МИНИСТЕРСТВО
НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
**«Национальный исследовательский ядерный университет «МИФИ»**
**(НИЯУ МИФИ)**
Каширское шоссе, д.31, г. Москва, 115409
Тел. (499) 324-77-77, факс (499) 324-21-11
http://www.mephi.ru
e-mail: info@mephi.ru

09.04.2026 № 043/04

На № _____ от _____

**УТВЕРЖДАЮ**
Первый проректор НИЯУ МИФИ
д.ф.-м.н., профессор

_____ О.В. Нагорнов

«09» апреля 2026 г.

# О Т З Ы В

ведущей организации
Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ)
на диссертацию Петренко Алексея Сергеевича «**Метод построения постквантовых алгебраических алгоритмов ЭЦП с двумя скрытыми группами**», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. – «Методы и системы защиты информации, информационная безопасность»

## 1. Актуальность темы диссертации

Актуальность темы диссертации Петренко А.С. объясняется необходимостью разрешения *проблемной ситуации*, состоящей в противоречии между беспрецедентным ростом угроз безопасности информации, повышением требований информационной безопасности к объектам критической информационной инфраструктуры (КИИ) Российской Федерации (РФ) и уже недостаточностью известных моделей и методов защиты информации в условиях появления новой квантовой угрозы безопасности информации. Разрешение названной проблемной ситуации подразумевает создание таких национальных постквантовых криптопримитивов, которые позволят сохранить конфиденциальность и целостность защищаемой информации на объектах КИИ РФ в условиях компьютерных атак злоумышленников с применением квантового компьютера.

К 2030 году ожидается появление релевантного (практически значимого) квантового компьютера, которое приведет к взлому большей части современных криптографических алгоритмов, стойкость которых базируется на вычислительной трудности решения задач факторизации и дискретного

логарифмирования по простому модулю. В первую очередь уязвимыми окажутся системы шифрования и протоколы с открытым ключом, а как следствие и информационные системы и технологии их использующие, в их числе весьма значимую роль играют цифровые финансовые активы: механизмы и подсистемы в блокчейн-системах, предоставляющие права на цифровые объекты или данные, а также более сложные — например, смарт-контракты и цифровые деньги, в частности, национальная платформа цифрового рубля. По этой причине основные усилия разработчиков криптоалгоритмов сосредоточены на разработке и стандартизации постквантовых криптографических механизмов, которые останутся действенными даже после появления практически релевантных квантовых компьютеров. Так, Национальный институт стандартов и технологий (NIST) США (National Institute of Standards and Technology, NIST) по результатам открытого конкурса среди 69 алгоритмов-кандидатов по выбору лучших квантово-устойчивых криптографических схем инкапсуляции ключа и цифровой подписи (2017-2024 гг.) подготовил первые четыре стандарта. Были стандартизованы первые три схемы постквантовой ЭЦП: FIPS 204 (на основе алгоритма CRYSTALS-Dilithium), FIPS 205 (на основе SPHINCS+) и FIPS 206 (на основе FALCON). Также были стандартизованы хэш-ориентированные схемы ЭЦП с сохранением состояния (XMSS и LMS) и многоуровневая многомерная квадратичная схема Rainbow. В России подобные исследования также проводятся под общим руководством Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26). Например, экспертами-криптографами научно-производственных компаний «Криптонит» и «QApp» был разработан постквантовый алгоритм электронной подписи «Шиповник», устойчивый к квантовым атакам злоумышленников. Модификации упомянутого алгоритма показывают различные результаты в скорости формирования ключей, формирования и проверки электронной цифровой подписи при различной криптостойкости. При этом сертификация постквантового алгоритма «Шиповник» по требованиям безопасности информации и доведение его до статуса национального стандарта постквантовой ЭЦП ещё не завершены.

К известным схемам постквантовых ЭЦП относятся:

– *Схемы на решетках*. Безопасность которых основана на задачах теории решеток. В том числе, на сложности проблемы обучения с ошибками (LWE) или нахождении короткого вектора в решетке. Например, схемы CRYSTALS-Dilithium и FALCON. Упомянутые схемы характеризуются высокой производительностью и относительно компактными ключами по сравнению с другими PQ-системами, однако длина подписи может быть значительной;

– *Схемы на основе Хэш*. Различают схемы с сохранением состояния (stateful) и схемы без сохранения состояния (stateless). Первые (например, XMSS и LMS) используют дерево Меркла для возможности многократной подписи и требуют ведения состояния (счетчика использованных ключевых пар). Вторые, например SPHINCS+, устраняют необходимость отслеживать состояние ценой увеличения размера подписи. Хэш-алгоритмы считаются криптографически консервативными в том смысле, что их надежность сводится

к стойкости используемого хэша, однако генерируемые подписи весьма объемны, а скорость подписи и проверки сравнительно низкие;

– *Многомерные квадратичные схемы* постквантовой электронной подписи. Безопасность упомянутых схем базируется на сложности решения систем многочленов над конечными полями (задача MQ, Multivariate Quadratic). Здесь большее распространение получила схема Rainbow, предлагавшая короткие подписи и высокую скорость их формирования и использования. Однако схема Rainbow была успешно взломана в 2022 году, что существенно замедлило ее развитие и распространение на практике;

– *Схемы на основе корректирующих кодов*. Например, схема Wave или схема Picnic/SDitH. Однако упомянутые схемы характеризуются значительными размерами подписи и высокой вычислительной трудоемкостью. В результате они рассматриваются для достаточно узких сценариев применения на практике.

Текущее состояние вопроса в этой области мотивирует соискателей продолжать научные исследования с целью создания универсальных постквантовых алгоритмов и схем ЭЦП с требуемыми характеристиками *по размеру ключа, производительности, стойкости, простоте внедрения и доказательной надёжности*. Активно изучаются задачи на решётках, вопросы декодирования случайных линейных кодов и ранговых кодов, а также многомерные квадратичные системы, изогенные конструкции, задачи изоморфизма многочленов и тензорных разложений, и подходы на некоммутативных группах и полугруппах. При этом последние представляют особый интерес, так как многие квантовые алгоритмы эффективно решают задачи в коммутативных структурах, но это не распространяется напрямую на некоммутативные структуры (в частности, некоммутативные кольца, групповые и матричные алгебры).

Таким образом, тема диссертации Петренко А.С. является своевременной и актуальной, а решаемая научная задача *«Разработка метода построения постквантовых алгоритмов ЭЦП с двумя скрытыми группами для применения в составе блокчейн-экосистем и платформ»* имеет важное теоретическое и практическое значение.

Актуальность диссертации Петренко А.С. подтверждается требованиями следующих нормативных документов:

– «Доктрина информационной безопасности России», 2024 г.;

– Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

– Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Приказы ФСТЭК России: № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»; № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»; № 55 «Об утверждении Положения о системе сертификации средств защиты

информации»; № 76 «Об утверждении Требований по безопасности информации, устанавливающие уровни доверия к средствам защиты информации и средствам обеспечения безопасности информационных технологий»;

– ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

– Приказ ФСБ РФ от 09.02.2005 N 66 (ред. от 12.04.2010) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (Зарегистрировано в Минюсте РФ 03.03.2005 N 6382) и др.

## 2. Научная новизна и основные результаты исследований

Целью диссертационной работы Петренко А.С. является понижение ресурсоёмкости постквантовых ЭЦП путём сокращения длины подписи и ключей при заданной криптостойкости для обеспечения применимости в составе блокчейн-экосистем и платформ, и повышение квантовой устойчивости упомянутых систем. В качестве *объекта исследования* выступают постквантовые алгебраические алгоритмы ЭЦП с малыми размерами длины подписи и открытого ключа. *Предметом исследования* являются механизм рандомизации подписи, способы оценивания стойкости к атакам на основе известных подписей и профили применимости алгоритмов ЭЦП.

Научную новизну диссертационную работы определяет следующее:

1. Разработан метод построения постквантовых алгоритмов ЭЦП с двумя скрытыми группами на основе КНАА, стойкость которых основана на вычислительной сложности решения больших систем степенных уравнений (БССУ), отличающийся заданием механизма рандомизации подписи в зависимости от выбора элементов из двух скрытых коммутативных групп как подструктур алгебраического носителя алгоритма и обеспечивающий снижение вычислительной сложности алгоритма по сравнению с аналогами.
2. Разработаны три постквантовых алгебраических алгоритма на основе метода построения, изложенного в первом положении, отличающиеся заданием вспомогательных скрытых коммутативных групп на основе известных подписей с использованием декомпозиции КНАА на конечные коммутативные кольца, пересекающиеся строго в множестве скалярных векторов и позволяющие вдвое уменьшить разрядность показателей степени при сохранении стойкости.
3. Разработан способ оценивания стойкости алгебраических алгоритмов ЭЦП к атакам на основе известных подписей, отличающийся заданием координат элементов из скрытой группы, по координатам представителя этой группы и обеспечивающий составление по известным подписям системы степенных уравнений с равным количеством уравнений и неизвестных.
4. Введена и реализована архитектура программного комплекса на основе разработанного метода построения постквантовых ЭЦП с двумя

скрытыми группами на основе КНАА для обеспечения квантовой устойчивости блокчейн-платформ и экосистем, отличающаяся внедрением маршрута интеграции ЭЦП без потери производительности в существующие архитектуры национальных блокчейн-экосистем и платформ и обеспечивающая формирование управляемых контуров сопряжения криптографических механизмов с сетевыми метриками и пороговых режимов защиты информации с доказуемой квантовой устойчивостью.

Результаты экспериментов подтверждают работоспособность и эффективность разработанных решений. Предложенный автором метод построения постквантовых ЭЦП позволил снизить ресурсоёмкость постквантовых ЭЦП путём сокращения длины подписи более чем в 6 раз и ключей не менее чем на 55% по сравнению с ближайшими аналогами при заданной криптостойкости для обеспечения применимости в составе блокчейн-экосистем и платформ, благодаря чему была повышена квантовая устойчивость упомянутых систем в 3 раза и более.

## 3. Достоверность и обоснованность основных выводов исследований

Достоверность и обоснованность основных выводов исследований, представленных в диссертации Петренко А.С. подтверждается результатами анализа предшествующих научных работ в данной области исследований, корректным использованием математического аппарата, полученными экспериментальными данными и апробацией результатов в научных публикациях и докладах на конференциях.

Основные результаты исследований и научных разработок докладывались и обсуждались на 8 всероссийских и международных научно-практических конференциях, проходивших в различных городах на территории Российской Федерации в 2022-2025 гг.: Всероссийский молодежный конкурс научных проектов #ВЦЕНТРЕНАУКИ (г. Сириус, 2022 г.), Современные тенденции развития методов и технологий защиты информации: III Всероссийская научная школа-семинар (г. Москва, 2023 г.), V Международная научная конференция «Наука будущего» и VIII Всероссийского молодежного научного форума (г. Орел, 2023 г.), VIII международная научно-практическая конференция «The 2024 Symposium on Cybersecurity of the Digital Economy» (г. Иннополис, 2024 г.), Безопасные информационные технологии: XII международная научно-техническая конференция (г. Москва, 2023, 2024 гг.), всероссийская конференция «Методы и технические средства обеспечения безопасности информации» (г. Санкт-Петербург, 2022, 2025 гг.), Экономика устойчивого развития региона: инновации, финансовые аспекты, технологические драйверы развития в сфере туризма и гостеприимства: X международная научно-практическая конференция (г. Симферополь, 2023 г.), II Международная конференция «Прикладной искусственный интеллект: перспективы и риски» (г. Санкт-Петербург, 2025 г.).

Также основные результаты работы были апробированы при выполнении и защите следующих научных проектов:

– Грант РНФ №24-41-04006 «Теоретические основы параметризуемых унифицированных способов задания конечных ассоциативных алгебр и разработка постквантовых криптографических алгоритмов с открытым ключом» (2024-2026 гг) (*Основной исполнитель научного проекта*);

– Гранта Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) и Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ) на проведение научных исследований и разработок в области информационной безопасности для задач цифровой экономики («Грант ИБ МТУСИ» в рамках соглашения №40469-19/2023-к от 05.07.2023) на тему «Метод (технология) обеспечения квантовой устойчивости блокчейн-экосистем и платформ Цифровой экономики Российской Федерации» (*Руководитель научного проекта)*.

## 4. Значимость результатов для развития постквантовой криптографии

*Теоретическая значимость* результатов исследования Петренко А.С. заключается в том, что предложено и обосновано применение двух скрытых коммутативных групп для повышения производительности постквантовых алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения больших систем степенных уравнений. Это позволило разработать три новых типа постквантовых алгебраических схем ЭЦП, отличающихся приемами обеспечения высокой стойкости к подделке подписи с использованием вектора **S** в качестве подгоночного параметра атаки. В первом типе используется прием дополнительного возведения в степень произведения, в которое входит вектор **S**, во втором типе — выполнение возведения в степень, равную значению хеш-функции, вычисляемой от **S**, и в третьем типе – комбинирование первых двух приемов. Осуществлены алгоритмические реализации схем ЭЦП каждого типа и показана корректность разработанных алгоритмов. Выполнены оценки стойкости к прямой атаке, атаке на основе известных подписей и к подделке подписи. Представлено сравнение предложенных алгоритмов ЭЦП с известными аналогами. В качестве приемов повышения производительности алгебраических алгоритмов ЭЦП использовано задание КНАА по прореженным таблицам умножения базисных векторов и умножение на скалярный вектор при вычислении вектора **S**.

*Практическая значимость* полученных результатов состоит в апробации способа усиления рандомизации подписи, включающего вычисление подгоночного элемента подписи S в зависимости от произведения двух взаимно некоммутативных векторов и одного скалярного вектора при разработке алгебраических алгоритмов трех различных типов, представляющих интерес в качестве прототипа практичного постквантового стандарта ЭЦП. Также практическая значимость заключается в достижении короткой подписи при контролируемой трудоёмкости, наличии воспроизводимой методики испытаний и в архитектурном внедрении на примере блокчейн-систем без

существенного увеличения сетевых затрат и затрат памяти. Это в свою очередь позволяет создавать надёжные реализации электронной подписи, устойчивые к компьютерным атакам с применением как квантового компьютера, так и СуперЭВМ фон Неймана высокой и сверхвысокой производительности.

Основные научно-технические результаты диссертационной работы Петренко А.С. нашли применение в проектной деятельности научно-производственной компании АО «Технологии радиоконтроля», Центре ИТ и ИИ НТУ «Сириус», Центре информационной безопасности Университета Иннополис, а также в учебном процессе СПбГЭТУ «ЛЭТИ» при проведении учебных занятий, что подтверждается соответствующими актами о внедрении.

## 5. Рекомендации по использованию результатов и выводов, приведенных в диссертации

Результаты, полученные в данной работе, рекомендуется внедрить в образовательные учреждения, специализирующиеся на подготовке специалистов в области постквантовой криптографии, такие как Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)» (СПбГЭТУ «ЛЭТИ»), АНО ВО «Университет Иннополис», АНО ВО «НТУ «Сириус»», а также использовать в Федеральном государственном бюджетном учреждении науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» и других профильных организациях для выполнения научных проектов в области постквантовой криптографии.

Также результаты исследования могут быть внедрены в научно-производственные компании, разрабатывающие квантово-устойчивые национальные блокчейн-экосистемы и платформы. В том числе, авторские метод построения постквантовых алгоритмов ЭЦП, устойчивых к атакам с использованием квантовых компьютеров; постквантовые алгебраические алгоритмы ЭЦП и методики их применения.

## 6. Общая оценка диссертационной работы

Представленная диссертационная работа Петренко А.С. является завершенной научно-исследовательской работой, выполненной лично автором на достаточно высоком уровне. В работе решена актуальная и практически значимая научная задача «Разработка метода построения постквантовых алгоритмов ЭЦП с двумя скрытыми группами для применения в составе блокчейн-экосистем и платформ».

Основные результаты работы были представлены на международных и российских конференциях, проходивших в различных городах на территории Российской Федерации в 2022-2025 гг., основные положения диссертации описаны в научных статьях, опубликованных в российских и зарубежных изданиях. Основные результаты по теме диссертации изложены в 26 печатных

изданиях, 14 из которых опубликованы в ведущих рецензируемых журналах, входящих в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук, 5 из которых проиндексированы в Web of Science/SCOPUS. Также были написаны 2 монографии по теме исследования и получены 6 свидетельств о регистрации программ для ЭВМ.

В качестве *замечаний к диссертационной работе* можно выделить следующее.

1. В третьей главе диссертации представлены три типа авторских постквантовых алгебраических алгоритмов ЭЦП, отличающихся механизмами обеспечения стойкости к подделке подписи: первый тип использует дополнительное возведение в степень произведения с вектором S, второй - возведение в степень, равную значению хеш-функции от S, третий - комбинирование обоих приёмов. При этом авторские постквантовые алгебраические алгоритмы ЭЦП представлены в графической форме в виде соответствующих блок-схем. Такой способ представления алгоритмов является больше программотехническим, чем математическим, и требует введения дополнительных текстовых комментариев с математическими формулами.
2. В четвертой главе предусмотрена защита от атак по побочным каналам, но результаты экспериментальной оценки устойчивости программных реализаций к конкретным видам таких атак (постоянное время исполнения, маскирование, контроль диапазонов значений) не представлены. Рекомендуется в дальнейшем обратить на это внимание.
3. В пятой главе представлена авторская архитектура программного комплекса для обеспечения квантовой устойчивости национальных блокчейн-экосистем с постквантовыми криптопримитивами ЭЦП, лично разработанными автором диссертации. При этом целесообразно было провести критический анализ и показать достоинства и недостатки возможных способов программнотехнической реализации такого программного комплекса (монолитная, клиент-серверная и микросервисная программные архитектуры).

Однако, указанные выше замечания не снижают существенным образом общей положительной оценки диссертационной работы Петренко А.С. Предложенный автором метод построения постквантовых ЭЦП позволил снизить ресурсоёмкость постквантовых ЭЦП путём сокращения длины подписи более чем в 6 раз и ключей не менее чем на 55% по сравнению с ближайшими аналогами при заданной криптостойкости для обеспечения применимости в составе блокчейн-экосистем и платформ, благодаря чему была повышена квантовая устойчивость упомянутых систем в 3 раза и более. Существенно, что предлагаемые автором работы решения вносят значимый вклад в создание и развитие национальных стандартов постквантовых алгоритмов ЭЦП.

Тема диссертации Петренко А.С., направленность проведенных исследований и полученных результатов соответствуют паспорту специальности 2.3.6. – «Методы и системы защиты информации, информационная безопасность» по п. 3 (методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной

безопасности объектов различного вида и класса), п. 5 (методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет) и п. 19 (исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов).

## 7. Заключение по работе

Диссертационная работа *Петренко Алексея Сергеевича* «Метод построения постквантовых алгебраических алгоритмов ЭЦП с двумя скрытыми группами» выполнена на актуальную тему, обладает научной новизной, теоретической и практической значимостью, прикладной ценностью полученных результатов, выполнена лично соискателем и имеет завершенный характер. Текст автореферата соответствует содержанию диссертации.

Представленная диссертационная работа удовлетворяет требованиям п.п. 9-14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 года № 842, предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ему ученой степени кандидат технических наук по специальности 2.3.6. – «Методы и системы защиты информации, информационная безопасность».

Диссертационная работа Петренко А.С и настоящий Отзыв были обсуждены и одобрены на расширенном научном семинаре кафедры стратегий и технологий кибербезопасности (№ 43) института интеллектуальных кибернетических систем НИЯУ МИФИ, на котором присутствовало 9 сотрудников, протокол № 4/2026 от «7» апреля 2026 года.

**Отзыв подготовили:**
Марков Алексей Сергеевич,
доктор технических наук, старший научный сотрудник.
Организация: Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ)
кафедра «Стратегии и технологии кибербезопасности» (№ 43) института интеллектуальных кибернетических систем
Почтовый адрес: 115409, Россия, Москва, Каширское шоссе, 31.
Телефон: +7 (495) 788-56-99 доп. 92-16
E-mail: ASMarkov@mephi.ru
Должность: Заведующий кафедрой № 43.
Специальность, по которой была защищена докторская диссертация: 05.13.19 – Методы и системы защиты информации, информационная безопасность
Сайт организации: https://mephi.ru

_____Марков А.С.

Дураковский Анатолий Петрович,
кандидат технических наук, доцент.
Организация: Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ)
кафедра «Стратегии и технологии кибербезопасности» (№ 43) института интеллектуальных кибернетических систем
Почтовый адрес: 115409, Россия, Москва, Каширское шоссе, 31.
Телефон: +7 (495) 788-56-99 доп. 92-16
E-mail: APDurakovskiy@mephi.ru
Должность: доцент кафедры № 43,
директор аттестационно-испытательного центра информационной безопасности и систем защиты информации НИЯУ МИФИ

_____ Дураковский А.П.

Я, Марков А.С., даю согласие на включение своих персональных данных в документы, связанные с работой диссертационного совета, и дальнейшую обработку.

_____Марков А.С.

Я, Дураковский А.П., даю согласие на включение своих персональных данных в документы, связанные с работой диссертационного совета, и дальнейшую обработку.

_____ Дураковский А.П.

Дата подписи: « 7 » апреля 2026 г.