.д. в АСУ ТП) обладают ограниченными вычислительными ресурсами: слабые процессоры, небольшой объём памяти, отсутствие аппаратного ускорения современных криптоалгоритмов. Во-вторых, режим работы часто реального времени: промышленные протоколы требуют минимальных задержек (стандарт IEC 62443 рекомендует выдерживать задержки в единицы миллисе-

кунд, иначе возможен сбой технологического процесса). Это означает, что постквантовые алгоритмы не должны существенно увеличить задержку обмена данными. В-третьих, многие устройства критической инфраструктуры работают по устаревшим или нестандартным коммуникационным стекам, а обновление прошивки затруднено. Поэтому новые схемы безопасности должны быть максимально совместимы и гибки во внедрении: поддерживать гибридное шифрование, когда традиционный алгоритм используется параллельно с PQC для плавного перехода [5].

Учитывая требования, за основу нашего решения берется решётчатая схема обмена ключами (KEM – key encapsulation mechanism). Модель предполагает следующий сценарий: два узла (полевой контроллер и центральный сервер) установливает общий секрет для зашифрованного канала связи. Вместо классического RSA или ECDH они используют постквантовый KEM – одна сторона генерирует пару ключей (открытый/секретный), другая на основе открытого ключа вычисляет шифротекст и общий секрет, первая сторона расшифровывает шифротекст своим секретным ключом и получает тот же общий секрет. Далее этот общий секрет используется как ключ симметричного алгоритма (AES-256) для быстрой шифрации канального трафика в режиме реального времени. Таким образом, постквантовая «нагрузка» ложится только на этап установки соединения, а передача оперативных команд и данных идёт с минимальной задержкой на устойчивом симметричном шифре [6].

Концептуальная схема нашего алгоритма соответствует подходу NTRU/Kyber с определёнными оптимизациями:

- Используется кольцо усечённых многочленов $R = Z_q[x]/(x^N - 1)$ – набор многочленов степени N-1 с коэффициентами по модулю q. Выбор такой алгебраической структуры позволяет эффективно выполнять операции (сложение/умножение многочленов), соответствующие векторно-матричным операциям на решётке. Кольцо R задаётся параметром N (степень полинома) и модулем q, при N=256 и q=3329 (как в Kyber) полином представляется 256 коэффициентами по ~12 бит.
- Генерация ключей основывается на выборе случайных малых многочленов. В частности, секретный ключ состоит из одного или двух многочленов с маленькими коэффициентами (f(x) и g(x) с элементами из {-1,0,1} или аналогичного распределения). Наличие *короткого* секрета гарантирует эффективность расшифрования. Открытый ключ вычисляется как многочлен $h(x) = f_q(x) * g(x)/q$, где $f_q(x)$ – обратный к f(x) по модулю q. Благодаря этому при расшифровании происходит избавление от влияния случайного шума.
- Для обеспечения стойкости к выбросу ошибок и CCA-атакам используется трансформ Фуджисаки – Окамото либо аналогичная методика: сессионный ключ шифруется вместе с проверочным значением, а итоговый общий секрет получается через хеширование шифротекста и/или сообщения.
- В целях совместимости мы используем стандартные криптопримитивы для всех вспомогательных операций: генерация случайностей, хеширование и вывод ключей основываются на SHA-256/SHA-3 и HKDF, а при необходимости – на AES-256 (реализация варианта с AES, доступная во многих контроллерах аппаратно).

На основе этой концепции разработан конкретный алгоритм, описанный ниже. Он удовлетворяет указанным требованиям по стойкости, эффективности и реализуемости. Далее приводятся оценки выбранных параметров и сравнительный анализ, а затем формальное описание алгоритма и его реализация.

Чтобы гарантировать требуемый уровень безопасности, выбираем параметры решётчатой схемы исходя из известных оценок стойкости. Основные параметры – размер многочлена N (определяющий размер решётки), модуль q и распределение/размеры случайных коэффициентов (шума).

С точки зрения вычислительной сложности наш алгоритм эффективен. Генерация ключа требует сгенерировать два случайных полинома и выполнить несколько умножений по модулю q и p (включая вычисление обратного f_q и f_p). Типичная сложность – O (N^2) при наивном умножении (для N=256 это ~65536 умножений целых чисел, что совсем немного). Существуют оптимизации с использованием БПФ/NTT, снижающие сложность до $O(N \log N)$, но на малых N можно обойтись и простыми методами. Операции с матрицами N/times N (как в некоторых LWE-схемах) у нас заменены на умножение полиномов в кольце, что существенно ускоряет вычисления и уменьшает память [7].

Чтобы оценить реальное время выполнения, рассмотрим типичное устройство в инфраструкту-

ре – контроллер на базе ARM Cortex-M или специализированный модуль. Такие CPU могут работать на частоте 100–200 МГц. Для них 65 тысяч умножений – доли миллисекунды (при аппаратном умножителе). Даже учитывая операции по модулю и хеширование, ключевой обмен LatticeCI оценивается в считанные миллисекунды. Реализация схемы Kyber-512 на микроконтроллере ESP32 (240 МГц) выполняет шифрование примерно за 17 мс. Наш алгоритм LatticeCI благодаря более простым операциям и использованию ускоряемых примитивов (AES вместо SHAKE) способен достичь сопоставимого или лучшего результата – оценки показывают около 10–15 мс на установление сессионного ключа на схожем оборудовании.

Для наглядности сравним параметры и производительность нашего предложения LatticeCI с одним из стандартных алгоритмов (Kyber-512) и классическим RSA (таблица 3).

Таблица 3

Сравнение алгоритмов обмена ключами

Алгоритм	Постквантовый	Открытый ключ (байт)	Шифротекст (байт)	Время ключевого обмена (на MCU)
RSA-2048	Нет	256	256	~50–100 мс (экспоненциальная сложность по показателю d)
Kyber-512	Да (решётки)	800	768	~15–20 мс
LatticeCI (наш)	Да (решётки)	~384	~384	~10–15 мс

Наконец, отмечаем оценку криптостойкости LatticeCI. Параметры ($N = 256, q = 2048,$ коэф. $-1,0,1$) ориентированы на то, чтобы атаки, основанные на решётках (метод BKZ, алгоритм истощения списка или hybrid attack) имели сложность не ниже 2^{128} операций. По опубликованным результатам для аналогичных схем, решётка размерности 256 с модулем $\sim 2^{11}$ и двоичным шумом обеспечивает около 130–140 бит классической стойкости и более 100 бит стойкости при учёте гипотетических квантовых ускорений. Таким образом, даже с запасом на возможные будущие оптимизации криптоанализа, алгоритм соответствует критериям надежности для использования в ОКИИ.

Алгоритм LatticeCI состоит из трёх процедур: генерация ключей, инкапсуляция (шифрование общего секрета) и декапсуляция (расшифрование секрета). Обозначим через || операцию конкатенации, а H () – криптографическую хеш-функцию (SHA-3 или SHA-256) для производных вычислений. Параметры алгоритма – (N, q, p, χ), где χ – распределение для случайных небольших коэффициентов. Предполагается, что $p \ll q$ и $gcd(p, q) = 1$. Ниже приведён код основных операций:

Параметры: N, q, p, распределение X для {-1,0,1}.

Функция KeyGen ( ):

1. *Сгенерировать многочлен f(x) $\in X^N$, обладающий обратимым по mod q (и mod p).*
2. *Сгенерировать случайный многочлен g(x) $\in X^N$.*
3. *Вычислить обратный многочлен f_q(x) = f(x)$^{-1}$ mod q.*
4. *Вычислить открытый ключ: h(x) = f_q(x) * g(x) mod q.*
5. *Вычислить вспомогательный f_p(x) = f(x)$^{-1}$ mod p (для дешифровки сообщения).*
6. *Вернуть открытый ключ pk = h(x) и секретный ключ sk = {f(x), f_p(x)}.*

Функция Encapsulate (pk):

Вход: открытый ключ h(x).

1. *Сгенерировать случайный сеансовый ключ K (битовая строка длиной k бит, например k=128).*
2. *Закодировать K как многочлен M(x) $\in R$ с коэффициентами в {0,1} (представление бита 1 как 1*x^i в полиноме и 0 как 0*x^i).*
3. *Сгенерировать случайный «шумовой» многочлен r(x) $\in X^N$.*
4. *Вычислить шифротекст: C(x) = p r(x)*h(x) + M(x) mod q.*
5. *Вычислить контрольное значение: d = H (M || r), где M – исходное сообщение (сеансовый*

ключ в битах), r – использованный шум.

6. Вычислить общий секрет: K_AB = H (K || C). (Применяется хеширование от комбинации собственного секрета K и шифротекста C.)

7. Вернуть шифротекст C и общий секрет K_AB.

Функция Decapsulate (sk, C):

Вход: секретный ключ {f(x), f_p(x)} и шифротекст C(x).

*1. Вычислить промежуточный полином: a(x) = f(x)*C(x) mod q.*

2. Привести коэффициенты a(x) в интервал (-q/2, q/2] (коррекция переполнения).

*3. Вычислить полином b(x) = f_p(x)*a(x) mod p.*

*4. В результате шагов 1–3 получается полином b(x), который равен f(x)*M(x) mod p. Благодаря малости M и свойству f_p, полином b(x) должен совпадать с исходным сообщением M(x) (коэффициенты b – это биты ключа).*

5. Извлечь из b(x) двоичный сеансовый ключ K (восстановить битовую строку).

6. Опционально: вычислить d' = H (M || r') из восстановленного сообщения M и «предполагаемого» шума r' (при CCA – режиме шума может не передаваться, а вычисляться детерминировано из K – в упрощённом описании этот шаг опущен).

7. Вычислить общий секрет: K_AB = H (K || C).

8. Если контрольное значение d' не совпало с пришедшим (в C), то вернуть ошибку (неуспешная расшифровка). Иначе вернуть общий секрет K_AB.

Алгоритм LatticeCI позволяет двум участникам безопасно согласовать секрет на открытом канале, обеспечивая защиту от квантовых атак. Отметим, что LatticeCI – не просто теоретическая конструкция: он учитывает множество практических нюансов (размеры данных, совместимость, простота вычислений), что делает его пригодным для реального развёртывания.

Для использования алгоритма LatticeCI на объектах критической инфраструктуры предлагается следующая стратегия: сначала провести инвентаризацию всех коммуникационных каналов и протоколов, где используется криптография. Это могут быть VPN-соединения между удалёнными подстанциями и центром, шифрование телеметрии от сенсоров, аутентификация команд управления и т.д. Далее определяются узлы, способные на программное обновление [8].

Для устройств, которые не могут быть перепрошиты (старое оборудование без поддержки новых алгоритмов), возможны решения уровня сети, установка квантово-устойчивых шлюзов: небольших внешних криптомодулей, выполняющих роль прокси. Такой шлюз на входе/выходе из сегмента сети будет перехватывать трафик, устанавливать с удалённой стороной PQC-защиту и передавать расшифрованные данные в устаревшее устройство по доверенному локальному каналу. Это, конечно, добавляет устройство в инфраструктуру и может стать точкой отказа, но позволяет защитить даже те узлы, которые сами не могут выполнять постквантовые вычисления.

С точки зрения криптоанализа, предложенный алгоритм основывается на задаче, эквивалентной близкой к NTRU: найти секрет f(x) по открытому $h(x) = f^{-1} * g mod q$. Это сводимо к задаче короткого вектора в решётке размерности N (примерно 256) и размером q – именно та задача, которую квантовый компьютер решить не способен (не известно алгоритмов эффективнее, чем классические методы, сложность которых экспоненциальна от N). В отличие от RSA/ECDH, где рост квантовой мощности напрямую означает угрозу, для решёток рост числа кубитов существенно не понижает сложность атаки – известные квантовые методы могут дать лишь небольшой полиномиальный выигрыш уменьшить показатель экспоненты, но не сломать экспоненциальный барьер.

Сопоставление с альтернативами. Почему именно LatticeCI, а не другой алгоритм? Рассмотрим кратко: кодовые схемы (McEliece) хороши с точки зрения безопасности, но требуют хранения сотен килобайт ключей – многие ПЛК (программируемый логический контроллер) и сенсоры просто не имеют столько свободной памяти, да и передача столь громоздких ключей по медленным каналам нежелательна. Хеш-подписи незаменимы для обновления прошивок (где размер не столь критичен, а долго-

вечность важна), но для оперативных команд их размер и задержка делают применение неэффективным. Квантовое распределение ключей (QKD) теоретически идеально – его не «взломать» математиками, ведь оно основывается на физических принципах. Однако QKD требует оптоволоконных линий или специальных квантовых устройств, что экономически и технически сложно масштабировать на всю инфраструктуру. Постквантовый же софт можно развернуть повсеместно, используя существующие каналы связи [9].

Практическая проверка. Алгоритм LatticeCI нуждается в тщательном тестировании вблизи реальных условий. На первом этапе следует провести имитацию работы в лаборатории: развернуть фрагмент сети с несколькими устройствами (контроллер, датчик, сервер) и заменить их криптографию на LatticeCI. Измеряются задержки, пропускная способность, корректность взаимодействия. Затем – аудит безопасности: моделируются возможные атаки (активный противник, пытающийся вставить свой публичный ключ, атаки повторного воспроизведения сообщений, анализ побочных излучений, попытки нарушить синхронность и т.п.).

Начинать переход на постквантовые алгоритмы нужно уже сейчас, до того, как квантовые атаки станут повсеместной реальностью. Представленный алгоритм LatticeCI демонстрирует, что квантовоустойчивая криптография может быть практически применима в условиях реальных ограничений. Дальнейшие работы будут направлены на оптимизацию реализации, сертификацию алгоритма по существующим стандартам безопасности и широкое тестирование на совместимость.

Список источников

1. Garcıa, L.C. Coronado. О безопасности и эффективности схемы подписания Меркле: технический доклад 2005/192. – Криптологический архив ePrint, 2021. (дата обращения: 22.05.2025).
2. Nannicini, G. Введение в квантовые вычисления без физики // SIAM Review. – 2021. – Т. 63. – № 4. – С. 936–981.
3. Криптография [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Криптография, свободный (дата обращения: 22.05.2025).
4. Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R. Applying Grover's Algorithm to AES: Quantum Resource Estimates // Post-Quantum Cryptography. – Springer International Publishing, 2021. – С. 29–43. – DOI: 10.1007/978-3-319-29360-8_3.
5. Logan O., Майлу, Льюис II Чарльтон Д., Риггс Кейси, Гримейла Майкл Р. Постквантовая криптография: что означают достижения в области квантовых вычислений для ИТ-специалистов // IT Professional. – 2021. – Т. 23(5). – С. 42–47.
6. Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M. и др. Status report on the second round of the NIST post-quantum cryptography standardization process. – National Institute of Standards and Technology, 2021. – DOI: 10.6028/nist.ir.8309.
7. Post-Quantum Cryptography / D.J. Bernstein, Johannes Buchmann, Erik Dahmen [Электронный ресурс]. – Springer Link, 2023. – URL: https://link.springer.com/book/10.1007/978-3-540-88702-7 (дата обращения: 22.05.2025).
8. NIST: сайт [Электронный ресурс]. – Вашингтон, 2023. – URL: https://csrc.nist.gov/projects/post-quantum-cryptography (дата обращения: 22.05.2025).
9. Barker, E. Guideline for using cryptographic standards in the federal government: National Institute of Standards and Technology. – 2021. – DOI: 10.6028/nist.sp.800-175br1.