АССОЦИАЦИЯ ФИНТЕХ

Постквантовая криптография

Квантово-устойчивая защита данных финансовой отрасли

ФИНТЕХ — РАДАР

№9 СЕНТЯБРЬ 2025

Постквантовая криптография – *новый класс асимметричных алгоритмов шифрования, устойчивых к кибератакам с применением как классических, так и квантовых компьютеров.*

СОВМЕСТНО С ЭКСПЕРТАМИ

АССОЦИАЦИЯ ФИНТЕХ

Ассоциация ФинТех *основана в конце 2016 г. по инициативе Банка России и ключевых участников отечественного финансового рынка. Это уникальная аналитическая площадка для конструктивного диалога регулятора с представителями бизнеса. Здесь формируется экспертная оценка инновационных технологий с учетом международного опыта, а также разрабатываются концепции финансовых технологий и подходы к их внедрению.*

ОБ ИССЛЕДОВАНИИ

Вот уже несколько лет мировое технологическое сообщество обсуждает неизбежное появление квантовых компьютеров — вычислительных машин, способных не только дать вычислительное преимущество в решении ряда сложных задач, но и перевернуть основы подходов к защите ценных данных. Угроза взлома традиционных алгоритмов шифрования становится всё более осязаемой, и финансовый сектор, как один из главных хранителей конфиденциальных данных, должен быть готов к этому вызову.

По оценкам экспертов, уже к 2030 году квантовые компьютеры достигнут достаточной мощности для взлома существующих криптографических алгоритмов. Это ставит под угрозу безопасность платежных систем, цифровых подписей и защищённых коммуникаций.

Мы изучили не только мировые тренды, но и то, как российские разработчики и регулятор готовятся к «квантовому переходу». Особое внимание уделено совместимости новых алгоритмов с действующими системами.

Этот выпуск подготовлен совместно с ведущими криптографами и специалистами по кибербезопасности. В нём мы постарались объяснить сложные концепции простым языком, чтобы исследование было полезно не только техническим специалистам, но и руководителям, отвечающим за стратегию цифровой трансформации.

МАРИАННА ДАНИЛИНА

Руководитель управления стратегии, исследований и аналитики ***Ассоциации ФинТех***

Постквантовая криптография — одновременно эволюция и революция традиционной криптографии. Квантовая угроза, о которой ранее велись только мысленные эксперименты, в ближайшее время может стать реальностью.

Финансовая отрасль особенно нуждается в надёжной защите данных на всех уровнях информационных систем. Это исследование — первая в России попытка систематизировать знания и профильный опыт апробации постквантовой криптографии.

Последние несколько лет мы наблюдаем стремительное развитие отечественной экосистемы по постквантовой криптографии. Совместные усилия регулятора, передовых научно-технических компаний, индустриальных компаний-новаторов и ведущих образовательных учреждений, несомненно, приведут Россию к высоким стандартам в области постквантовых алгоритмов и надёжным квантово-устойчивым решениям.

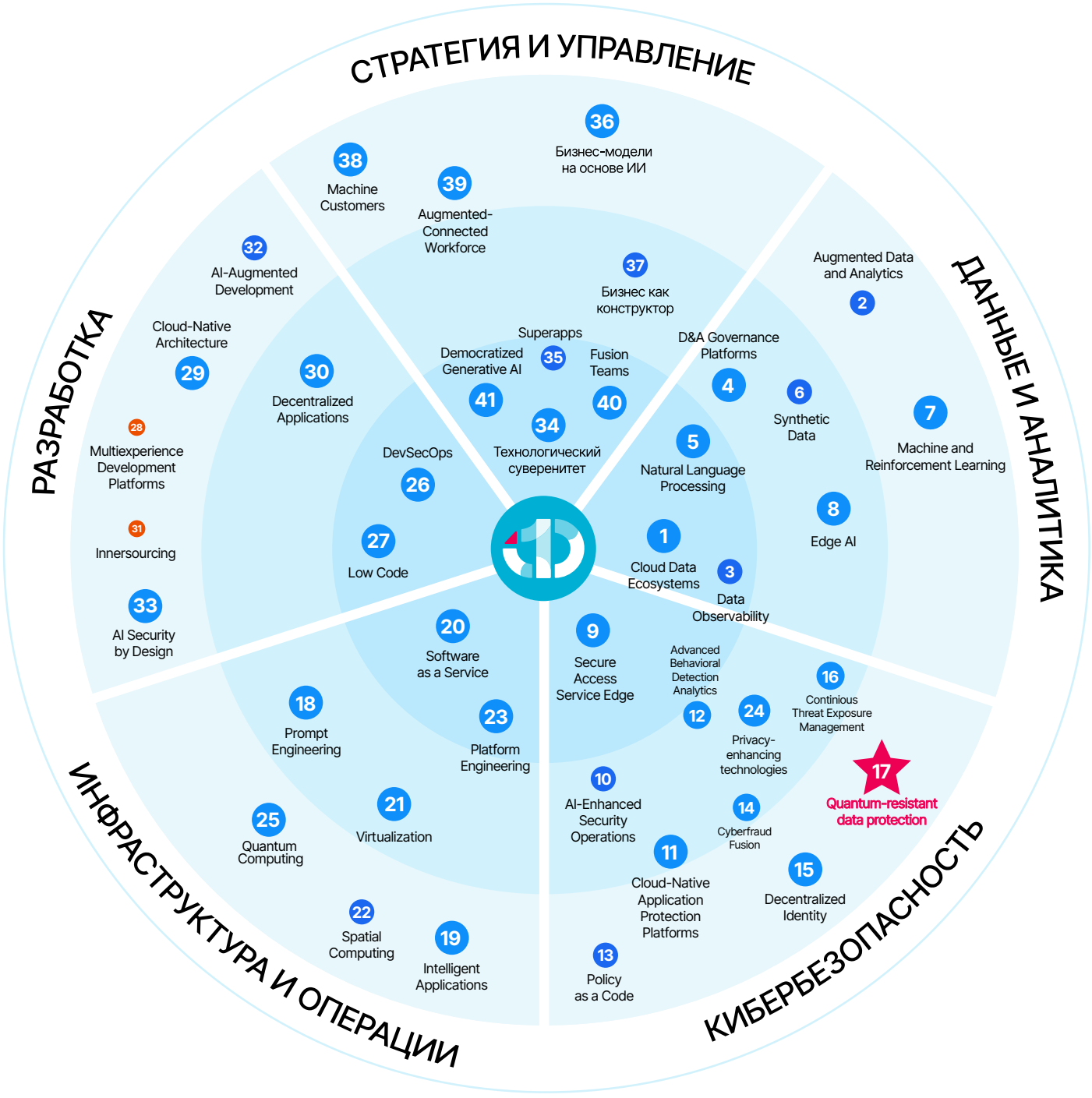
ГУГЛЯ АНТОН

Генеральный директор ***«QApp»***

По вопросам Финтех-Радара и с обратной связью, пожалуйста, обращайтесь к команде исследований и аналитики Ассоциации ФинТех

research.analytics@fintechru.org

ТЕХНОЛОГИЧЕСКИЙ ФИНТЕХ-РАДАР 2025 ГОДА



Горизонт адаптации*:

3-6 лет · 1-3 года · Сейчас (до 1 года)

Степень влияния:

Высокая · Средняя · Низкая

Технология выпуска:

★ **Quantum-resistant data protection**

* Для российского рынка горизонт адаптации трендов может увеличиваться на 1-3 года

АССОЦИАЦИЯ ФИНТЕХ

Постквантовая криптография. Почему это важно?

Современный цифровой мир основан на криптографии, защищающей конфиденциальные данные, финансовые транзакции и государственные коммуникации. Однако с развитием квантовых вычислений традиционные методы шифрования становятся уязвимыми. **Квантово-устойчивая криптография** – это новое поколение алгоритмов, способных противостоять атакам как классических, так и квантовых компьютеров.

Финтех-Радар — это аналитический фреймворк от экспертов Ассоциации ФинТех для отслеживания и оценки технологических трендов. *С его помощью можно определить зрелость технологий, готовность рынка к их адаптации и потенциал влияния на инновационное развитие компаний.*

В этом выпуске мы исследуем постквантовую криптографию — технологию, которая формирует новый стандарт защиты данных. Мы разберем, как она обеспечивает устойчивость финансовой отрасли к киберугрозам будущего и какие шаги для противодействия предпринимают глобальный и российский рынки уже сегодня.

Уже сегодня злоумышленники могут реализовать атаку **«сохранение данных сейчас – взлом потом»**, накапливая зашифрованную информацию для будущего взлома с помощью квантовых компьютеров. Это создает серьезные риски для бизнеса, государства и частных лиц.

к 2029 году

угроза применения квантовых вычислений сделает традиционную криптографию небезопасной. Переход к квантово-устойчивой (постквантовой) криптографии стоит начинать уже сейчас.

(Gartner)[1]

Важность этого перехода подтверждают ключевые игроки финансового рынка. По данным исследовательского агентства **Gartner**, постквантовая криптография входит в топ критически важных технологий 2025 года[2]. **Ассоциация Финтех в исследовании «3х10 трендов на 2025 год»** выделяет квантово-устойчивую криптографию как один из главных технологических трендов, отвечающих новым вызовам кибербезопасности[3].

[1] По данным Gartner: *gartner.com*

[2] По данным Gartner: *gartner.com*

[3] По данным Ассоциации ФинТех: *fintechru.org*

ЭТАПЫ ПЕРЕХОДА НА КВАНТОВО-УСТОЙЧИВЫЕ РЕШЕНИЯ[1]

2022 2023 2024 2025 2026 2027 2028 2029 2030

Текущий этап:

- Создание базы данных криптографических метаданных
- Разработка крипто-политик для следующих этапов
- Резервирование данных (кратко-/средне-/долгосрочное использование)
- Планирование этапа перехода к криптографической защите
- Начало стратегической разработки

Переходный этап:

- Реализация плана перехода к криптографической защите
- Удаление бесполезных/устаревших данных со слабой безопасностью
- Внедрение переходных крипто-политик
- Реализация криптографически-гибкой разработки приложений

Непрерывный этап:

- Завершение поддержки небезопасных приложений
- Применение строгих крипто-политик для данных
- Проверка и тестирование новых постквантовых алгоритмов
- Полный переход на квантово-устойчивую защиту данных

Переход на квантово-устойчивую криптографию – не просто технологическая эволюция, а **стратегическая необходимость** для обеспечения долгосрочной безопасности данных в условиях стремительного развития квантовых технологий.

ОЛЬГА АВРЯСОВА

Руководитель направления развития инноваций, Московская биржа

Быстрое развитие технологий ведёт не только к созданию средств защиты от киберугроз, но и к появлению средств для атак. Мировые учёные предрекают создание квантового компьютера, способного уже в 2028 году за доли секунды взломать все хранилища данных. Группа «Московская биржа» как финансовая инфраструктура внимательно анализирует потенциальные риски в области информационной безопасности и уделяет особое внимание защите данных клиентов. На базе Лаборатории инноваций Московской биржи был проведён пилот совместно с компанией QApp, который подтвердил эффективность предлагаемого решения для повышения уровня квантово-устойчивой защиты информации.

[1] По данным Gartner: *gartner.com*

Только 8,6% сайтов готовы к квантовой угрозе

По данным исследования F5 Labs[2], на сегодняшний день лишь ~8,6% сайтов из миллиона самых посещаемых ресурсов глобальной сети используют гибридные TLS-сертификаты с поддержкой постквантовых алгоритмов.

Несмотря на доступность соответствующих реализаций и поддержку в последних версиях некоторых браузеров, большинство интернет-ресурсов, включая банковские, государственные и медицинские, пока не перешли на постквантовую криптографию.

Для взлома современной криптографии необходимо в 20 раз меньше кубитов, чем ожидалось

Google Quantum AI[1] опубликовал препринт, демонстрирующий, что 2048-битное RSA шифрование теоретически может быть взломано квантовым компьютером с 1 миллионом зашумленных кубитов за одну неделю работы.

Это представляет 20-кратное уменьшение количества кубитов по сравнению с предыдущей оценкой Google от 2019 года и в 1000 раз меньше, чем оценки 2012 года. Данные результаты показывают, что криптографически значимые квантовые компьютеры могут появиться ранее, чем ожидалось.

Области, уязвимые для взлома:

- Сквозное шифрование: HTTPS-трафик, мессенджеры, VPN.
- Цифровые подписи: аутентификация веб-сайтов, подписание ПО, документооборот.
- Инфраструктура PKI: корневые сертификаты, аппаратные модули безопасности.

Рекомендованные NIST временные рамки перехода бизнеса на постквантовые алгоритмы:

- 2030 год: прекращение использования уязвимых криптосистем.
- 2035 год: полный запрет RSA и эллиптической криптографии.

ИЛЬЯ ЛИВАШВИЛИ

Начальник Департамента аналитики и внедрения технологий, Газпромбанк

За последние несколько лет технологии квантовых вычислений сделали существенный прорыв, и практически каждый месяц ученые из разных уголков мира сообщают о новых достижениях в сфере проектирования и создания квантовых компьютеров. Вместе со всеми преимуществами, которые могут дать человечеству подобные разработки, они несут в себе и большую угрозу информационной безопасности, так как квантовые компьютеры в ближайшем будущем станут мощнейшим инструментом взлома традиционных алгоритмов шифрования. Более того, уже сейчас злоумышленники начинают собирать зашифрованные данные для того, чтобы расшифровать их позднее.

Мы, как банк, отвечающий за огромные массивы данных своих клиентов, не можем не отнестись со всей серьезностью к этой угрозе и уже активно апробируем квантово-устойчивые методы защиты, созданные нашим партнером QApp. Мы позитивно оцениваем результаты пилотной интеграции этих программных решений и планируем продолжать совместное пилотирование постквантовых методов защиты в будущем.

[1] По данным F5 Labs: *f5.com*

[2] По данным Google Security Blog: *googleblog.com*

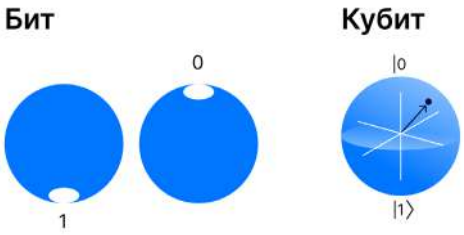
Квантовая угроза

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Квантовые вычисления (англ. Quantum computing) — направление на стыке информатики, физики и математики, в котором используются законы квантовой механики для решения сложных вычислительных задач.

Квантовый бит или кубит (англ. quantum bit, qubit) — квантовый аналог классического бита, который используется в квантовых вычислениях для описания информации.

Кубит является наименьшей единицей информации в квантовом компьютере.



По аналогии с классическим битом, который находясь в состоянии 0 или 1, может описывать классическую информацию (цифры, буквы и и т. п.), квантовый бит используется для описания квантовой информации. При этом состояние кубита имеет более сложную структуру, что является одним из факторов, почему квантовые вычисления могут быть эффективней классических.

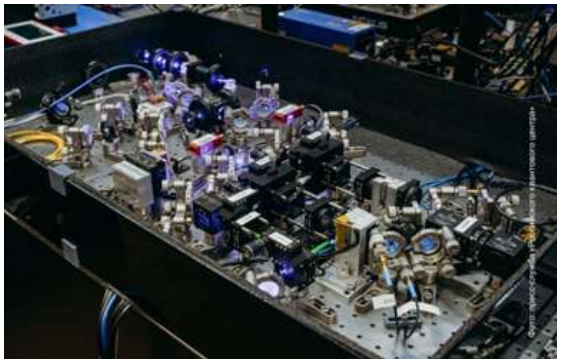
КВАНТОВЫЙ КОМПЬЮТЕР

Квантовый компьютер (англ. Quantum computer) — вычислительное устройство, которое использует принципы квантовой механики для обработки информации. В отличие от обычных компьютеров, он содержит квантовые регистры (кубиты) наряду с классическими регистрами и способен выполнять квантовые вычисления и измерения.

Ключевые компоненты:

- Квантовые регистры:
Основные вычислительные элементы, состоящие из кубитов
- Классические регистры:
Обычная память для хранения результатов измерений
- Квантовые операции:
Специальные вычисления, использующие суперпозицию и запутанность
- Система измерений:
Преобразует квантовые состояния в классическую информацию

Российские учёные разработали 50-кубитный ионный квантовый компьютер. *На сегодняшний день только шесть стран, включая Россию, обладают квантовыми компьютерами на ионах в 50 кубитов и более. Над проектом трудилась научная группа Российского квантового центра и Физического института имени П. Н. Лебедева РАН*[1].



[1] По данным ТАСС: nauka.tass.ru

КВАНТОВАЯ УГРОЗА

Квантовая угроза — новый риск для кибербезопасности, который становится актуальнее с каждым годом. С помощью высокопроизводительных квантовых компьютеров злоумышленники смогут атаковать данные, защищённые традиционными методами шифрования. На горизонте нескольких лет небезопасными становятся многие традиционные алгоритмы криптографии:

- Распределение ключей
- Асимметричное шифрование
- Электронная подпись

Квантовая угроза усиливает ключевые риски кибербезопасности по ряду направлений:

1. Сетевая инфраструктура
2. Стандартное программное обеспечение
3. Интернет вещей
4. Блокчейн-решения

Источник: Наука.РФ[1]

Квантовая угроза становится актуальнее с каждым годом. Мощность зарубежных квантовых компьютеров возрастает, а наличие облачного доступа упрощает их использование.

Отечественные квантовые компьютеры развиваются под контролем Госкорпорации «Росатом» в рамках реализации дорожной карты высокотехнологичной области «Квантовые вычисления» и атак от них мы не ждем.

МАКСИМ БУДКИН

Руководитель направления, эксперт в области квантовых технологий, Банк ДОМ.РФ

Мы оставляем приоткрытой цифровую дверь, надеясь, что в неё никто не догадается войти, если не проявляем интерес к условиям новой технологической среды. Постквантовая криптография — это не попытка угнаться за угрозой, а шанс опередить её, пока она не получила форму. Переход к новым стандартам займёт годы, а квантовый прорыв может занять минуты. Начать сейчас — это выиграть время, а значит — сохранить безопасность в мире, где время становится очень дорогим ресурсом.

[1] По данным Наука.РФ: *наука.рф*

Постквантовые алгоритмы

Постквантовые алгоритмы — оптимальный метод защиты ценных данных от квантовой угрозы. Это новый класс асимметричных алгоритмов шифрования, устойчивых к кибератакам с применением как классических, так и квантовых компьютеров. Постквантовая криптография может быть легко интегрирована с серверной инфраструктурой, мобильными и веб-сервисами.

ИНФРАСТРУКТУРА, С КОТОРОЙ МОЖЕТ БЫТЬ ИНТЕГРИРОВАНА ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ


Пользовательские данные


Хранение данных


Аутентификация


Внутренние и внешние коммуникации


Электронный документооборот

ОТЛИЧИЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ ОТ КВАНТОВОЙ КРИПТОГРАФИИ

	Постквантовая криптография	Квантовое распределение ключей
Область применения	Асимметричное шифрование, схемы цифровой подписи, механизмы инкапсуляции ключа	Распределение симметричного ключа
Безопасность	Основана на математических предположениях, проверенных временем	Основана на законах квантовой механики
Реализация	Программная, но может быть ускорена аппаратно	Аппаратная
Стоимость	Невысокая, так как основные решения являются программными	Высокая цена из-за использования специализированного оборудования
Сертификация	Россия: Технический комитет ТК26 Росстандарта Мир: конкурсы NIST, CACR	Россия: Технический комитет ТК26 Росстандарта Мир: Проекты ETSI, ISO, ITU-T
Коммуникация	Может использоваться в любых цифровых типах коммуникации (беспроводные сети, оптические каналы и т. д.) на любом расстоянии	В основном используются волоконно-оптические линии связи (ВОЛС). На данный момент соединение между двумя точками ограничено 100 км при использовании оптоволоконных линий связи и практически не ограничено при использовании атмосферных оптических линий связи (АОЛС)

CACR: Конкурс, по выбору постквантовых криптографических алгоритмов, который проводила в течение 2018-2019 Китайская ассоциация криптологических исследований (CACR, Chinese Association for Cryptologic Research), источник: сайт QApp

NIST: Комплекс мероприятий, организованный Национальным институтом стандартов и технологий США с целью стандартизации набора квантово-устойчивых криптографических схем инкапсуляции ключа и цифровой подписи, источник: сайт QApp

ЧТО ПОЧИТАТЬ ПО ТЕМЕ?

АНО «Цифровая экономика» совместно с Ассоциацией ФинТех и Российским квантовым центром подготовили отчет «Перспективные сценарии применения квантовых и смежных технологий в отраслях». Материал включает перспективные сценарии пилотирования постквантовой криптографии и конфиденциальных вычислений в финансовом секторе, ритейле и телекоммуникациях.

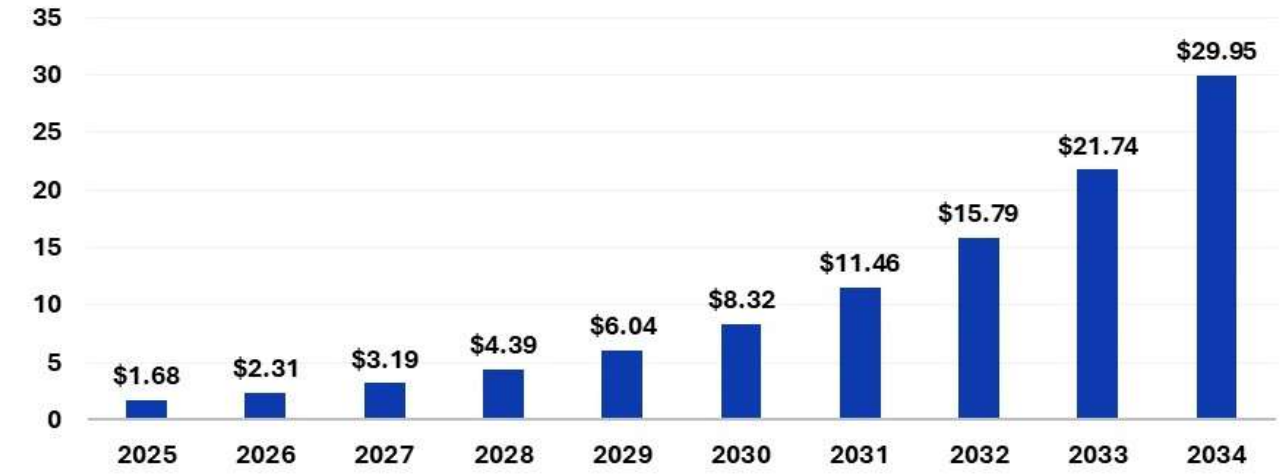
Источник:

d-economy.ru

Глобальный рынок постквантовой криптографии

Постквантовая криптография — новые асимметричные криптографические алгоритмы, устойчивые к кибератакам с применением как классических, так и квантовых компьютеров. Разрабатываемые и используемые сегодня квантово-устойчивые решения информационной безопасности на основе постквантовых алгоритмов не заменяют традиционные методы шифрования, а усиливают их.

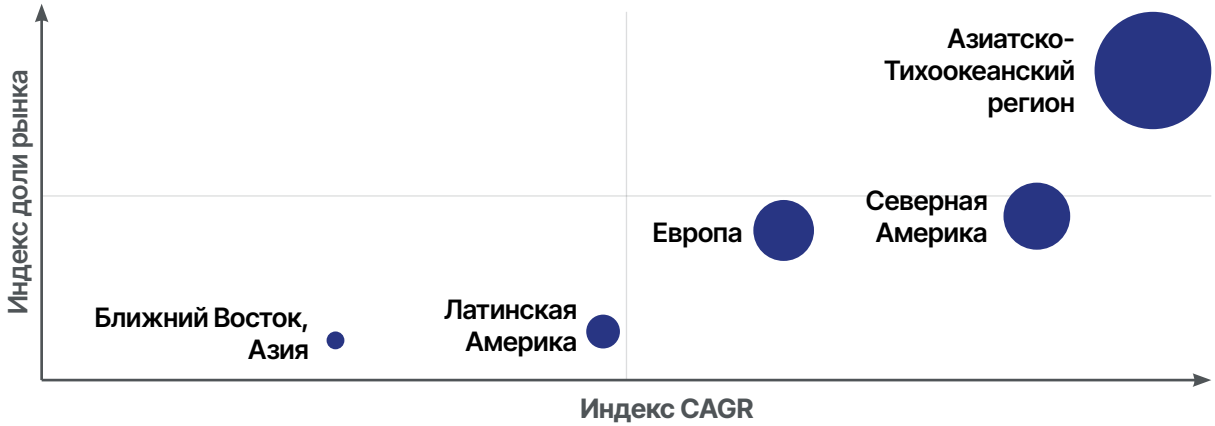
ОЦЕНКА ГЛОБАЛЬНОГО РЫНКА ПОСТКВАНТОВОЙ КРИПТОГРАФИИ НА 2025-2034 ГГ., МЛРД ДОЛЛ. США[1]



Программные решения на основе постквантовых алгоритмов не требуют привнесения новых специализированных аппаратных решений в инфраструктуру конечного бизнес-клиента, при этом некоторые параметры постквантовых алгоритмов могут быть **ускорены на аппаратном уровне.**

За последние несколько лет в мире возросла актуальность квантовой угрозы. Государства и бизнес переходят на постквантовые решения, что подтверждается ростом объёма глобального рынка.

ПЕРСПЕКТИВЫ РАЗВИТИЯ ГЛОБАЛЬНОГО РЫНКА ПОСТКВАНТОВОЙ КРИПТОГРАФИИ ПО РЕГИОНАМ[2]



Согласно прогнозам, именно **Азиатско-Тихоокеанский регион** продемонстрирует наиболее впечатляющий рост, показав максимальный среднегодовой темп увеличения (CAGR) в обозримой перспективе.

[1] По данным precedenceresearch: *precedenceresearch.com*

[2] По данным Growth Market: *growthmarketreports.com*

Зарубежные решения в области постквантовой криптографии

США опубликовали первые постквантовые стандарты

NIST National Institute of Standards and Technology U.S. Department of Commerce

Источник:

3 августа 2024 года **Национальный институт стандартов США (NIST)** опубликовал окончательные версии первых стандартов в области постквантовой криптографии:

• FIPS 203 (ML-KEM) • FIPS 204 (ML-DSA) • FIPS 205 (SLH-DSA)

Стандартизованные алгоритмы, разработанные в ходе конкурса, будут служить качественным инструментом защиты данных.

Представлен прототип первого чипа, поддерживающего постквантовые алгоритмы

PQSHIELD

Источник:

Новый чип от **PQCShield** защищён согласно недавно вышедшим стандартам NIST и поддерживает большинство актуальных постквантовых алгоритмов.

С помощью чипа PQCShield тестирует продукты с позиции клиента, получая данные по энергопотреблению и производительности. Исследователи также оценивают, насколько хорошо чип защищен от атак злоумышленников по сторонним каналам.

Европол предупреждает о необходимости срочного перехода на квантово-защищённую криптографию для финансового сектора

European Commission

Источник:

Еврокомиссия выпустила рекомендации по разработке дорожной карты по переходу на постквантовую криптографию. Дорожная карта должна быть разработана в течение ближайших двух лет.

При этом Европол предупреждает о растущей угрозе атак **«Сохранение данных сейчас – взлом потом»**, при которых злоумышленники крадут зашифрованные данные в надежде взломать их в будущем с помощью квантовых компьютеров. По мнению ведомства, финансовые организации Европы должны уже сейчас начинать подготовку к переходу на квантово-защищённую криптографию.

Microsoft добавила постквантовые алгоритмы в открытую библиотеку SymCrypt

Microsoft

Источник:

Постквантовые алгоритмы добавлены в открытую библиотеку **SymCrypt**, предоставляющую базовые криптографические функции, применяемые в таких проектах Microsoft, как Windows, Azure, Microsoft 365, Azure Stack HCI и Azure Linux.

Библиотека SymCrypt написана на языке Си и распространяется под лицензией MIT. В Linux библиотека SymCrypt также поддерживается.

Linux Foundation объявила о создании альянса Post-Quantum Cryptography

LINUX FOUNDATION

Источник:

Альянс планирует подготовить **реализации стандартизированных постквантовых алгоритмов**, обеспечить их сопровождение, а также участвовать в стандартизации и создании прототипов новых постквантовых алгоритмов.

В число учредителей вошли компании **Amazon Web Services (AWS), Google, IBM, NVIDIA** и другие. В настоящее время альянсом реализуется два проекта:

1. Open Quantum Safe
Проектом разрабатывается открытая Си-библиотека liboqs с реализацией постквантовых алгоритмов, а также подборка проектов по интеграции данных алгоритмов в различные протоколы.

2. PQ Code Package
Проект нацелен на создание и сопровождение высоконадёжных реализаций постквантовых алгоритмов, продвигаемых в качестве стандартов.

Apple выпустила новый протокол шифрования PQ3 для iMessage, который обеспечивает постквантовую защиту переписок

Apple

Источник:

Apple решила действовать на опережение, внедрив **PQ3** — протокол, который сохраняет совместимость с обычными устройствами, но при этом **устойчив к квантовым атакам**.

Блокчейн Ethereum защищен от квантовых атак

Виталий Бутерин, соучредитель Ethereum, заявил, что блокчейн-платформа уже имеет механизмы защиты от потенциальных атак с использованием квантовых компьютеров.

Для защиты Ethereum разработчики планируют внедрить новый тип транзакций в рамках **протокола RIP-7560**. Он будет использовать Winternitz-подписи и STARK-доказательства, позволяя переводить существующие кошельки на новые коды верификации. Это предотвратит раскрытие приватных ключей и сделает аккаунты устойчивыми к квантовым атакам.

Источник:

Zoom внедряет постквантовое шифрование для видеоконференций

Компания Zoom Video Communications объявила о глобальном **запуске постквантового сквозного шифрования (E2EE)** для продукта «Zoom Meetings» в рамках платформы «Workplace». Новая система безопасности призвана противостоять потенциальным атакам с использованием квантовых компьютеров в будущем. Хотя высокопроизводительные квантовые компьютеры пока не получили широкого распространения, **компания заранее модернизировала алгоритмы шифрования**, чтобы обеспечить долгосрочную защиту пользовательских данных.

Источник:

Рынок постквантовых решений в России

Рынок постквантовых решений в России активно формируется, демонстрируя значительный рост и привлекая внимание как государственных, так и частных игроков. В условиях глобальной цифровой трансформации и возрастающих киберугроз **разработка, стандартизация и последующее внедрение постквантовых алгоритмов становятся ключевым направлением обеспечения информационной безопасности.**

Разработка государственных стандартов в этой области вышла на новый уровень: ведутся активные работы по созданию нормативной базы, которая определит требования к криптографическим алгоритмам, устойчивым к квантовым атакам. Российские научные институты, ИТ-компании и регуляторы совместно участвуют в формировании этих стандартов, чтобы обеспечить безопасность критической инфраструктуры и цифровых сервисов в долгосрочной перспективе.

Разработка новых государственных стандартов в Техническом комитете по стандартизации «Криптографическая защита информации». *За техническим комитетом закреплены объекты стандартизации, относящиеся к методам криптографического шифрования информации, способам их реализации, а также методам обеспечения безопасности ИТ.*

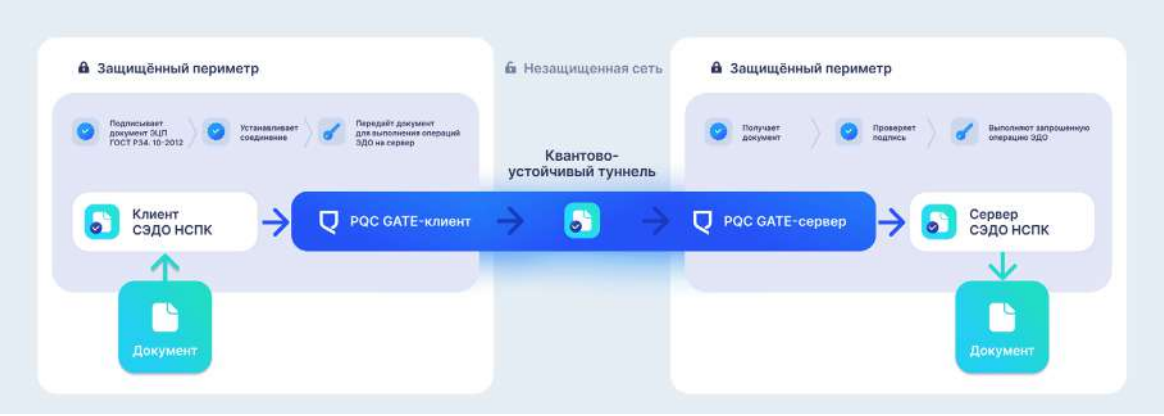
Источник:

ПРИМЕРЫ ПИЛОТНЫХ ИНТЕГРАЦИОННЫХ ПРОЕКТОВ ПО ПОСТКВАНТОВОЙ КРИПТОГРАФИИ В РОССИИ

Постквантовое шифрование документооборота Национальной системы платежных карт

Цифровой продукт QApp PQC GATE использовался как обратный прокси, выполняющий туннелирование трафика системы электронного документооборота. Обмен документами с банками НСПК осуществляет через квантово-устойчивый туннель, построенный с применением алгоритмов постквантовой криптографии.

Защищаемые данные: Клиринг, транзакционные отчеты, отчеты по нетто-позиции, диспутная и другая информация.



Источник:

Квантово-устойчивое шифрование канала передачи резервных копий данных Московской биржи

QApp

MOEX

Источник:

Реализация квантово-устойчивого туннеля между двумя удаленными площадками Московской биржи для передачи зашифрованных резервных копий данных больших размеров.

Защищаемые данные: резервные копии данных больших размеров.

Постквантовое шифрование в платформе видеоконференций «DION»

QApp

DION

Источник:

Сервис DION стал первой отечественной ВКС-системой, способной на программном уровне противостоять кибератакам с применением квантовых компьютеров.

ВТБ принял участие в тестировании полностью защищенного постквантовыми алгоритмами канала связи между пользователем и сервером.

Результатом тестового внедрения стал первый сеанс видеосвязи, в котором приняли участие председатель ЦБ РФ Эльвира Набиуллина и старший вице-президент ВТБ Сергей Безбогов.

Защищаемые данные: видео и аудио-коммуникации.

Постквантовое шифрование в блокчейн-платформе «Конфидент»

Компании QApp и Web3 Tech совместно разработали и апробировали **первую в России блокчейн-платформу** с постквантовым шифрованием, защищенную от взлома при помощи квантовых компьютеров.

Защищаемые данные: данные государственных и корпоративных информационных систем.

Источник:

КИРИЛЛ АНТОНОВ

Директор по развитию, Web3 Tech

Постквантовая криптография перестаёт быть экспериментом — она становится новой нормой для финансовых инфраструктур.

В ходе пилота мы подтвердили, что возможен гибридный переход от классических схем к постквантовым подписям и обмену ключами без ломки существующих процессов. Это важный сигнал рынку: постквантовая защита может встраиваться в банковские АБС, кастодиальные хранилища, DeFi-протоколы и смарт-контракты, сохраняя требуемую производительность и удобство интеграции — будь то через HSM/KMS или SDK для узлов и кошельков.

Для финансовых организаций и госструктур связка «блокчейн + постквантовое шифрование» решает две критические задачи одновременно: защищает долгоживущие данные и транзакции от сценария «собери сейчас — расшифруй потом» и повышает устойчивость реестров к подделке «задним числом». Это фундамент доверия к токенизации активов, платежам, цифровым валютам и конфиденциальным ведомственным системам — сегодня и через десятилетия.

Пилотный интеграционный проект «Квантово-устойчивая защита host-to-host коммуникаций»

ГАЗПРОМБАНК

QApp

Источник:

Основные сигналы к старту проекта

Технологии квантовых вычислений представляют собой серьезную угрозу для используемых в настоящее время традиционных асимметричных алгоритмов криптографии. Асимметричные криптографические алгоритмы являются важной частью систем безопасности для защиты персональных и финансовых данных, а также корпоративной и банковской тайны.

Основные риски соединений host-to-host финансового сектора, в том числе при реализации модели квантовой угрозы «Сохранение данных сейчас — взлом потом»:

• Финансовые риски при судебных издержках (при обнаружении взлома коммуникаций и краже данных),

• Упущенная коммерческая выгода и потеря клиентов,

• Репутационные риски, включая шантаж банка расшифрованным трафиком (выписки и данные клиентов),

• Фрод по платежам, подмена реквизитов.

Результаты проекта

Специалисты QApp совместно с Банк ГПБ (АО) реализовали уникальный для РФ пилотный интеграционный проект по обеспечению квантово-устойчивой безопасности host-to-host соединений Газпромбанка.

Проект был реализован путем интеграции в инфраструктуру host-to-host соединений Газпромбанка программного продукта PQC GATE — клиент-серверного решения, которое позволяет обеспечить квантово-устойчивое соединение в сетях любой топологии. Решение PQC GATE использует библиотеку постквантовых алгоритмов PQLR, взлом которых невозможен с применением классических и квантовых компьютеров.

Проект по квантово-устойчивой защите данных Газпромбанка получил высокое признание и был удостоен премии RB Digital Awards 2022 в номинации «Кибербезопасность». Премию RB Digital Awards вручают компаниям, которые сумели повысить эффективность бизнеса с помощью новых технологий.

Газпромбанк совместно с QApp намерены и дальше активно развивать сотрудничество, внедряя самые инновационные разработки в области криптографии и безопасности. Полученный опыт можно масштабировать для защиты различных информационных систем банка от квантовых угроз, например мобильных сервисов или ДБО корпоративных клиентов.

Пилотный интеграционный проект «Квантово-устойчивые мобильные BLE-платежи»

НСПК
QApp
ГАЗПРОМБАНК

Источник:

О проекте

В рамках пилотного проекта специалистами QApp при поддержке АО «НСПК» и Банка ГПБ (АО) было разработано ПО «PQC PAY», позволяющая проводить квантово-устойчивые платежи посредством протокола BLE, в том числе в условиях отсутствия подключения устройств к сети интернет.

Проект позволил впервые апробировать технологию квантово-устойчивой защиты бесконтактной оплаты на основе отечественных постквантовых алгоритмов. Данные платёжной транзакции подписываются отечественной электронной цифровой подписью «Гиперикум» (из состава ПО «PQC SDK») и передаются по протоколу BLE между устройствами, выполняющими роль «платёжного средства» и «платёжного терминала», выполненных в виде мобильного приложения, реализующего BLE-кошелек способный функционировать и в режиме офлайн.

Проект стал победителем премии FINAWARD 2025 в категории «Финтех-проект года». Премия учреждена деловым журналом «Банковское обозрение» и оценивает результаты ярких продуктовых и ИТ-внедрений в финансовом секторе.

Презентация проекта на FINOPOLIS 2024

Проект был представлен в рамках форума инновационных финансовых технологий FINOPOLIS 2024.

Демонстрация работы продукта PQC SDK на платформе Эльбрус-8С

эльбрус

QApp

Производитель отечественных универсальных микропроцессоров МЦСТ совместно с разработчиком комплексных квантово-устойчивых программных решений кибербезопасности QApp завершил пилотный проект по демонстрации работы библиотеки постквантовых алгоритмов на процессорах «Эльбрус».

По итогам демонстрации совместимости программного продукта с архитектурой микропроцессора эксперты провели первые замеры ключевых характеристик: времени генерации ключей, процедур цифровой подписи и механизмов выработки общего ключа (инкапсуляции/декапсуляции) для защиты информации в системах.

Источник:

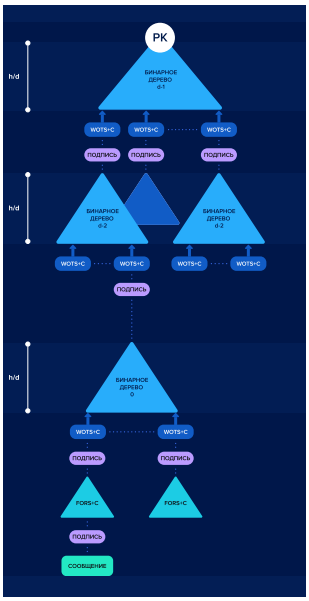
Разработан новый постквантовый алгоритм цифровой подписи «Гиперикум»

QApp

гиперикум

«Гиперикум» — алгоритм-кандидат на включение в новые государственные стандарты РФ по постквантовой криптографии.
Разработка ведется в рамках профильной подгруппы Технического комитета ТК26 Росстандарта.

Источник:



Опубликована первая в России открытая реализация алгоритма

Алгоритм представлен на профильных мероприятиях

конференция РусКрипто · РКИ ФОРУМ Россия 2023 · Музей криптографии · НФО Берег

Демонстрация работы продукта PQC SDK на платформе Байкал-М

В ходе выполнения данного проекта было выполнено портирование одной из ключевых компонент ПО «PQC SDK» на отечественную платформу «Байкал-М». Также было проведено сравнение производительности используемых в PQC SDK постквантовых алгоритмов, включая проверку применимости ГОСТ хэш-функций.

Источник:

Образовательные инициативы в области постквантовой криптографии

В сфере постквантовой криптографии активно развиваются образовательные инициативы, помогающие специалистам оставаться в курсе современных технологий:

Специализированные образовательные продукты – доступны онлайн-курсы, вебинары и учебные программы от ведущих экспертов в области квантово-устойчивых алгоритмов.

Компании с образовательной лицензией – ряд организаций предлагают сертифицированное дополнительное профессиональное образование по постквантовой криптографии, включая практические занятия и тестирование.

Митапы и другие мероприятия – регулярные встречи, хакатоны и лекции на базе университетов и исследовательских центров, где можно обсудить последние тенденции с коллегами.

Открытая база знаний[1] – статьи и научные работы, позволяющие углубленно изучать постквантовую криптографию.

Ведущие вузы, занимающиеся исследованиями в области постквантовой криптографии:

МГТУ им. Н.Э. Баумана · ИТМО · ГУАП · МФТИ · ЮФУ · МИЭМ · Университет Лобачевского · ПГУТИ · Новосибирский государственный университет *настоящая наука · Университет Иннополис

БАСТРАКОВА МАРИНА

Заведующий лабораторией теории наноструктур НИФТИ ННГУ, к.ф.-м.н.

В Университете Лобачевского ведутся научно-исследовательские работы по квантово-устойчивой защите инфраструктуры платежных терминалов в рамках стратегического технологического проекта «Нейроморфные и квантовые технологии искусственного и гибридного интеллекта» программы «Приоритет-2030» при поддержке индустриального партнёра — Газпромбанка. Реализация проекта и последующее пилотирование в ограниченном периметре станет важным шагом на пути к созданию опережающих решений защиты данных финансовой отрасли от будущих киберугроз.

[1] https://qapp.tech/help

Образовательные ресурсы по постквантовой криптографии

В МГТУ им. Н.Э. Баумана при поддержке технологических партнеров внедряются передовые технологии в учебный процесс, расширяя горизонты для студентов и специалистов.

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ ДЛЯ СТУДЕНТОВ

На **кафедре ИУ10 «Защита информации»** МГТУ им. Н.Э. Баумана тематика интегрирована в образовательные программы для студентов, обучающихся по направлению информационной безопасности, в том числе по специализации **«Безопасность автоматизированных систем в кредитно-финансовой сфере»**.

Теперь студенты изучают постквантовую криптографию **на реальных кейсах:** от теории и математики до практических решений. Это позволяет будущим специалистам не только освоить теоретические основы, но и сформировать практические навыки работы с современными методами защиты информации.

Источник:

ПРОФПЕРЕПОДГОТОВКА ДЛЯ СПЕЦИАЛИСТОВ ПО ИБ

Для заместителей руководителей организаций по ИБ и специалистов в области ИБ демонстрируются **экспертные видеолекции от QApp в рамках реализации программ дополнительного профессионального образования** в БАУМАНТЕХе. Слушатели на обучении узнают о ключевых аспектах постквантовой криптографии и ее критической важности в современном мире: актуальность квантовой угрозы, разработка новых алгоритмов и их стандартизация, направления интеграции и опыт пилотирования. На курсе **«Управление информационной безопасностью в организации»** уже было обучено **более 300 специалистов.**

Источник:

МЕРОПРИЯТИЯ И ПРОФЕССИОНАЛЬНОЕ СООБЩЕСТВО

В 2025 году на площадке МГТУ им. Н.Э. Баумана при экспертной поддержке компании QApp прошел **митап по постквантовой криптографии.** Мероприятие собрало более **160 участников** — студентов, исследователей и ИТ/ИБ-специалистов, интересующихся безопасностью в условиях развития квантовых технологий.

Спикеры раскрыли основные темы: риски квантовых вычислений для безопасности, различия между классической, квантовой и постквантовой криптографией, а также представили обзор пилотных проектов в России и мире.

Источник:

ЛЕТНЯЯ ШКОЛА «КРИПТОГРАФИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Традиционное мероприятие, организуемое **Криптографическим центром (Новосибирск) и Математическим центром в Академгородке** в сотрудничестве с разными принимающими сторонами. Летняя школа уже проходила в Санкт-Петербурге, Новосибирске, Калининграде, Таганроге и ежегодно собирает множество увлечённых криптографией студентов и преподавателей.

В течение двух недель студенты **выполняют научно-исследовательские проекты под руководством опытных криптографов**, слушают лекции, готовят тезисы и выступают на отчётной конференции, посещают экскурсии и спортивные занятия.

Темы проектов затрагивают различные вопросы современной криптографии и информационной безопасности.

В 2023, 2024 и 2025 годах Летняя школа включала темы докладов и проекты по постквантовой криптографии.

Cryptographic Center (Novosibirsk)

МАТЕМАТИЧЕСКИЙ ЦЕНТР В АКАДЕМГОРОДКЕ

Источник:

НАД ИССЛЕДОВАНИЕМ РАБОТАЛИ:

ИССЛЕДОВАНИЯ & АНАЛИТИКА АФТ

МАРИАННА ДАНИЛИНА

Руководитель Управления стратегии, исследований и аналитики **АФТ**

МАРИЯ ЧЕРНЫШЕВА

Ведущий бизнес-аналитик **АФТ**

АЛЕКСАНДРА ЩЕДРИНА

Арт-директор **АФТ**

ПРИВЛЕЧЕННЫЕ ЭКСПЕРТЫ

АНТОН ГУГЛЯ

Генеральный директор **«QApp»** (ООО «КуАпп»)

МАКСИМ БУДКИН

Руководитель направления, эксперт в области квантовых технологий **Банк ДОМ.РФ**

АССОЦИАЦИЯ ФИНТЕХ

ИССЛЕДОВАНИЯ & АНАЛИТИКА

research.analytics@fintechru.org

ТЕЛЕГРАМ-КАНАЛ АФТ

WWW.FINTECHRU.ORG

Ассоциация ФинТех *основана в конце 2016 г. по инициативе Банка России и ключевых участников отечественного финансового рынка. Это уникальная площадка для конструктивного диалога регулятора с представителями бизнеса.*

Здесь формируется экспертная оценка инновационных технологий с учетом международного опыта, а также разрабатываются концепции финансовых технологий и подходы к их внедрению.