



ВПЕРЕДИ  
ВРЕМЕНИ  
И ТЕХНОЛОГИЙ

10

АСПЕКТЫ  
ПОСТКВАНТОВОЙ  
КРИПТОГРАФИИ

52

МОЦ КАРАНЕУ,  
БЕЗДАНЬ  
НЯБЕСАУ

62

ДТП  
С УЧАСТИЕМ  
ДИКИХ ЖИВОТНЫХ

70

# Наука и инновации

№8 (246)  
АВГУСТ 2023

научно-  
практический  
журнал

● **КВАНТОВЫЕ  
ТЕХНОЛОГИИ —**  
время  
больших  
ожиданий

ISSN 1818-9857



9 771818 985001 08

ISSN 2412-9372 (online)



НЕПРЕРЫВНО ИЗМЕНЯЯСЬ

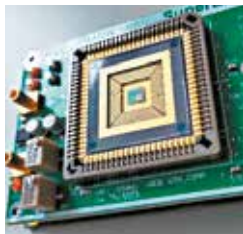


## ЦЕНТР «КВАНТОВАЯ ОПТИКА И КВАНТОВАЯ ИНФОРМАТИКА»

Института физики им. Б.И. Степанова  
НАН Беларуси проводит исследования  
в области квантовой оптики,  
квантовой коммуникации, квантовой  
сенсорики и квантовых процессов



Детекторы  
одиночных  
фотонов фирмы  
idQuantique



Высокоскоростная  
времяразрешающая  
матрица SuperEllen  
из  $32 \times 32 = 1024$   
лавинных  
детекторов  
одиночных  
фотонов  
с собственной  
оцифровкой  
времени отсчета



Быстродействующий  
цифровой  
осциллограф  
Tektronix MSDO64-  
BW4 с полосой 4 ГГц  
и частотой выборок  
до 25 ГГц



Анализатор  
оптического  
спектра  
771A-NIR-APC



Сканирующий  
ближнеполевой  
оптический  
микроскоп

## ДОСТИЖЕНИЯ И РАЗРАБОТКИ

пр. Независимости, 68-2, к. 1, комн. 486,  
220072, Минск, Беларусь  
тел. +375 17 2708613,  
+375 17 2708442,  
факс +375 17 2708879 (с пометкой «для ЦКОКИ»)  
<https://master.basnet.by/lqo/>  
E-mail: kilin at dragon.bas-net.by



**Схема квантового процессора на основе NV-центров в алмазе и ядерных спинов изотопа  $^{13}\text{C}$ , 2001 г. (совместно с университетом Штутгарта)**



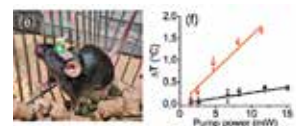
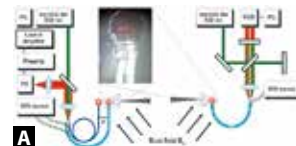
**Первая в СНГ оптоволоконная линия квантового распределения ключа на основе кодирования фотонов во временные окна (time-bin coding) 50 км, 2007 г.**



**Квантово-оптические генераторы случайных чисел на одиночных фотонах, используемые в криптографических системах для обеспечения информационной безопасности**



**Оптоэлектронный искусственный нейрон, на основе оптоэлектронной пары «вертикально-излучающий лазер – однофотонный лавинный фотодиод» – воспроизводит свойства биологических нейронов**



**Квантовые сенсоры на основе примесных центров в алмазе, (совместно с МГУ, 2016, 2020 гг.)**

Квантовый сенсор высокочувствительной векторной градиентометрии магнитного поля на основе NV-центров в алмазе (А).

Квантовый оптоэлектронный сенсор температуры мозга на основе микрокристалла алмаза с центрами окраски германий-вакансия (GeV) (Б).



Зарегистрирован в Министерстве информации Республики Беларусь, свидетельство о регистрации №388 от 18.05.2009 г.

**Учредитель:**

Национальная академия наук Беларуси

**Редакционный совет:**

В.Г. Гусаков – <i>председатель совета</i>	А.Е. Дайнеко А.И. Иванец
П.А. Витязь – <i>зам. председателя</i>	Н.С. Казак А.В. Кильчевский
С.А. Чижик – <i>зам. председателя</i>	Э.И. Коломиец С.А. Красный
Ж.В. Комарова	М.В. Мясникович
В.Ф. Байнев	О.Г. Пенязьков
О.Ю. Баранов	Ф.П. Привалов
А.И. Белоус	С.П. Рубникович
В.Г. Богдан	О.О. Руммо
С.В. Гапоненко	С.В. Харитончик
В.Л. Гурский	И.П. Шейко
	А.Г. Шумилин
	С.С. Щербаков

**Главный редактор:**

Жанна Комарова

**Ведущие рубрик:**

Ирина Емельянович	Татьяна Жданович
Наталья Минакова	Юлия Василичишина

**Дизайн и верстка:**

Алексей Петров

**Адрес редакции:**

220072, г. Минск, ул. Академическая, 1-129.  
Тел.: (017) 351-14-46,  
e-mail: nii2003@mail.ru,  
www.innosfera.belnauka.by

**Подписные индексы:**

**007 532 (ведомственная)**

**00 753 (индивидуальная)**

Формат 60x84 1/8. Бумага офсетная.

Усл. печ. л. 9,8. Тираж 542 экз.

Цена договорная.

Подписано в печать 18.08.2023.

**Издатель:** РУП «Издательский дом

«Беларуская навука». Свид. о гос. рег. №1/18 от 02.08.2013. г. Минск, ул. Ф. Скорины, 40. Заказ №168.

© «Наука и инновации»

При перепечатке и цитировании ссылка на журнал обязательна.

За содержание рекламных объявлений редакция ответственности не несет.

Мнение редакции не всегда совпадает с мнением авторов статей.

Рукописи не рецензируются и не возвращаются.

# Содержание

ТЕМА НОМЕРА: **КВАНТОВЫЕ ТЕХНОЛОГИИ**

*Александр Михальчев*

**Квантовая механика и ее основные принципы** ..... 4

В статье обсуждаются основы квантовой механики, особенности измерений и состояний микрообъектов, а также различия квантового и классического описания физических систем.

*Сергей Килин*

**Универсальный квантовый компьютер – впереди времени и технологий** ..... 10

Дан обзор достижений в сфере квантовых компьютеров, проанализирован уровень потенциальных возможностей, которыми могут обладать эти устройства, а также первых продуктов квантовых технологий.

*Глеб Салахов, Антон Божедаров, Алексей Федоров*

**Квантовые технологии: новые возможности, успехи и вызовы** ..... 18

В статье дан обзор состояния квантовых технологий на пути к их практическому применению.

*Илья Родионов, Ольга Ефремова*

**Квантовые вычисления: в поисках когерентности** ..... 24

Материал посвящен сверхпроводниковым квантовым схемам, занимающим одну из лидирующих позиций среди платформ для реализации вычислений нового поколения.

*Сергей Кулик*

**Квантовые сенсоры** ..... 31

Рассмотрена квантовая сенсорика как одно из перспективных научно-технологических направлений, благодаря которому создаются современные устройства, а также стимулируются передовые научные разработки в области квантовой механики.

*Дмитрий Могилевцев*

**Квантовые радары** ..... 37

Рассмотрены новые методы диагностики удаленных объектов с помощью квантовых радаров, позволяющих улучшать возможности обнаружения и распознавания движущихся либо стационарных целей.

*Алексей Акимов*

**Квантовые сенсоры на базе центров окраски в алмазе** ..... 41

Рассмотрено одно из важных направлений в развитии квантовых технологий будущего – квантовые сенсоры и метрология.

*Александр Низовцев, Александр Пушкарчук,  
Дмитрий Филимоненко, Сергей Килин*

## **Квантовые технологии на основе центров окраски азот-вакансия в алмазе**.....46

Представлен краткий обзор результатов компьютерного моделирования характеристик NV-центров в алмазе и их комплексов с ядерными спинами <sup>13</sup>C, использование полученных данных для реализации различных квантовых технологий на их основе.

*Геннадий Матвеев*

## **Математические аспекты постквантовой криптографии**.....52

Автор обосновывает необходимость приведения системы криптографической защиты информации в республике в соответствие с новыми постквантовыми требованиями.

*Жанна Комарова*

## **Доверие к технологиям**.....57

Ученые обсуждают перспективы квантовой криптографии, ее преимущества и недостатки.

### ЛАБОРАТОРИЯ НАДЕЖД

*Тацяна Ждановіч*

## **Моц каранёў, бездань нябёсаў. Як маладая беларуская даследчыца расшыфравала наш культурны код праз шохалісты**.....62

Нарыс пра маладога гісторыка і этнолага Яну Шаўчэнка, яе шлях да навукі і даследчыцкую працу, а таксама пра тое, чаму аснова нашага жыцця, фізічнага і духоўнага, схаваная пад зацэнню лясоў.

### БИОРАЗНООБРАЗИЕ

*Павел Гештовт, Степан Гузней*

## **ДТП с участием диких животных: закономерности и сравнительный анализ**.....70

Проанализированы разносторонние статистические данные, а также причины роста дорожной аварийности с участием диких животных. На основе изучения мирового опыта приведен перечень мероприятий, реализация которых поможет снизить количество таких ДТП в нашей стране.

### ДИССЕРТАЦИОННЫЕ ИССЛЕДОВАНИЯ

*Олег Кузнецов*

## **Клинико-генеалогические критерии опухолей кишечника**.....76

Предложены критерии формирования групп риска развития опухолей толстого кишечника, удобные для онкогенетического консультирования.



# Квантовая механика и ее основные принципы



**Александр Михальчев,**  
старший научный сотрудник  
Центра «Квантовая оптика  
и квантовая информатика»  
Института физики НАН  
Беларуси, кандидат физико-  
математических наук

К началу XX в. накопился ряд несоответствий между предсказаниями классической физики и экспериментально наблюдаемыми эффектами [1, 2]. В частности, традиционная теория предвещала бесконечно большую мощность излучения энергии нагретым телом, не могла объяснить, почему существует красная граница фотоэффекта, и предложить реалистичную модель атома, в которой бы электроны не падали на ядро. Результатом работы над возникшими противоречиями стало переосмысление основ физики и зарождение квантовой механики. Если прежние каноны строились последовательно и на каждом этапе были интуитивно понятны, то квантовая идея зародилась в значительной мере постулативно – на основе подбора математических конструкций, которые позволят воспроизвести наблюдаемые свойства реальности. Только в дальнейшем (параллельно с выработкой математического аппарата квантовой механики и даже с запозданием) появилась глубокая физическая интерпретация используемых математических объектов.

Практически с момента своего возникновения (в 1920–30-е гг.) квантовая механика начала приводить исследователей к нетривиальным и неожиданным предсказаниям: был сформулирован ряд квантово-механических парадоксов, включая широко известные – кота Шредингера [3] и Эйнштейна-Подольского-Розена [1]. В то время существовали значительные сомнения в корректности квантовой механики и области ее применения, причем даже среди основоположников этой теории. Например, критике подвергалось предсказание существования так называемых перепутанных

состояний, обеспечивающих сильные корреляции между квантовыми системами, сохраняющиеся даже на больших расстояниях, и высказывались предположения о неприменимости квантовой теории для описания нелокальных систем.

Некоторые из обнаруженных парадоксов лишь указывали на неприменимость классических принципов в отношении квантовых систем и их большую сложность, в то время как другие представляли собой предсказание важных эффектов, подтвержденных экспериментально через полвека и используемых сейчас для решения практических задач. Например, перепутанные состояния стали эффективным инструментом квантовой коммуникации и микроскопии. В настоящее время корректность предсказаний не вызывает сомнений благодаря многократным экспериментальным подтверждениям, однако по-прежнему остаются актуальными некоторые вопросы интерпретации квантовых принципов.

## Квантовые состояния

При построении аксиоматики квантовой механики ключевую роль играет состояние рассматриваемой системы, неразрывно связанное с процессом его приготовления и информацией об этом процессе, которая доступна наблюдателю. Квантовое состояние имеет принципиальное отличие от состояния в классической физике: оно является неотъемлемой частью описания и предсказания наблюдаемых эффектов, но недоступно для непосредственного измерения само по себе. В классической механике состояние материальной точки естественным образом определяется

ее положением и скоростью (импульсом): данные величины одновременно наблюдаемы и достаточны для предсказания последующей динамики системы. Для аналогичного квантового объекта не удается выбрать переменные, которые были бы достаточны для полного задания его состояния и одновременно наблюдаемы.

Из-за невозможности непосредственного измерения квантового состояния существует множество равноправных и эквивалентных методов описания таких систем. Например, чистое состояние материальной точки (процедура приготовления которого известна наиболее полно) может описываться волновой функцией  $\Psi(\vec{r})$  в координатном или  $\Psi(\vec{p})$  в импульсном представлении, а также абстрактным вектором  $|\Psi\rangle$  в линейном (гильбертовом) пространстве. Смешанное состояние (известное с некоторой долей неопределенности) моды электромагнитного поля описывается как оператором плотности  $\rho$ , так и функцией Глаубера-Сударшана  $P(\alpha)$ .

## Квантовый принцип суперпозиции

Важную особенность квантовой механики определяет принцип суперпозиции: для любых двух допустимых состояний системы линейная комбинация также является допустимым физическим состоянием. Например, квантовый бит (с двумя базисными состояниями  $|0\rangle$  и  $|1\rangle$ , аналог классического бита) может быть представлен в следующем виде (рис. 1А):

$$|\psi(\theta, \varphi)\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle. \quad (1)$$

Произвольное состояние, описываемое формулой (1), можно отобразить в виде точки на сфере Блоха, откладывая угол  $\theta$  от оси  $z$ , а угол  $\varphi$  от оси  $x$ . Каждая ее точка задает некоторое допустимое состояние квантового бита. Классическому биту доступны лишь базисные состояния «0» и «1», соответствующие полюсам сферы Блоха (рис. 1А).

Наличие квантовых суперпозиций указывает на возможность интерференционных эффектов, подобных интерференции классических волн (примером может служить дифракция электронов [4]). Однако у квантовых объектов и классических волн есть ряд фундаментальных отличий. Во-первых, возможность суперпозиционных состояний и квантовой интерференции присуща любым квантовым объектам, в том числе не обладающим волновыми свойствами в классическом понимании (например, частицам). Во-вторых,

классическая суперпозиция волн соответствует их одновременному воздействию на объект (измерительный прибор) и сложению соответствующих им комплексных амплитуд, в то время как квантовое суперпозиционное состояние указывает на параллельное существование нескольких возможностей, которые могут совместно (интерферируя) влиять на динамику квантового объекта, но при измерении реализуется только одна из них.

## Квантовые измерения

Поскольку наблюдаемые экспериментально величины и состояние квантовой системы не тождественны друг другу, важную роль в аксиоматике квантовой механики занимает подробное описание *квантового измерения* и его взаимосвязи с состоянием [5]. Этот процесс обусловлен двумя составляющими: измеряемой величиной и квантовым состоянием объекта. Возможные результаты (допустимые показания прибора) предопределяются самой измеряемой величиной, причем для многих (включая энергию) квантовая механика предсказывает дискретный спектр доступных значений. Квантовое состояние системы конкретизирует вероятности получения различных вариантов измерения (рис. 2). Если достоверно известен его исход, говорят, что оцениваемая величина имеет определенное значение в данном квантовом состоянии. В противном случае результат обладает *случайностью*.

Воспроизводимость идеального измерения (получение тех же показаний прибора при повторе) указывает на неизбежность изменения квантового состояния: при первом замере вероятны различные исходы, при последующих –

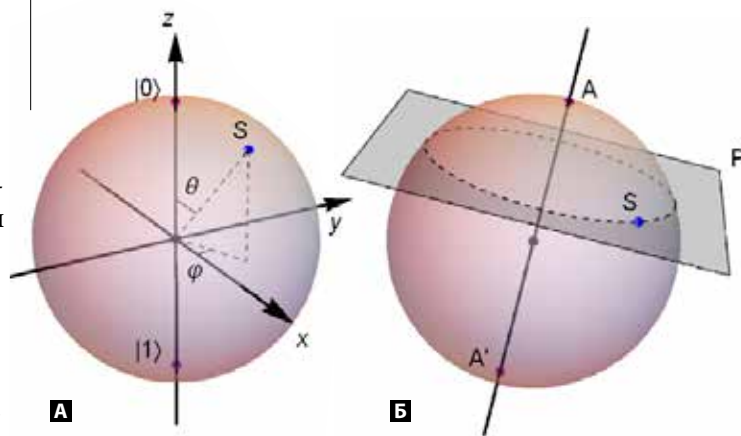


Рис. 1. Представление состояний квантового бита на сфере Блоха

результат известен с достоверностью. Таким образом, из ряда доступных возможностей, определяемых входным квантовым состоянием, выделяется и фиксируется одна, соответствующая полученному показанию прибора. Редукция состояния (коллапс волновой функции) является фундаментальной особенностью квантового измерения в копенгагенской интерпретации квантовой механики [6].

Принципиальная особенность квантового описания – существование *несовместных* наблюдаемых величин, то есть таких физических характеристик объекта, которые не могут одновременно иметь определенные значения ни в одном его квантовом состоянии. Типичный пример – пара «координата материальной точки» и «её импульс» (точнее, его проекция на соответствующую координатную ось) – величины, связанные соотношением неопределенностей Гейзенберга [6]. Логично предположить, что, проведя достаточно большое количество различных идеальных измерений, можно получить исчерпывающую информацию о системе и результирующее чистое квантовое состояние будет соответствовать нашему максимально подробному знанию. С другой стороны, согласно соотношению неопределенностей, даже в таком состоянии мы не можем с достоверностью предсказать результат некоторых измерений. Таким образом, даже максимально точное задание состояния системы не приводит к четкому знанию

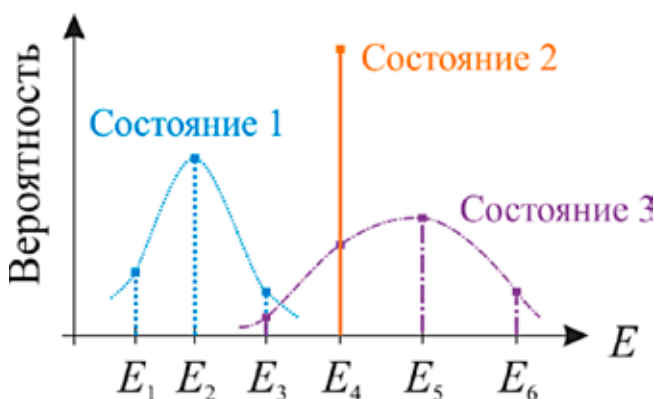


Рис. 2. Возможные результаты измерения и их вероятности. Схематично представлено измерение энергии  $E$  некоторой модельной квантовой системы. Набор допустимых результатов (показаний прибора)  $E_1, \dots, E_6$  определяется свойствами исследуемого объекта и прибора (измеряемой величины), в то время как конкретное квантовое состояние несет в себе информацию о вероятностях различных результатов. В состояниях 1 и 3 присутствует неопределенность энергии, а в состоянии 2 энергия имеет определенное значение  $E = E_4$  и результат измерения известен заранее

всех ее наблюдаемых свойств. Так проявляется вероятностный характер квантовой механики.

В классической физике (например, в статистической физике или термодинамике) некоторые физические величины также могут быть определены не точно и описываться распределением вероятностей. Причина тому – неполнота нашего знания, устраняемая (в идеальном случае) путем получения дополнительной информации при измерениях. В квантовой же физике неопределенности носят фундаментальный характер. Они проявляются даже при наличии максимальной информации о системе. Попытка избавиться от неопределенности одной физической величины (например, координаты) путем ее измерения приводит к редукции состояния и увеличивает неопределенность других величин, несовместных с данной – например, импульса [5].

## Проблемы и интерпретации квантовой механики

Соотношения неопределенностей, фундаментальная случайность при квантовых измерениях, необходимость разделения понятий истинного состояния и наблюдаемых характеристик квантовой системы, существование суперпозиций – не просто следствия произвольно выбранного для описания математического аппарата. Необходимость введения определенных свойств в математические модели квантовой механики была продиктована результатами экспериментов, необъяснимыми более привычным для классической физики образом. Например, уже ранние эксперименты по наблюдению интерференции электронов указывали на проявление несовместимых с классической точкой зрения свойств [7]: детектирования в виде локализованных частиц и интерференции в пространстве (рис. 3). Такое поведение квантовых объектов (получившее название корпускулярно-волнового дуализма), как и другие законы, не совпадает с привычными правилами, «здоровым смыслом». Как следствие, квантовая теория, описывающая эффекты микромира, вынуждена строиться противоречащим нашей интуиции образом и требует дополнительного философского осмысления и интерпретации ее постулатов и предсказаний [2].

Мы не в состоянии точно представить, что есть квантовые объекты на самом деле, поскольку не встречаемся с характерными для них свойствами в обычной жизни, однако можем проводить аналогии их поведения с тем, что знаем: с волнами и части-

цами. Доступная информация о квантовых объектах ограничивается результатами экспериментов, которые, в свою очередь, зависят от типов проводимых измерений – «вопросов», которые мы задаем исследуемой системе. Согласно копенгагенской интерпретации квантовой механики, именно выбор измерительной установки определяет те черты, которые квантовая система проявит при наблюдении.

Описание процесса измерения – ключевого элемента квантовой механики – также сопряжено с рядом сложностей. Если применимость квантовой теории не ограничивается объектами микромира, то и измерительный прибор, и даже наблюдатель, также должны подчиняться ее законам. Тогда процедура оценки сведется к взаимодействию нескольких квантовых систем: микроскопического объекта и макроскопических прибора и наблюдателя. Если состояние исследуемого объекта было суперпозиционным, то прибор и наблюдатель также окажутся в таком состоянии, его редукция не произойдет, и останутся доступными все присутствующие возможности. Это категорически противоречит нашему восприятию мира – ожиданию увидеть вполне определенное показание прибора (реализацию лишь одной из возможностей). Для разрешения данного противоречия в традиционной копенгагенской интерпретации постулируется, что измерение происходит скачкообразно, не подчиняется уравнениям непрерывной квантовой динамики и вызывает редукцию состояния (переход от возможного, заложенного в квантовом состоянии, к действительному – результату измерения). Более убедительное обоснование такого процесса можно дать, если принять во внимание необратимость динамики сложных макроскопических систем и процесс декогеренции, описанный ниже. Существуют и альтернативные трактовки. Например, согласно одной из интерпретаций, все возможности, заложенные в суперпозиционном состоянии наблюдателя после измерения, продолжают существовать, порождая отдельные версии Вселенной, в которых наблюдатель будет обладать различным опытом (записями о результатах эксперимента) [8].

Еще более сложным для понимания процесс измерения оказывается при рассмотрении составных квантовых систем: например, двух частиц, родившихся при распаде исходной элементарной частицы и разлетевшихся на достаточно большое расстояние. Сильные корреляции характеристик (энергий, импульсов, положений в пространстве) не позволяют описывать их квантовые состояния отдельно, требуя введения коллектив-



Рис. 3. Схема экспериментов по наблюдению интерференции электронов. Одиночные частицы – электроны – проходят через щели и регистрируются на экране. Каждая из них детектируется в некоторой вполне определенной точке, то есть проявляет привычные для частиц свойства. Однако рисунок, возникающий на экране при накоплении большого количества зарегистрированных электронов, имеет вид, характерный для интерферирующих волн. Такой эффект сохраняется, даже если электроны летят по одному (следующий вылетает не раньше, чем произошло детектирование предыдущего). Это позволяет предположить, что способность интерферировать, «чувствуя» одновременно обе щели, – не коллективный эффект (как в случае волн на поверхности водоема или звуковых волн), а свойство каждой отдельной частицы

ного нелокального (перепутанного) квантового состояния. Измерение одной частицы приведет к редукции нелокального состояния и, следовательно, дистанционно повлияет на вторую, причем мгновенно. Хотя такой процесс и не может служить для обмена полезной информацией (коммуникации) со скоростью, превышающей скорость света, мгновенное воздействие на расстоянии значительно расходится с основными принципами, заложенными А. Эйнштейном в начале XX в. Физики неоднократно пытались построить альтернативные теории, однако работа Дж. Белла и последующие эксперименты (в том числе с расстояниями между фотонами в перепутанном состоянии более 100 км) убедительно показали, что любая идея, не противоречащая реальным экспериментальным данным, обязана содержать некоторый элемент нелокальности [9].

## Особенности одиночных квантовых объектов

Существенный нюанс работы с одиночными квантовыми объектами задается теоремой о запрете квантового клонирования [10, 11].

Имея в наличии одиночный квантовый объект в заранее не известном состоянии, невозможно создать его клоны – другие квантовые объекты, гарантированно находящиеся в таком же состоянии. Попытка предварительно узнать состояние объекта с помощью измерения также обречена на неудачу: одиночное наблюдение не дает полной информации, но разрушает (изменяет) данное состояние. Таким образом, квантовая информация имеет скрытый характер: для точного задания квантового состояния нужно определить значения большего числа параметров, чем можно узнать в результате измерений, проводимых над одиночным объектом. Например, чистое состояние квантового бита (1) определяется двумя параметрами  $\theta$  и  $\varphi$ , в то время как одиночное измерение, проводимое над объектом, дает не более одного бита информации. На рис. 1Б проходящая через центр сферы Блоха прямая  $AA'$  задает идеальное измерение, проводимое над квантовым битом. Здесь возможны лишь два исхода, переводящие квантовый бит в состояния  $A$  и  $A'$ . При этом реализуется одна из двух возможностей, что соответствует получению 1 бита информации. Повторное измерение для ансамбля одинаковых квантовых объектов позволяет оценить вероятности двух исходов и определить плоскость  $P$ , в которой лежит характеризующая состояние квантового бита точка  $S$ . Чтобы найти ее положение (определить состояние квантового бита) необходимо провести повторные измерения как минимум 2 типов и получить 2 пересекающиеся плоскости.

Запрет получения полных данных о состоянии одиночного объекта в результате измерения, однако, не препятствует подробному анализу квантовых систем. Если существует ансамбль квантовых объектов в одинаковых состояниях (либо источник, позволяющий создавать их по требованию), можно провести специальную процедуру квантовой томографии – восстановления неизвестного квантового состояния по результатам нескольких типов измерения, повторяемых достаточно большое количество раз с одинаковыми объектами. Подобно классической томографии, каждый тип измерения задает некоторую «проекцию» пространства состояний квантовой системы на классическую наблюдаемую величину. Совместная математическая обработка таких проекций позволяет получить полную информацию об исходном квантовом состоянии рассматриваемых объектов.

Скрытый характер квантовой информации служит важным инструментом для защищенной коммуникации [11]. Данные (например, биты секретного ключа) можно кодировать в квантовых состояниях одиночных объектов: обычно для этого используются фотоны. Теорема о запрете квантового клонирования и редукция состояния при измерении запрещают полное и безошибочное считывание информации, закодированной в заранее не известном состоянии объекта, без ее повреждения. Вообще говоря, с данной проблемой сталкиваются как легитимный получатель сообщения, так и злоумышленник, пытающийся перехватить секретный ключ. Однако между ними есть принципиальное различие. Перехватчик, чтобы остаться незамеченным, должен корректно определять и воспроизводить квантовое состояние каждого отдельного объекта. Легитимный же получатель может отложить анализ наличия прослушки до накопления достаточной статистики (большого количества переданных битов) и сделать вывод о секретности передаваемого ключа с высокой точностью. Как следствие, методы квантовой криптографии обеспечивают защиту информации на основе фундаментальных физических принципов, гарантируя обнаружение перехвата ключей.

## Квантовое измерение как инструмент для управления состоянием

Обратное воздействие квантового измерения на исследуемый объект не только усложняет считывание информации, но и может служить эффективным инструментом для управления квантовыми системами – целенаправленного изменения или сохранения их состояний. Яркий пример такого влияния измерения на динамику квантового состояния – квантовый эффект Зенона [12], названный в честь апории древнегреческого философа Зенона Элейского, гласящей, что движущаяся стрела покоится, поскольку в каждый момент времени находится в определенной точке пространства. Если для классических объектов данное утверждение было призвано указать на противоречивость философских представлений о движении, то квантовый эффект Зенона тщательно подтвержден экспериментально: частое наблюдение за квантовым состоянием может «замораживать» квантовую динамику, препятствуя его переходу в какое-либо другое.



Квантовое измерение может не только оставаться квантовой динамикой, но и направлять ее желаемым образом. В частности, существуют вероятностные методы преобразования квантовых состояний. Чтобы придать объекту целевые свойства, можно подобрать такое измерение, которое при получении одного из возможных результатов гарантированно переведет систему в требуемое состояние [13].

## Открытые квантовые системы. Декогеренция

Реальные квантовые системы неизбежно взаимодействуют с окружением: макроскопическими объектами, обладающими большим числом степеней свободы. Возникают сильные корреляции (перепутанность) между состояниями квантового объекта и его окружения, а в дальнейшем – и всего мира. Хотя с теоретической точки зрения уравнения, описывающие такое взаимодействие, симметричны относительно прошлого и будущего, на практике обратить данный процесс невозможно. Чтобы наблюдать когерентные квантовые эффекты – интерференцию различных слагаемых квантовой суперпозиции – необходимо задействовать все описываемые данным состоянием квантовые объекты. После включения в коррелированное состояние окружения (и всего мира) такая интерференция становится невозможной. Таким образом, объект в результате взаимодействия с окружением теряет способность к проявлению когерентных свойств, и происходит *декогеренция* квантового состояния.

С одной стороны, именно воздействие окружения позволяет объяснить необратимое изменение состояния квантовой системы (редукцию) при измерении [2]. Взаимодействие с детектором приводит к декогеренции – превращению квантовой суперпозиции в смесь возможностей, не способных интерферировать между собой и полностью описываемых классическим распределением вероятностей. Считывание показания измерительного прибора наблюдателем лишь позволяет ему узнать, какая именно из данных возможностей реализовалась, подобно тому, как устраняется неопределенность знания о системе в классической физике. Важно отметить, что редукция состояния происходит фактически в результате взаимодействия с детектором и не требует дальнейшей регистрации его показаний мыслящим наблюдателем.

С другой стороны, декогеренция разрушает целевые суперпозиционные состояния квантовых объектов, препятствуя получению квантовых преимуществ в метрологии и обработке информации. Важно отметить, что разрушение квантовой когерентности может происходить значительно быстрее, чем изменение средней энергии квантового объекта. Например, если скорость затухания энергии оптической моды поля равна  $\gamma$ , суперпозиционное состояние может превратиться в смесь за время порядка  $N\gamma$ , где  $N$  – среднее число фотонов в данном состоянии. Именно этим эффектом обусловлены сложность работы с суперпозиционными квантовыми состояниями многочастичных систем и создание практических устройств, использующих квантовую интерференцию (например, квантовых компьютеров), не ранее, чем через 100 лет после появления квантовой механики.

Интересно отметить, что взаимодействие квантовой системы с макроскопическим окружением может не только разрушать ее квантовое состояние, но и обеспечивать полезные преобразования. Создавая резервуары (системы с большим числом степеней свободы) специальным образом, можно приводить квантовые объекты в целевые состояния, обеспечивая, например, уменьшение флуктуаций числа фотонов (дробовой шум) [14]. ■

### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бом Д. Квантовая теория / Д. Бом. – М., 1965.
2. Гриббин Дж. Шесть невозможностей: загадки квантового мира / Дж. Гриббин. – М., 2021.
3. Шредингер Э. Избранные труды по квантовой механике / Э. Шредингер. – М., 1976.
4. R. Bach. Controlled double-slit electron diffraction / R. Bach [et al.] // *New Journal of Physics*. 2013. Т. 15. №3. С. 033018.
5. Фон Нейман И. Математические основы квантовой механики / И. фон Нейман. – М., 1964.
6. Гейзенберг В. Физика и философия. Часть и целое / В. Гейзенберг. – М., 1989.
7. C. Davisson, L. H. Germer. Diffraction of electrons by a crystal of nickel / C. Davisson, L. H. Germer // *Physical review*. 1927. Т. 30. №6. С. 705.
8. Д. Дойч. Структура реальности. Наука параллельных вселенных / Д. Дойч. – М., 2014.
9. G. Brassard. Profile of John Clauser, Alain Aspect and Anton Zeilinger: 2022 Nobel laureates in Physics / G. Brassard // *Proceedings of the National Academy of Sciences*. 2023. Т. 120. №23. С. 2304809120.
10. С.Я. Килин. Квантовая информация / С.Я. Килин // *Успехи физических наук*. 1999. Т. 169. №5. С. 507–527.
11. Бауместер Д. Физика квантовой информации / Д. Бауместер, А. Экерт, А. Цайлингер. – М., 2002.
12. Л.А. Халфин. Квантовый эффект Зенона / Л.А. Халфин // *Успехи физических наук*. 1990. Т. 160, вып. 10. С. 185–188.
13. S. Ya. Kilin, A. B. Mikhalychev. Optical qudit-type entanglement creation at long distances by means of small cross-Kerr nonlinearities / S. Ya. Kilin, A. B. Mikhalychev // *Physical Review A*. 2011. Т. 83. №5. С. 052303.
14. M. Thornton. Coherent diffusive photon gun for generating nonclassical states / M. Thornton, A. Sakovich, A. Mikhalychev [et al.] // *Physical Review Applied*. 2019. Т. 12. №6. С. 064051.

# УНИВЕРСАЛЬНЫЙ КВАНТОВЫЙ КОМПЬЮТЕР — ВПЕРЕДИ ВРЕМЕНИ И ТЕХНОЛОГИЙ

Мнений о квантовых компьютерах (КК) в настоящее время очень много, причем часто весьма противоречивых, что связано с тем уровнем потенциальных возможностей, которыми могут обладать эти устройства, а также выходом ряда первых продуктов квантовых технологий на рынок. Данный материал — попытка краткого анализа изменений, происходящих в рассматриваемой области. 24 года назад вышел первый русскоязычный обзор по квантовой информации, опубликованный в журнале «Успехи физических наук» [1]. Это было время ожиданий быстрой реализации квантовых компьютеров и тех возможностей, которые они могут принести в связи со сделанными накануне предсказаниями. Что изменилось за прошедшие годы? Какие рубежи достигнуты?



**Сергей Килин,**  
заведующий  
Центром «Квантовая  
оптика и квантовая  
информатика»  
Института физики  
им. Б. А. Степанова  
НАН Беларуси, академик

Простая оценка показывает: объем памяти классических устройств ограничен. Используя все частицы Вселенной, то есть  $2^{200}$ , мы можем создать память ограниченного размера, в которую реально записать все 200-разрядные бинарные числа, но не более. Квантовая память такого же объема реализуется на основе всего 200 кубитов (квантовых частиц с двумя состояниями). Другой пример — химическая реакция образования из относительно простых молекул новой. Природа находит глобальный минимум энергии взаимодействующих частиц, при котором они соединяются и образуют устойчивое состояние новой молекулы, за фемтосекунды. Человек, используя современные суперкомпьютеры, не решит эту задачу за разумное время. На основе какого принципа Природа решает данную задачу — открытый вопрос, который активно стал обсуждаться в последнее время в связи с КК. Но то, что он связан с эффективным управлением системой квантовых частиц, — очевидно. В конце прошлого века было показано, что человек, научившись управлять системой кубит, сохраняя их когерентность, получит способ реализовывать экспоненциальное число возможностей  $2^K$ , выполнив  $K$  операций

над кубитами (*квантовый параллелизм*). Именно это обеспечивает основное преимущество квантовых компьютеров над традиционными, работающими с классическими носителями информации – битами. В 1994 г. американский физик Б. Шор доказал, что универсальный квантовый компьютер может факторизовать большое число  $N$  за полиномиальное время  $\log N$ . Это показало, что квантовый компьютер представит реальную угрозу информационной безопасности, построенной на различной сложности прямых и обратных задач (например, нахождения произведения простых чисел и факторизации числа, составленного из произведения простых чисел). Последовавшее через 2 года открытие Л. Гровером квантового алгоритма, ускоряющего поиск в неструктурированной базе данных с  $O(N)$  операций до  $O(\sqrt{N})$ , показало, что квантовый компьютер может быть полезным и для задач такого класса.

## КВАНТОВЫЙ ПАРАЛЛЕЛИЗМ

Квантовый параллелизм можно проиллюстрировать на примере операции записи числа в регистр из  $N$  битов в классическом и  $N$  кубитов в квантовом компьютере. Произведя  $N$  операций в классическом регистре, мы запишем только одно число длиной  $N$  бит. В квантовом случае, выполнив над каждым из кубитов, первоначально находящемся в состоянии  $|0\rangle$ , операцию Адамара  $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ , мы в результате  $N$  операций получим все  $2^N$  числа длиной  $N$  в виде суперпозиции:

$$|x\rangle = H^{\otimes N} |0\rangle_1 |0\rangle_2 \dots |0\rangle_N = 2^{-N/2} (|0\rangle + |1\rangle)_1 (|0\rangle + |1\rangle)_2 \dots (|0\rangle + |1\rangle)_N = 2^{-N/2} \sum_n |n\rangle, \text{ где } n \in (0, 2^N - 1).$$

Это центральный момент в возможности создания *полезного квантового компьютера* (табл. 1), и он связан с разработкой эффективных кодов, исправляющих ошибки, и достижением очень низкого порогового значения скорости генерации ошибок. Использование таких кодов с неизбежностью приводит к увеличению количества кубитов для исправления ошибок и сохранения унитарности для кубитов, выполняющих основные преобразования (*логических кубитов*).

Взаимодействие кубитов в УКК, то есть его *архитектура*, – принципиальный вопрос эффективности квантового компьютера. Крупномасштабный УКК должен связать воедино миллионы или даже миллиарды кубитов. Есть два подхода к построению таких устройств. Первый, подразумевающий использование *однородной архи-*

## ПРИМЕР УНИВЕРСАЛЬНОГО НАБОРА ГЕЙТОВ

Один из универсальных наборов гейтов Адамара  $\{U\} = \{X, Z, Y, H, CNOT, T\}$  представлен пятью однокубитными операциями, описываемыми тремя операторами Паули  $X, Z, Y$  оператором Адамара  $H$ , диагональным оператором  $T = \text{diag}(1, e^{i\pi/4})$  сдвига фазы на  $\pi/4$ , и одной двухкубитной операцией УСЛОВНОГО НЕТ ( $CNOT$ ).

Абстрактно *универсальный квантовый компьютер* (УКК) определяется как устройство, которое может выполнять *любую* унитарную операцию  $U$ , переводя регистр *кубитов* из одного состояния в другое в гильбертовом пространстве  $U|\psi\rangle = |\psi'\rangle$ , при этом  $U$  эффективно компилируются из конечного набора элементарных гейтов (*универсальный набор гейтов*). Именно для УКК в такой формулировке и проводились математические доказательства эффективности первых квантовых алгоритмов. Проще говоря, унитарные преобразования некоторого количества кубитов и есть квантовый компьютер. Однако любая его реализация будет сопряжена с *ошибками*, которые нарушают необходимое условие унитарности операций квантовых вычислений.

*тектуры*, где каждый кубит напрямую соединен со своими соседями, технически привлекателен, но плохо масштабируется. В зависимости

ПОЛЕЗНЫЙ КВАНТОВЫЙ КОМПЬЮТЕР	
Универсальный	Не ограничивается одним классом задач
Точный	Вероятность ошибки на выходе может быть сколь угодно малой
Масштабируемый	Требования к ресурсам не растут экспоненциально с уменьшением целевой вероятности ошибки

Таблица 1. Необходимые свойства УКК при наличии ошибок


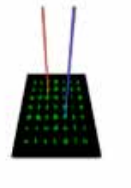
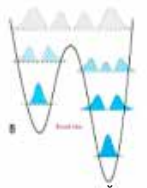


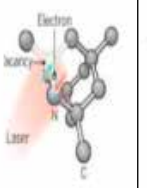
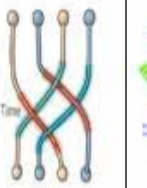
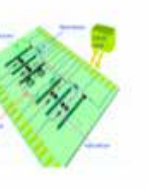














АТОМЫ		ЭЛЕКТРОНЫ СВЕРХПРОВОДНИКОВЫЕ КОНТУРЫ И УПРАВЛЯЕМЫЕ СПИНЫ					ФОТОНЫ
 ионы в ловушках	 холодные атомы	 квантовый отжиг	 сверхпроводники	 кремний	 NV-центры	 топологические	 фотоны
ПРОИЗВОДИТЕЛИ							
							

Таблица 2. Платформы, производители и исследователи (адаптировано из Olivier Ezratty (2021), arXiv:2111.15352 [quant-ph])

от платформы (ионы, сверхпроводящие устройства, фотоны, твердотельные системы и др.) может потребоваться множество управляющих лазеров или микроволн, направленных на одну физическую область, или очень большой криостат, вмещающий все кубиты. Альтернативный подход – модулярная архитектура, где квантовый компьютер формируется из множества небольших модулей (каждый состоит только из (относительно) небольшого числа кубит), которые необходимо связать вместе и выполнять межмодульные шлюзы между удаленными кубитами с помощью (А) их физического перемещения (*shuttling* для ионных платформ) или (В) *телепортации*.

Если на первых этапах количество квантовых алгоритмов практически ограничива-

лось алгоритмами Шора и Гровера и упоминанием идеи Фейнмана о симуляции квантовых процессов на квантовых компьютерах, то сейчас их количество растет [2, 3], включая в себя все новые по областям применения алгоритмы. Математически алгоритмы подразделяются на 4 группы: алгебраические и относящиеся к теории чисел (1); основанные на использовании процедуры так называемого оракула (2); симуляции и аппроксимации (3); оптимизации, численные методы и машинное обучение (4). По ускорению времени выполнения квантового алгоритма по сравнению с классическим выделяются суперполиномиальные (например, алгоритм Шора) и полиномиальные (алгоритм Гро-

вера). Для некоторых алгоритмов, например квантового отжига, ускорение неизвестно.

Наблюдается рост интереса к квантовым компьютерам для прикладных задач симуляции химических [4] и биомедицинских процессов [5], к задачам оптимизации, машинного обучения. Использование небольших квантовых специализированных вычислителей в качестве параллельных или последовательных сопроцессоров совместно с классическими суперкомпьютерами позволит добиться преимуществ в выяснении особенностей химических процессов. Так, имея всего 200 безошибочных идеальных кубитов, квантовый компьютер может разгадать биологическую фиксацию азота. Отметим, что в настоящее время процесс Гебера-Боша (получения аммиака) потребляет 2% мирового годового запаса энергии. С помощью квантового процессора IBM Q Valencia был вычислен дипольный момент молекулы LiH – одного из элементов литий-серных батарей [6].

Создание универсальных квантовых компьютеров – сложная, многоаспектная задача. Первые попытки добиться успехов в данной области показали отсутствие у исследователей необходимого опыта изоляции, управления и измерений одиночных квантовых объектов. Так, работы по флуоресценции одиночных молекул появились только в 1990-х гг., и потребовалось достаточно много времени и усилий для разработки новых методов и технологий для наблюдения и управления в лабораторных условиях не только одиночными молекулами, но и атомами, ионами, примесными центрами в твердых телах, электронами, одиночными электронными и ядерными спинами, а также фотонами с целью их использования в качестве кубитов для УКК на соответствующих платформах. Плодами этих достижений уже пользуются в многочисленных приложениях, в том числе и технологиях, которые относят к квантовым. Это квантовые сенсоры с повышенной чувствительностью, устройства для квантовой криптографии, квантовые генераторы случайных чисел и др.

Над решением задачи создания устройств квантовых вычислений работают не только в лабораториях университетов и научных центров, но и в корпорациях (Google, IBM, Intel, NEC, Honeywell и др.) (см. табл. 2, на которой представлены как производители, так и исследователи, разнесенные по соответствующим платформам используемых физических кубитов).

Однако несмотря на усилия, УКК продолжает оставаться технологическим вызовом. Причина этого – «хрупкость» квантовой информации и факт, что КК – принципиально вероятностные устройства. Растущая с увеличением числа перепутанных кубитов *декогеренция* вынуждает предпринимать специальные меры по изоляции КК и сети кубитов от внешних возмущений, а также разработке специальных квантовых кодов, исправляющих ошибки. Ответы на технологический вызов ищут физики и математики совместно с инженерами. На этом пути в качестве реперных требований для разработчиков выступают *критерии Ди Винченцо* (табл. 3). С другой стороны, физики хотели бы получить от квантовой индустрии ответы на вопросы, которые формулируются как *опросник Скотта Аэронсона* (табл. 4). Ответы на данные вопросы формируют уровень доверия к выпускаемой аппаратуре.

#### КРИТЕРИИ ДИ ВИНЧЕНЦО

- 1 Масштабируемость
- 2 Надежная инициализация кубитов
- 3 Большие времена декогеренции по сравнению с временем срабатывания отдельных гейтов
- 4 Возможность реализации универсального набора гейтов
- 5 Индивидуальное считывание состояний кубитов

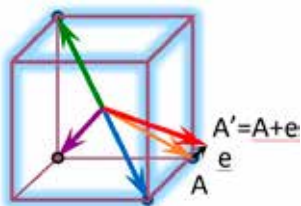
Таблица 3. Чек-лист для разработчиков КК

#### ОПРОСНИК СКОТТА АЭРОНСОНА

- 1 Сколько используется кубитов?
- 2 С какими временами когерентности?
- 3 С какой архитектурой связей?
- 4 Какова точность (фиделити) одно- и двухкубитных гейтов, а также вывода данных (измерений)?
- 5 Какова глубина схемы?
- 6 Какие ресурсы необходимы стандартным классическим алгоритмам для моделирования системы?  
В чем заключается главный недостаток используемой системы, какие ее характеристики хуже всего, и что прежде всего надо улучшить?
- 7
- 8 Что мешает компании иметь масштабируемый квантовый компьютер прямо сейчас?

Таблица 4. Что хотят узнать исследователи у производителей КК

## КЛАССИЧЕСКИЕ КОДЫ, ИСПРАВЛЯЮЩИЕ ОШИБКИ



Измененный за счет ошибки  $e$  кодовый символ  $A$  (коричневый вектор) превращается в символ  $A' = A + e$  (красный вектор), который отличается от других кодовых символов (вектора разных цветов) при условии, что минимально расстояние между ними (кодовое расстояние  $d$ ) больше  $2e$ . То есть  $d = 2t + 1$ , где  $t$  – количество исправляемых бит кода.

Возвращаясь к основной проблеме создания УКК (ошибкам при выполнении гейтов), отметим, что основная идея ее решения совпадает с методом борьбы с ошибками в обычных компьютерах (использование классических кодов, исправляющих ошибки). Путем добавления к битам данных избыточных битов растет расстояние между кодовыми символами, тем самым увеличивается их различимость даже при возникновении ошибки в одном или нескольких битах символа.

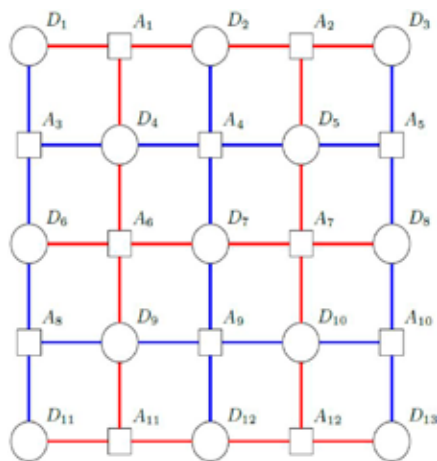
Квантовые коды, исправляющие ошибки, сложнее классических, так как они должны исправлять не только перевороты кубита ( $Z$ ), но и изменение относительной фазы кубита ( $X$ ). Как следствие, увеличивается число избыточных кубитов для обеспечения исправления ошибок логических кубитов. Например, для квантового кода Шора [9, 1, 3] с кодовым расстоянием 3, исправляющего любую ошибку в одном логическом кубите, требуется 9 физических кубитов. Разработаны различные квантовые коды: Шора, Стина, CSS (Калдербанк, Шор и Стин), стабилизационные коды, топологические (Китаев), поверхностные и др.

Однако даже их использование не избавляет от неконтролируемого распространения ошибки при выполнении логических операций (гейтов): возникнув в одном логическом кубите, она переносится при выполнении гейта на другой и так далее лавинообразно.

Существуют некоторые устойчивые к ошибкам гейты (трансверсальные). Например, трансверсальная CNOT-операция над двумя логическими кубитами в 7-кубитном коде Стина. Было показано, что некоторые подмножества универсального набора гейтов  $\{U\}$  являются трансверсальными. Однако в 2009 г. доказана no-go-теорема, согласно которой полный универсальный набор гейтов  $\{U\}$  не является трансверсальным [8]. Поэтому единственное, что «спасает»

идею универсального квантового компьютера, оставляя надежду на его реализацию, – это **квантовая пороговая теорема** (Аронов Д., Бен-Ор М.; Китаев А.; Книлл Е., Лафлам Р., Журека В.). Согласно ей, квантовый компьютер с коэффициентом физических ошибок  $p$  ниже определенного порога  $p_{th}$  может, применяя схемы квантовой коррекции ошибок, подавить коэффициент логических ошибок до сколь угодно низкого уровня. Для поверхностного кода текущие оценки устанавливают порог порядка 1%, хотя они сильно различаются и трудновычислимы из-за экспоненциальной сложности моделирования больших квантовых систем. При вероятности деполяризационной ошибки 0,1% поверхностный код потребует приблизительно 1000–10 000 физических кубитов на 1 логический кубит данных (~166 млн физиче-

## КВАНТОВЫЕ ПОВЕРХНОСТНЫЕ КОДЫ



Код  $[[13, 1, 3]]$  – наименьший поверхностный код, способный обнаруживать и исправлять ошибки за один прогон. Кружки – кубиты данных, квадраты – вспомогательные кубиты. Красными линиями обозначены гейты КОНТРОЛИРУЕМОЕ  $X$ , синим – КОНТРОЛИРУЕМОЕ  $Z$ . Архитектура – однородная: связь между соседними кубитами.



Рисунок. Прогнозируемая эволюция создания УКК как функция достигаемой пороговой вероятности ошибки гейта

## НАХОЖДЕНИЕ КВАНТОВОГО ОБЪЕМА

Протокол квантового объема определяет самую большую квадратную квантовую цепь, в которой ширина и глубина равны и которая может быть запущена на КК. Протокол состоит в многократном запуске случайной 2-кубитной схемы глубины два, с проверкой теста – наиболее вероятные строки возникают с вероятностью  $>2/3$  и с уровнем доверительного интервала более 97,725% и последующем повторе с тремя кубитами на третьей глубине, четырьмя кубитами на четвертой глубине, и т.д. до невыполнения теста.

ских кубитов для факторизации числа в 1000 бит). Исходя из данной теоремы, прогнозируется эволюция создания УКК как функция достигаемой пороговой вероятности ошибки гейта  $p_{th}$  (рисунок).

Сегодняшняя точность (фиделити) однокубитных гейтов достигает 99,9X%, двухкубитных – 99X% в зависимости от типа кубитов (платформы). Эти показатели очевидным образом демонстрируют, что пока УКК можно рассматривать в лучшем случае как отдаленную перспективу.

Так, запланированный к выпуску в 2023 г. IBM квантовый компьютер «Condor» на сверхпроводниках, содержащий 1121 физический кубит, сможет реализовывать *только* 1 логический кубит поверхностного кода с коррекцией ошибок. В ближайшей перспективе, по мере решения проблемы уменьшения вероятности ошибки гейта  $p_{th}$ , на первый план выйдут задачи создания КК *небольших масштабов* (NISQ) – квантовых ускорителей вычислений, решающих *специализированные*

задачи и работающих совместно с суперкомпьютерами [9].

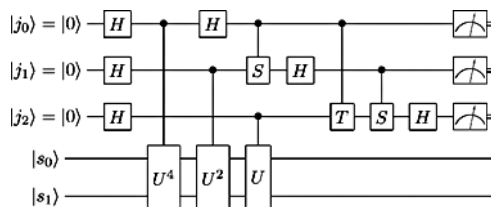
Чтобы показать имеющиеся практические преимущества в вычислениях квантовых машин (даже на уровне NISQ) по сравнению с обычными компьютерами, производителями был введен специальный термин – «квантовое превосходство». Термин, имеющий и рекламный характер, основан на том, что квантовый компьютер можно эмулировать на обычном. Однако количество кубитов для такой эмуляции ограничено памятью компьютера, а не его вычислительной мощностью. Самый большой суперкомпьютер сегодня имеет ~ 10 петабайт памяти, что позволяет имитировать операции с ~ 48 кубитами.

Любой квантовый компьютер с более чем примерно 50 кубитами невозможно смоделировать

любой квантовый компьютер с более чем примерно 50 кубитами невозможно смоделировать

## ШИРИНА И ГЛУБИНА КВАНТОВОЙ ЦЕПИ

Ширина квантовой цепи – количество используемых кубитов, глубина – максимальное число операций.



Глубина данной цепи равна 7. Регистр 3 имеет 5 гейтов, но 2-й (КОНТРОЛИРУЕМОЕ-U) не может быть выполнен, пока не будут выполнены КОНТРОЛИРУЕМЫЕ - U4 и U2, что добавляет 2 шага.

Гейт КОНТРОЛИРУЕМОЕ-T может быть реализован одновременно с H. Следовательно, глубина цепи равна 7.

## ЗАДАЧИ ДЛЯ NISQ

Квантовая оптимизация

Цифровая/аналоговая квантовая симуляция

Квантовое вычисление/симуляция промежуточного масштаба

Квантовая химия

Квантовое глубокое машинное обучение

Вариационное квантовое вычисление

Квантовые стохастические процессы, игры

Квантовые адиабатические вычисления (отжиг)

Таблица 5. Где будет полезен NISQ?

на обычном компьютере. Причем эти кубиты не обязательно должны быть корректируемыми. Можно использовать физические кубиты, которые достаточно хороши для выполнения тысяч операций раньше, чем возникает ошибка. Данная машина не масштабируется и может выполнять только относительно *короткие алгоритмы*. Тем не менее даже такой не универсальный квантовый компьютер нельзя эмулировать на обычном, поэтому он может показать квантовое превосходство и оказаться полезным для некоторых приложений (табл. 5).

Гонка за большим числом кубитов в квантовом компьютере не должна являться самоцелью. Недавно введенный еще один термин «квантовый объем» (КО) определяет величину пространства состояний, доступное конкретному КК. Увеличение числа кубитов в компьютере с высоким уровнем ошибок не увеличивает его квантовый объем. В то время как десятикратное снижение уровня ошибок при заданном числе кубитов повышает КО в 24 раза.

Задачи для КК типа NISQ, которые будут определять перспективы квантовой индустрии вычислений в обозримом будущем, весьма многообразны, и многие из них, как и сама индустрия, находятся только на пороге своего развития. Для каждой из специализированных задач будет использоваться наиболее подходящий тип платформы (кубитов). Наряду с при-

кладными элементами (оптимизация, квантовая химия, квантовая симуляция, глубокое обучение) NISQ будут применять как инструменты характеристики и калибровки создаваемых устройств, что невозможно сделать с помощью классических вычислительных средств. Примером может служить недавняя работа [10], в которой для этих целей использовался 127-кубитный процессор с высоким уровнем ошибок.

Особняком в списке задач для NISQ стоят *адиабатические квантовые вычисления* (квантовый отжиг). В отличие от квантового компьютера на основе цепей (ЦКК), адиабатические квантовые компьютеры (АКК) выполняют очень специфический вид вычислений, но чрезвычайно полезный: оптимизацию. АКК используется для поиска набора переменных, который минимизирует некоторые функции с несколькими переменными, и *считается*, что он может делать это быстрее, чем обычный компьютер, хотя математика, лежащая в основе этого, на данный момент не совсем ясна. Любое стандартное квантовое вычисление в принципе может быть выполнено с помощью АКК и наоборот, но доказательство не показывает простого пути перехода от одной системы к другой.

В зависимости от вида используемых кубитов существует несколько основных *платформ*, реализующих КК типа NISQ: сверхпроводники (IBM, Google, D-Wave); ионы в ловушках (IONQ, Honeywell); нейтральные атомы (Pascal, QuERA); фотоны (PsiQuantum, Xanadu); NV-центры в алмазе (эта платформа [11] была впервые

## АКК: ОТКРЫТЫЕ ВОПРОСЫ

Исправление ошибок. В отличие от ЦКК неизвестно, как исправлять ошибки в АКК.

Проблема энергетической щели. Суть работы АКК: при медленном изменении параметров система остается в основном состоянии, но уже в новой конфигурации. Количественная оценка «насколько медленно» обратно пропорциональна «энергетической щели между основным и первым возбужденным состоянием». Величина энергетической щели не совсем понятна теоретически и зависит от конкретной проблемы.

Щель уменьшается с увеличением размера системы. Вследствие этого время вычислений увеличивается. Таким образом, АКК ограничен размером задач, которые он может решить.

Идеальный АКК должен работать при чрезвычайно низкой температуре, чтобы тепловые флуктуации не могли перекрыть энергетическую щель. АКК, работающий при конечной температуре, коммерчески доступен сегодня (D-Wave).

предложена в работе 2001 г. [12]; продемонстрирована система из 27 ядерных спинов  $^{13}\text{C}$  [13] в окружении NV-центра); электронные и дырочные спины в полупроводниках, а также ядерные спины в молекулах и топологические КК. Один из последних обзоров платформ представлен в [14].

Если оглянуться на пройденный путь – от появления яркой идеи использования квантовых систем для ускорения вычислений до первых реализаций простейших квантовых процессоров, – ясно видно, что ученые в результате многочисленных исследований в течение четверти века (серия 17 международных конференций по квантовой оптике и квантовой информатике ICQOQI, организованных белорусскими физиками, в определенной мере отражает этот путь [15]) научились *манипулировать и измерять* различные квантовые системы на *одиночном уровне*, включая электроны, фотоны, ядерные спины молекул и примесных центров. При этом получены новые знания о функционировании таких систем и попутно предложен ряд методов прецизионных измерений и уникальных сенсоров. Столкнувшись с явлением декогеренции, ученые разработали квантовые коды, исправляющие ошибки. Осознав, что УКК составит угрозу для современной системы защиты информации, исследователи создали противодействие в виде квантовой криптографии (квантового распределения ключа) [16]. Все эти достижения подтверждают широкие возможности квантового мира, который, будучи контринтуитивным, слегка приоткрыл перед нами свои тайны. Его особенности требуют для освоения и соответствующей подготовки тех, кто будет использовать уже полученные результаты, и дальнейшего развития изысканий.

Только сейчас КК начинают входить в наш мир. Общество заинтересовано в новых ярких возможностях. Необычные квантовые технологии вряд ли оставят в стороне инвесторов «всех мастей». Идея невероятного прогресса с помощью КК в бизнесе, совмещенная с «легкой» популяризацией КК (на многих сайтах и в выступлениях описывают данную технологию как достижимую и прорывную для всех сфер), может привести к эффекту доткомов. Как слово *blockchain* в названии компании в 2016–2018 гг. провоцировало панические скупки, так и слово *quantum* будет заставлять трейдеров покупать акции. В итоге – возможный очередной финансовый пузырь.

Создание универсального КК – слишком сложная задача, чтобы увидеть план ее реа-

лизации с точными датами. На первый план выходит получение КК небольших масштабов (NISQ) – ускорителей вычислений, работающих совместно с суперкомпьютерами. Получаемые при этом результаты следует анализировать и рассматривать в контексте их важности для реализации УКК. Стоимость современного КК запредельно велика даже для очень крупных компаний. Естественной бизнес-моделью использования таких компьютеров является облачная модель. Задача создания УКК – исключительно наукоемкая и решается по законам науки. Рыночными инструментами ускорить этот процесс невозможно. Прогресс технологий на этом пути – пожалуй, самый важный результат, полученный за последние 25 лет истории освоения квантового мира. ■

#### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. С.Я. Килин. Квантовая информация // Успехи физических наук. 1999. Т. 169. №5. С. 507–527 // <https://doi.org/10.1070/PU1999v042n05ABEH000542>.
2. S. Jordan. Quantum Algorithm Zoo // <https://quantumalgorithmzoo.org/>.
3. J. Abhijith [et al]. Quantum Algorithm Implementations for Beginners // ACM Transactions on Quantum Computing. 2022. №3, 4. Article 18. P. 92 // <https://doi.org/10.1145/3517340>.
4. R. Jarrod [et al]. What the foundations of quantum computer science teach us about chemistry // J. Chem. Phys. 2021. Vol. 155. №15. P. 150901. // <https://doi.org/10.1063/5.0060367>.
5. B.A. Cordier [et al]. Biology and medicine in the landscape of quantum advantages // J. R. Soc. Interface. 2022. Vol. 19. P. 20220541. // <https://doi.org/10.1098/rsif.2022.0541>.
6. M. Reiher [et al]. Elucidating reaction mechanisms on quantum computers // PNAS. 2017. Vol. 114. №29. P. 7555. // <https://doi.org/10.1073/pnas.1619152114>.
7. J.E. Rice [et al]. Quantum computation of dominant products in lithium–sulfur batteries // J. Chem. Phys. 2021. Vol. 154. №13. P. 134115. // <https://doi.org/10.1063/5.0044068>.
8. B. Eastin, E. Knill. Restrictions on Transversal Encoded Quantum Gate Sets // Phys. Rev. Lett. 2009. Vol. 102. P. 110502. // <https://link.aps.org/doi/10.1103/PhysRevLett.102.110502>.
9. J. Preskill. Quantum computing in the NISQ era and beyond // Quantum. 2018. Vol. 2. P. 79. // <https://doi.org/10.22331/q-2018-08-06-79>.
10. Y. Kim [et al]. Evidence for the utility of quantum computing before fault tolerance // Nature. 2023. Vol. 618. P. 500. // <https://doi.org/10.1038/s41586-023-06096-3>.
11. S. Pezzagna, J. Meijer. Quantum computer based on color centers in diamond // Applied Physics Reviews. 2021. Vol. 8. №1. P. 011308. // <https://doi.org/10.1063/5.0007444>.
12. J. Wrachtrup, S.Y. Kilin, A.P. Nizovtsev. Quantum computation using the  $^{13}\text{C}$  nuclear spins nearby the single NV defect center in diamond // Оптика и Спектроскопия. 2001. Т. 91. №3. С. 460–467 // <https://doi.org/10.1134/1.1405224>.
13. M. H. Abobeih [et al]. Atomic-scale imaging of a 27-nuclear-spin cluster using a single-spin quantum sensor // Nature. 2019. Vol. 576. P. 411. // <https://doi.org/10.1038/s41586-019-1834-7>.
14. B. Cheng [et al]. Noisy intermediate-scale quantum computers // Front. Phys. 2023. Vol. 18. P. 21308. // <https://doi.org/10.1007/s11467-022-1249-z>.
15. History of ICQOQI // <https://master.basnet.by/icqoqi2019/>.
16. Килин С.Я. Квантовая криптография: идеи и практика / С.Я. Килин [и др.]; под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. – Минск, 2007.



# КВАНТОВЫЕ ТЕХНОЛОГИИ: НОВЫЕ ВОЗМОЖНОСТИ, УСПЕХИ И ВЫЗОВЫ



**Глеб Салахов,**  
младший научный  
сотрудник Российского  
квантового центра,  
магистр МФТИ



**Антон Божедаров,**  
научный сотрудник  
Российского квантового  
центра, аспирант



**Алексей Федоров,**  
руководитель научной  
группы «Квантовые  
информационные  
технологии» Российского  
квантового центра,  
Национальный  
исследовательский  
технологический  
университет «МИСиС», PhD

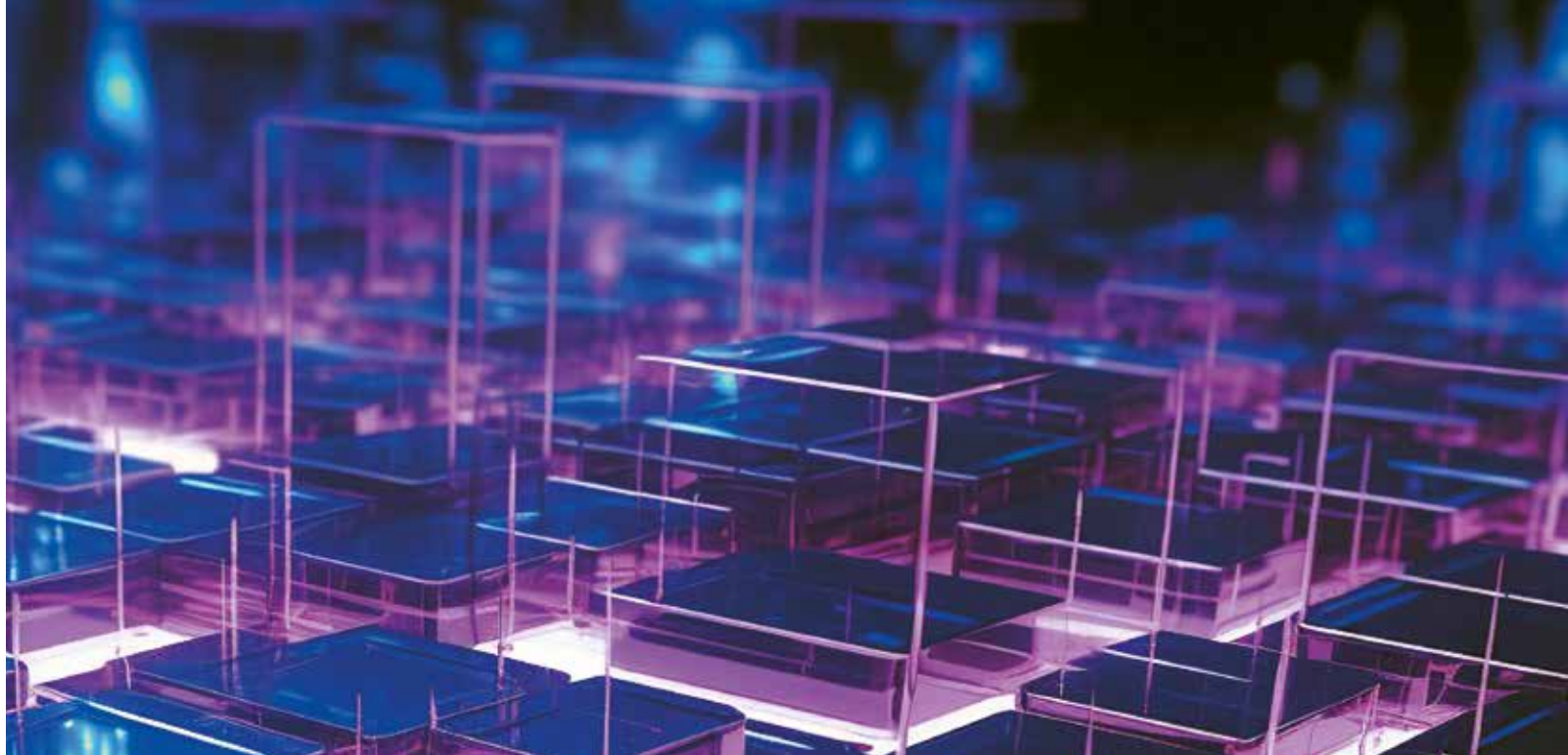
Последние десятилетия квантовые технологии, то есть совокупность методов для создания приборов и устройств, основанных на управлении индивидуальными квантовыми системами, активно развиваются и привлекают все больший интерес как со стороны исследователей, так и потенциальных потребителей.

Первая волна квантовых технологий, ознаменовавшая развитие физики в первой половине XX в., привела к созданию широко используемых устройств, наиболее важными из которых, пожалуй, являются лазеры и транзисторы. Эти изобретения вызвали скачкообразный прогресс полупроводниковой электроники, коммуникаций, Интернета, мобильной связи и многих других направлений, сформировав тем самым облик современного информационного общества.

С конца XX в. мир находится на пороге становления второй квантовой волны, кото-

рая может оказать еще большее влияние. Ее ключевое отличие от первой, в которой технологии и приборы строились на управлении коллективными квантовыми явлениями, заключается в способности управлять сложными квантовыми системами на уровне индивидуальных квантовых объектов – например, (искусственных) атомов, ионов и фотонов – и их свойств. Методы, основанные именно на таком уровне контроля, сегодня принято объединять термином «квантовые технологии», которым уделяется все большее внимание в силу возрастания их роли в вопросах национальной безопасности, а также в таких стратегически важных отраслях, как ИТ, медицина. Кроме того, квантовые технологии востребованы во всех направлениях цифровой экономики и экономики данных, в том числе, например, искусственного интеллекта (ИИ).

Квантовые технологии принято делить на 3 основных направления.



**Квантовые вычисления** – новый класс вычислительных устройств, использующий для решения задач принципы квантовой механики, такие как квантовая суперпозиция и квантовая перепутанность [1–2]. Прогнозируется, что в целом ряде случаев квантовые компьютеры обеспечат многократное ускорение в сравнении с существующими суперкомпьютерными технологиями, базирующимися на полупроводниковой электронике, – в сфере кибербезопасности, оптимизации (финансовой, производственной, логистической и т.д.), ИИ, обработки данных, при создании новых материалов и лекарств. При этом стоит отметить, что квантовые компьютеры рассматриваются не как замена традиционных вычислительных технологий, а как их усиление для решения определенных классов задач.

**Квантовые коммуникации** – технология передачи информации с помощью квантовых объектов; наиболее зрелой частью этой области

является квантовое распределение ключей (КРК) [3]. Главное преимущество квантовых коммуникаций – защищенность информации, гарантированная законами физики.

**Квантовые сенсоры и метрология** – совокупность высокоточных измерительных приборов, основанных на квантовых эффектах. Высокая степень контроля состояния отдельных микроскопических систем позволяет создавать сверхточные квантовые сенсоры с пространственной разрешающей способностью, сравнимой с размером одиночных атомов, а также высокоточные атомные часы [4].

Уже сейчас некоторые направления квантовых технологий близки к коммерческому внедрению, и многие компании вкладывают свои средства в их развитие. Значительные инвестиции были направлены такими мировыми корпорациями, как, например, Google, Microsoft, Intel и IBM. Другие – Airbus, Volkswagen

и MasterCard – с помощью этих методов уже решают прикладные задачи. Сети квантовых коммуникаций активно используются коммерческими фирмами Китая [5].

Ожидается, что нарастание применения квантовых технологий будет напоминать развитие лазерных приложений во второй половине XX в. Сначала исследовался лазер сам по себе, позже он стал инструментом для смежных научных отраслей – атомной, молекулярной и оптической физики, и далее для широкого спектра наук, в том числе химии и биологии. Текущий статус квантовых технологий схож: например, квантовые вычисления и разработанные устройства применяются для научных исследований в области квантовой физики многих тел и физики конденсированного состояния, а квантовые сенсоры – для биомедицинских исследований. В случае лазера дальнейший прогресс привел к появлению сначала специализированных

приложений, таких как голография и спектроскопия, а впоследствии и к тому, что лазер стал незаменимой технологией, которая присутствует во многих устройствах. По всей видимости, такой же путь пройдут и квантовые технологии. Например, первые специализированные приложения квантовых вычислений могут быть связаны с обучением нейронных сетей, а что касается квантовых технологий защиты информации, то распределенные ключи используются в высоконагруженных каналах связи. С учетом значительного потенциала последних спектр их применения будет расширяться.

## КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Текущую степень применения квантовых технологий для решения прикладных задач можно связать с двумя аспектами: уровнем развитости аппаратной реализации квантовых компьютеров и алгоритмами, которые разрабатываются для решения задач квантовыми методами.

Квантовые компьютеры и симуляторы – это вычислительные системы, использующие для решения задач квантовые явления, такие как квантовая суперпозиция и квантовая перепутанность. Устройства, созданные на основе квантовых вычислений, могут многократно превосходить классические компьютеры при решении задач криптоанализа, моделирования сложных (квантовых) систем, машинного обучения. На данный момент существует множество различных видов квантовых компьютеров, которые отличаются как физиче-

ской платформой, так и моделью квантовых вычислений.

Что касается последней, то ее можно разделить на 2 основные категории: универсальные и специализированные. В сравнении с классическими компьютерами, где универсальность означает возможность проводить произвольную последовательность операций над строкой бит, универсальный квантовый компьютер обеспечивает произвольное преобразование над состоянием кубитов. Примерами универсальных моделей квантовых вычислений являются цифровые (вентильные, или гейтовые) квантовые компьютеры, адиабатические квантовые компьютеры, однонаправленные, а также вариационные квантовые вычисления. Специализированные квантовые компьютеры создаются для решения конкретной задачи или определенного класса задач, например, для моделирования специальных классов квантовых систем или комбинаторной оптимизации [2].

Для реализации моделей квантовых вычислений можно использовать различные физические принципы управления квантовой информацией. Отличие заключается в том, какие системы применяются для кодирования этой информации. Например, это могут быть сверхпроводниковые кубиты, контролируемые с помощью микроволновых импульсов, или атомные кубиты, которые управляются с помощью лазеров.

Масштаб цифровых квантовых компьютеров достигает 433 кубитов, а уже концу 2023 г. прогнозируется появление систем до 1000 кубитов [6]. Нынешнее состояние

квантовых технологий называют NISQ-эрой (от англ. Noisy Intermediate-Scale Quantum), когда размеры систем еще невелики – до 1000 кубитов, и при этом процессоры крайне чувствительны в части взаимодействия с окружением. Уровень ошибок в таких системах настолько высок, что не представляется возможным выполнять их квантовую коррекцию [7] – совокупность специальных процедур по исправлению эффектов декогеренции кубитов во время проведения квантовых операций.

Вместе с тем, даже NISQ-устройства претендуют на то, чтобы решать задачи, которые находятся за пределами возможностей классических технологий. В 2019 г. первый такой эксперимент представила компания Google, используя задачи запуска случайных квантовых цепочек [8]. Однако спустя некоторое время были найдены эффективные классические методы решения данной проблемы. Серия последующих опытов показала возможность достижения квантового превосходства с количеством кубитов более 70. Схожий эксперимент был зафиксирован с использованием задачи бозонного сэмпинга. Определенной особенностью является тот факт, что как моделирование случайных цепочек, так и бозонный сэмплинг пока что не имеют ясных практических приложений. Так что пока речь может идти в лучшем случае о демонстрационном квантовом превосходстве.

В 2023 г. научная группа ИВМ заявила о способе достижения «полезного» превосходства [9]. Используя усовершенствованную технику пода-

вления ошибок, им удалось воспроизвести на 127-кубитном компьютере физическую модель Изинга, которая, в частности, описывает магнетизм постоянных магнитов. Результаты сопоставили с вычислениями на суперкомпьютере для 68 кубитов; в свою очередь, более крупную систему – на 127 кубитах – классическими вычислениями, как утверждалось, посчитать невозможно. Однако спустя короткое время были показаны эффективные классические методы моделирования подобных систем. Поэтому текущий статус развития квантовых вычислений следующий: с помощью созданных NISQ-устройств можно решать демонстрационные задачи на уровне современных суперкомпьютеров, однако вычислительного превосходства, имеющего прикладное значение, пока не найдено. Тем не менее поиски продолжаются. Параллельно с разработкой новых квантовых компьютеров создаются и алгоритмы, но многие из них демонстрируют лишь возможность решения реальных задач уменьшенных масштабов в связи с ограничением размеров текущих квантовых компьютеров. Среди примеров можно назвать следующие:

- *квантовая химия (поиск основного состояния молекулы) [10];*
- *разработка новых лекарств [11] и сборка генома [12];*
- *финансы (оптимизация финансового портфеля, кредитный скоринг, прогнозирование обвалов рынка) [13];*
- *логистика (оптимизация трафика и поиск кратчайшего пути) [14];*
- *телекоммуникации (оптимизация оптических сетей связи) [15];*

■ *нефтегазовая отрасль (определение подземных пород в местах нефтяных месторождений).*

Как уже отмечалось, на данный момент решаются задачи небольшой размерности и демонстрируется принцип работы алгоритма с возможностью масштабирования при увеличении мощности квантовых компьютеров.

Одним из возможных кандидатов на демонстрацию полезного квантового превосходства являются задачи машинного обучения. Отчасти это связано с тем, что, как предполагается, для ускорения задач машинного обучения может быть достаточно ресурса квантовых компьютеров, работающих с ошибками, тогда как в других, например в химическом моделировании, требования к ошибкам более строгие [2].

Таким образом, квантовые вычисления находятся на грани прикладной применимости – разрабатываются квантовые или гибридные алгоритмы, позволяющие на текущих размерах квантовых компьютеров решать небольшие прикладные задачи, в то время как количество кубитов в современных квантовых системах удваивается с каждым годом. Еще несколько лет назад предполагалось, что текущее состояние квантовых вычислений будет достигнуто через несколько десятков лет. Сейчас же видно, что множество исследований в этой области привело к бурному росту и достижениям, которые позволили приблизиться к полезному квантовому превосходству. Ожидается, что квантовые вычисления со временем перерастут из нишевого решения для узкого класса

проблем в технологию, способную повлиять на развитие многих секторов экономики.

## КВАНТОВЫЕ КОММУНИКАЦИИ

С развитием квантовых компьютеров возникает опасность взлома информации, передаваемой криптографическими алгоритмами на основе публичного ключа, например, одного из наиболее популярных протоколов – RSA. Криптографическая стойкость данного алгоритма сводится к предложению о сложности решения определенного класса математических задач, в данном случае – разложения числа на простые множители. Для классических компьютеров эта задача требует экспоненциально растущего времени в зависимости от размера числа. Однако квантовые компьютеры могут использовать для факторизации алгоритм Шора. На данный момент получены результаты, подтверждающие лишь принцип работы алгоритма, где на универсальных компьютерах были разложены числа 15, 21 и 35. Проведенные исследования предсказывают, что для разложения 2048-битного ключа будет необходимо 8 часов и 20 млн кубитов [16]. Таким образом, при появлении квантового компьютера возникает серьезная угроза современной архитектуре информационной безопасности.

Среди возможных решений этой проблемы – квантовые коммуникации, или, более точно, КРК, а также постквантовая криптография. Каждый из подходов обладает явными преимуществами, но и не лишен недостатков.

Квантовые коммуникации – область технологий, связанных с передачей квантовых состояний. Одним из направлений является создание защищенных каналов связи, основанных на квантовом распределении ключей (КРК) – методе защиты передаваемой информации с использованием технологий коммуникации, позволяющем гарантированно защитить данные от компрометации и несанкционированного доступа. Главное преимущество КРК – сохранность информации, обеспеченная законами физики. Сложность коммерциализации заключается в том, что большинство протоколов квантовой связи пока что обладают низкой скоростью распределения ключей, ограниченным расстоянием и требованием к инфраструктуре. Тем не менее уже сегодня в мире создаются протяженные сети КРК.

Многие страны развивают и другой подход – постквантовые алгоритмы. Это новое поколение криптографических методов, которые устойчивы к атакам, как с применением классических, так и квантовых компьютеров. Ряд государств уже ведет работу по стандартизации постквантовых алгоритмов. Также стоит отметить, что КРК и постквантовая криптография – не конкурирующие технологии, а, скорее, дополняющие друг друга при решении разных задач. Например, КРК может быть использовано для защиты высоконагруженных каналов связи между центрами обработки данных, тогда как постквантовая криптография – для защиты мобильных устройств и цифровых подписей.

Еще одной сферой квантовых коммуникаций является передача определенных

типов квантовых состояний, что необходимо для создания квантового Интернета – сети взаимосвязанных квантовых устройств [17]. Основное их применение в ближайшем будущем – создание распределенных квантовых вычислений. Объединение нескольких квантовых компьютеров в одну систему позволит увеличить мощность вычислительной системы. Квантовый интернет находится на раннем этапе своего развития – на уровне лабораторных исследований. В 2022 г. была продемонстрирована перепутанность между двумя атомами, разделенными 33-километровым оптическим волокном – следующий шаг к квантовому Интернету и распределенным квантовым вычислениям. Эти изыскания представляют собой развитие идеи передачи перепутанности для практически важных задач квантовых технологий.

Квантовые коммуникации – область квантовых технологий, которая больше всего готова к реальным квантовым приложениям. Сети квантовых коммуникаций уже сейчас используются компаниями (например, в Китае), а планы по внедрению и увеличению таких сетей есть у многих крупных стран мира. Более того, надвигающаяся угроза взлома наиболее популярных протоколов передачи информации квантовым компьютером повышает интерес к развитию квантовых коммуникаций.

## КВАНТОВЫЕ СЕНСОРЫ И МЕТРОЛОГИЯ

Квантовые сенсоры – высокоточные измерительные приборы, основанные на кванто-

вых эффектах. Ожидается, что они будут иметь высокое пространственное и временное разрешение, что позволит повысить точность измерений в сравнении с существующими классическими сенсорами, а использование свойств суперпозиции, перепутанности и сжатия квантовых состояний, в свою очередь, обеспечит в перспективе максимально возможную чувствительность измерения за счет преодоления стандартного квантового предела.

На данный момент квантовые сенсоры обладают ограниченным спектром использования, но количество возможных областей их приложения растет с каждым днем.

Яркий тому пример – атомные часы [18]. Технология существует уже несколько десятков лет, и одним из примеров ее удачного и востребованного применения считается система глобального позиционирования (GPS). Квантовые часы представляют собой хронометр, который умеет проводить самокалибровку благодаря собственным колебаниям, связанным с процессами на уровне атомов и молекул.

Также активно развиваются градиометры и гравиметры [19]. Существуют как коммерческие, так и лабораторные датчики. Основной плюс квантовых датчиков – их повышенная чувствительность. Подобные устройства нашли применение в георазведке, археологии, почвоведении, гидрологии и картировании. Некоторые исследования показывают, что квантовые датчики на холодных атомах в 1,5–2 раза эффективнее классических для решения задач по определению небольших закопанных объектов.

Магнитометры – датчики, способные измерять различные характеристики магнитного поля [20]. Существует несколько их физических реализаций: от датчиков на центрах окраски алмазов до приборов, называемых СКВИД, и специальных материалов (например, пленок феррит-граната). Благодаря повышенной точности они востребованы в широком спектре различных отраслей, среди которых можно выделить геологию, археологию, сейсмологию, навигацию, дефектоскопию, биологию и медицину.

Несмотря на вариативность возможного применения, квантовые сенсоры обладают своими минусами, проблемы с которыми сейчас пытаются решить ученые: например, ограничение количества шума для повышения точности технологий. Многие компании сталкиваются с потребностью в больших камерах охлаждения для использования сенсоров, что является одной из проблем при коммер-

циализации. На текущем этапе в силу повышенной точности квантовых сенсоров их используют как инструмент для исследований в различных отраслях, не связанных с квантовыми технологиями. Постепенно с уменьшением их размеров такие приборы получают более широкое коммерческое применение.

Развитие квантовых технологий достигло этапа, когда создаются государственные программы поддержки и дорожные карты квантовых технологий, все больше средств вкладывается со стороны частного бизнеса. Однако у каждого из направлений – вычислений, коммуникаций и сенсорики – имеются определенные ограничения, которые нужно преодолеть, чтобы перейти от лабораторных исследований к решению практических задач на индустриальном уровне.

Если ранее классические компьютеры и Интернет считались нишевыми технологи-

ями, то сейчас они развились за пределы ожиданий, изменив весь технологический и экономический ландшафт. Это произошло за счет увеличения вычислительных мощностей и, фактически, качества технологии, а также повышения их доступности для массового пользователя. Сейчас сфера квантовых технологий развивается подобным образом, научные институты, государства и крупные компании стараются создавать более продвинутые версии квантовых компьютеров, устройств квантовых коммуникаций и сенсоров, пока параллельно ведется разработка масштабируемых квантовых алгоритмов и других подходов с реальной промышленной эксплуатацией. Поэтому можно ожидать демонстрации первых примеров полезного применения квантовых технологий, и в первую очередь квантовых вычислений, уже в ближайшие годы. ■

#### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Килин С.Я. Квантовая информация // Успехи физических наук. 1999. №5. Т. 169. С. 507–527.
2. Quantum computing at the quantum advantage threshold: a down-to-business review. Fedorov A. K. [and al.] 2022 г. // <https://doi.org/10.48550/arXiv.2203.17181>.
3. Килин С.Я. [и др.]. Квантовая криптография: идея и практика. – Минск, 2007.
4. Хабарова К.Ю., Заливако И.В., Колачевский Н.Н. Методы квантовой логики в ионных стандартах частоты, квантовых вычислителях и современной спектроскопии // Успехи физических наук. 2022. №12. Т. 192. С. 1305–1312.
5. Chen Yu-Ao [and al.]. An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. 2021. №7841. Т. 589. P. 214–219.
6. Choi Charles Q. IBM's Quantum Leap: The Company Will Take Quantum Tech Past the 1,000-Qubit Mark in 2023 // IEEE Spectrum. 2023. №1. Т. 60. P. 46–47.
7. Lau J., Wei Zhong [and al.]. NISQ computing: where are we and where do we go? // AAPP Bulletin. 2022. №1. Т. 32. P. 27.
8. Arute F. [and al.]. Quantum supremacy using a programmable superconducting processor. // Nature. 2019. №574. Т. 574. P. 505–510.
9. Kim Y., Eddins A., Anand S. Evidence for the utility of quantum computing before fault tolerance // Nature. 2023. №618. P. 500–505.
10. Sapova M.D., Fedorov A.K. Variational quantum eigensolver techniques for simulating carbon monoxide oxidation // Communications Physics. 2022. №1. Т. 5. P. 199.
11. Gircha A.I. [and al.]. Hybrid quantum-classical machine learning for generative chemistry and drug design. // Scientific Reports. 2023. №1. Т. 13. P. 8250.
12. Boev A.S. Genome assembly using quantum and quantum-inspired annealing // Scientific Reports. 2021. №11. Article number: 13183.
13. Mugel S. [and al.]. Dynamic portfolio optimization with real datasets using quantum processors and quantum-inspired tensor networks // Physical Review Research 4.1. 2022. 013006.
14. Neukart F. [and al.]. Traffic flow optimization using a quantum annealer // Frontiers in ICT 4. 2017. №29.
15. Boev A.S. [and al.]. Quantum-inspired optimization for wavelength assignment // Frontiers in Physics. 2023. №10. P. 1092065.
16. Gidney C., Eker M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits (2019) // Quantum. 2021. Т. 5. P. 433.
17. Gyongyosi L., Imre S. Advances in the quantum internet // Communications of the ACM. 2022. Т. 65(8). P. 52–63.
18. Ludlow A.D. [and al.]. Optical atomic clocks // Reviews of Modern Physics. 2015. Т. 87(2). P. 637.
19. Rademacher M., Millen J., Li Y.L. Quantum sensing with nanoparticles for gravimetry: when bigger is better // Advanced Optical Technologies. 2020. №5. Т. 9. P. 227–239.
20. Hrvoic I. [and al.]. Brief review of quantum magnetometers // GEM Systems Technical Papers. 2005.



# КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: В ПОИСКАХ КОГЕРЕНТНОСТИ

## КВАНТОВЫЙ ЭКСПРЕСС УЖЕ В ПУТИ: ГЛОБАЛЬНЫЕ ИНВЕСТИЦИИ



**Илья Родионов,**  
директор НОЦ «Функциональные  
Микро/Наносистемы» (ФМНС)  
Московского государственного  
технического университета  
им. Н.Э. Баумана, кандидат  
технических наук, доцент



**Ольга Ефремова,**  
заместитель директора  
НОЦ ФМНС Московского  
государственного  
технического университета  
им. Н.Э. Баумана

Мир технологий находится на пороге эпохи глобальных преобразований, и квантовые вычисления становятся драйвером этой революции. Принимая во внимание невероятные возможности, которые может обеспечить вычислитель на новых физических принципах, правительства ведущих стран выносят развитие данного направления на фронт научной и технологической повестки, инвестируя в него значительные средства.

Лидером по объему вложений в квантовые технологии является Китай: порядка 15,3 млрд долл. в общей сложности. Второе место занимает Европейский союз: в формате различных квантовых консорциумов и объединений в «кванты» инвестировано 8,4 млрд долл. Третье место – за Сое-

По оценкам аналитического агентства McKinsey&Company, общий объем финансирования государственных программ по квантовым вычислениям в мире с 2015 по 2022 г. превысил 22 млрд долл.

диненными Штатами Америки, правительство которых потратило на отрасль более 3,7 млрд долл. Впрочем, относительное отставание США не должно вводить в заблуждение: мощнейшие потоки средств в квантовые технологии остаются неанонсированными. Более того, инвестиции в уникальные направления осуществляют крупнейшие бигтехи: IBM, Google, Amazon, Honeywell, что, в свою очередь, обеспечивает лидерство американских компаний в развитии той или иной технологической платформы (рис. 1).

Согласно аналитическим данным McKinsey&Company, крупный мировой бизнес в 2022 г. вложил в общей сложности 2,35 млрд долл. в стартапы в этой области, включая компании, занимающиеся квантовыми вычислениями, коммуникациями и сенсорикой. Подавляющая доля – 82% от общего объема средств – пришлось на разработчиков аппаратного и программного ПО (рис. 2).

Максимальные инвестиции со стороны мировых бигтехов получили разработчики сверхпроводниковых схем (2 млрд долл.). Инвестиции в стартапы относительно сопоставимы при лидерстве фотонной (1,491 млрд долл.), сверхпроводниковой (1,486 млрд долл.) и ионной платформ (порядка 1,454 млрд долл.).

### Драйвер нового технологического уклада

Идея квантовых вычислений была предложена независимо советским физиком Юрием Маниным и американским ученым Ричардом Фейнманом в начале 1980-х гг. С этого момента для создания практически полезного квантового компьютера мировыми группами проделана колоссальная работа. Почти 40 лет спустя в активе разработчиков появились уникальные технологии процессоров на различных физических платформах, с использованием которых уже было продемонстрировано квантовое превосходство на сверхпроводниковых процессорах Google Sycamore и Zuchongzhi (Китайская академия наук), а также фотонном Xanadu, код коррекции ошибок (Китайская академия наук, Google), разработка и тестирование квантовых алгоритмов и программного обеспечения для решения различных практических задач: от глубокого хеджирования для оценки рисков до расчета химических и физических свойств материалов и т.д. 2022 г. ознаменовался рядом значительных событий в индустрии квантовых вычислений:

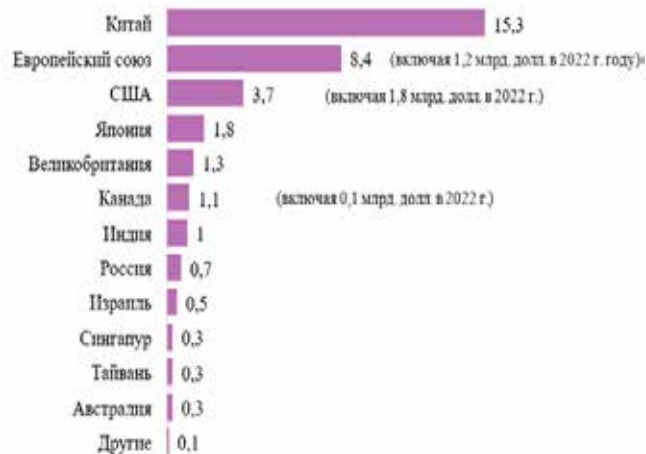


Рис. 1. Общий объем государственных инвестиций в квантовые технологии, млрд долл. (Quantum Technology Monitor 2022, McKinsey&Company)

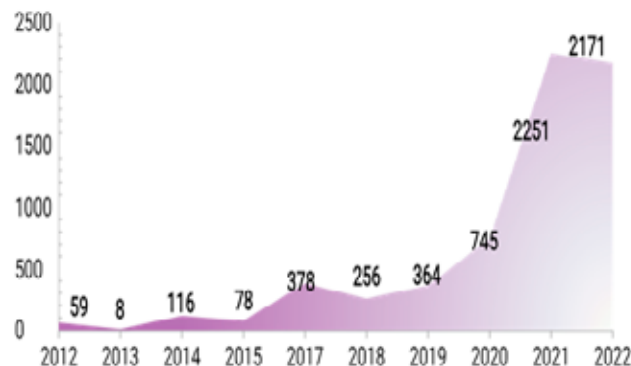


Рис. 2. Рост частных инвестиций в квантовые технологии, млн долл.

- Нобелевская премия по физике 2022 г. присуждена ученым-исследователям квантовой перепутанности Алену Аспе, Джону Клаузеру и Антону Цайлингеру;
- IBM представила процессор Osprey из 433 кубитов и обновила собственную дорожную карту развития квантовых вычислений. Цель – создание процессора на 4000+ кубитов к 2025 г.;
- Xanadu (стартап из Канады) продемонстрировал квантовое превосходство при решении задачи выборки гауссовых бозонов (проблема выборки распределения вероятностей) на фотонном квантовом компьютере Borealis;
- Университет науки и технологий Китая и Google продемонстрировали код коррекции ошибок на сверхпроводниковых кубитах. Для решения задачи американцы использовали 49 физических кубитов;

- *Стремительное развитие системного и прикладного квантового ПО. Ряд крупных игроков – от диттех-гиганта IBM до стартапа QC Ware – предлагают уникальные решения для бизнес-партнеров с целью реализации исследований, которые невозможно или слишком дорого (и долго) проводить с помощью современных технологий.*

Именно на сверхпроводниковых процессорах Google и Университет науки и технологий Китая продемонстрировали код коррекции ошибок, а IBM – уникальный своей технологией сборки 127-кубитный Condor (433 кубита уже на очереди и очень скоро «оживут», несмотря на сомнения скептиков). При этом технологии IBM постепенно распространяются по миру: сегодня IBM Quantum Network включает более 60 организаций по всей Европе, пользующихся облачным доступом к квантовому оборудованию и ПО американского гиганта. Более того, IBM Q System 1 установлен в Институте Фраунгофера в Мюнхене и скоро появится в Токийском университете.

С учетом текущих темпов развития индустрии и потока инвестиций в ключевых разработчиков, в число отраслей экономики, которые уже в течение ближайшего десятилетия ощутят максимальные изменения, связанные с квантовыми вычислениями, входят автомобилестроение, химическая промышленность, финансовые услуги и биотехнологии. Прогнозируемый экспертами объем вложений в эти направления превысит 1,3 трл долл. к 2035 г.

## Как достигнуть квантового превосходства: сверхпроводниковые схемы

Сверхпроводниковые кубиты – одна из наиболее продвинутых и перспективных платформ реализации квантовых процессоров. Все ведущие мировые державы (США, Китай, Япония и др.) и хайтек-гиганты выбрали именно сверхпроводниковую элементную базу, вложив в ее развитие за последние 10 лет несколько миллиардов долларов.

Главными преимуществами сверхпроводниковых кубитов являются возможность их изготовления на базе технологических процессов, сходных с современными процессами микроэлектроники, а также

фактор использования классической управляющей электроники для их измерения и контроля, что существенно упрощает дальнейшее масштабирование сверхпроводниковых систем. Тем не менее сверхпроводниковые кубиты чрезвычайно чувствительны к дефектам в материалах и шумам различной природы, и это приводит к повышенным требованиям к техно-

логическим операциям их производства, точности и скорости управления и контроля, методикам измерения.

Для построения практически полезной квантовой вычислительной системы потребуются большое количество кубитов: от сотен до миллионов, по некоторым оценкам. Однако точность выполнения квантового алгоритма ограничена точностью двухкубитных логических операций, а с увеличением количества кубитов ошибка вычисления растет экспоненциально. При таких условиях квантовый процессор с боль-

шим количеством кубитов будет практически бесполезен. Таким образом, по мнению большинства ведущих мировых экспертов, для создания эффективных вычислительных систем необходимо в первую очередь обеспечить высокую точность двухкубитных квантовых операций, а затем уже масштабировать систему.

На данный момент в мире достигнут существенный прогресс в разработке сверхпроводниковых квантовых процессоров. Так, компанией Google в 2019 г. было продемонстрировано квантовое превосходство, а в 2022 г. реализован одномерный алгоритм коррекции ошибок на 54-кубитном процессоре Sycamore с точностью операций более 99%. Компания IBM предоставила облачный доступ к своему 127-кубитному процессору Eagle со средней точностью операций более 98%.

Квантовый бит (кубит) – элементарная единица информации в квантовых процессорах. В отличие от классического, он может находиться не только в состояниях 0 и 1, но и в их произвольной суперпозиции, что обуславливает экспоненциальный рост мощности вычислений с увеличением количества кубитов.

Основной характеристикой кубитов является время когерентности, в течение которого в искусственном атоме может храниться записанная информация.

В России с каждым годом наращиваются технологические компетенции в области квантовых вычислений. Платформа консолидации научного сообщества и индустрии, глубокий анализ мировых трендов и формирование фундамента развития данных технологий были обеспечены Фондом перспективных исследований (ФПИ). С 2013 по 2020 г. Фонд успешно реализовал передовые проекты в этой сфере на различных платформах.

Основы создания российских сверхпроводниковых квантовых процессоров были заложены проектом ФПИ, реализованным широким консорциумом исполнителей в 2016–2019 гг.

Квантовый процессор – система из кубитов, связанных между собой. Вычислительные алгоритмы, реализуемые квантовыми процессорами, состоят из однокубитных (1Q) и двухкубитных (2Q) логических операций, которые формируют необходимый и достаточный набор инструментов для построения алгоритмов практически любой сложности.

Вследствие неидеальности физических кубитов процесс выполнения логических операций обладает конечным уровнем точности, или «шумом».

В рамках проекта – благодаря разработкам объединенной команды под руководством ФГУП «ВНИИА им. Н.Л. Духова» – был совершен технологический прорыв: получена технология квантовых сверхпроводниковых интеграль-

ных схем, позволившая вывести качество российских кубитов на уровень ведущих мировых лабораторий, а также созданы первые образцы квантовых процессоров и симуляторов.

## ЭЛЕМЕНТНАЯ БАЗА СВЕРХПРОВОДНИКОВЫХ КВАНТОВЫХ ПРОЦЕССОРОВ

Чип сверхпроводникового квантового процессора включает ряд микро- и наноразмерных элементов, для моделирования и изготовления которых требуются высокие компетенции команд теоретиков, технологов, инженеров и экспериментаторов (рис. 3).

Джозефсоновские переходы – самая миниатюрная, но и самая важная часть сверхпроводниковой квантовой схемы. Именно этот элемент привносит нелинейность в квантовый осциллятор и позволяет выделить два нижних энергетических уровня, которые используются для создания в кубитах логических уровней  $|0\rangle$  и  $|1\rangle$ . Конструктивно джозефсоновский переход представляет собой два сверхпроводящих электрода нанометровых масштабов, разделенных тонким слоем диэлектрика толщиной всего 0,5–3 нм. Чаще всего сверхпроводниковые схемы изготавливаются из сверхпроводящего алюминия – в таком случае «сэндвич» джозефсоновского перехода состоит из слоев Al-AlO<sub>x</sub>-Al.

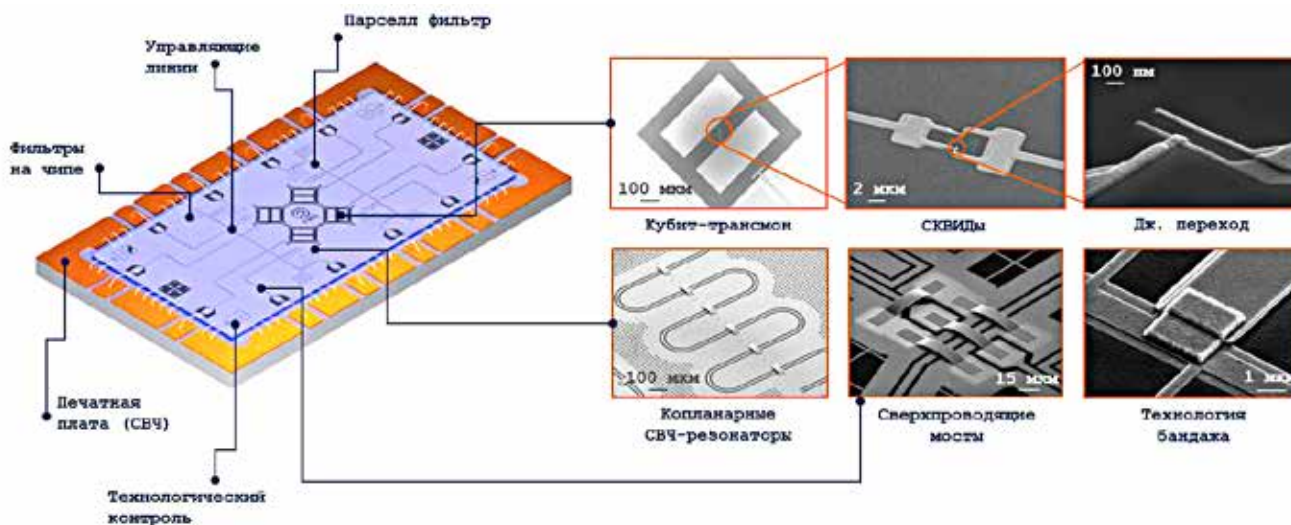


Рис. 3. Сверхпроводниковый процессор: модель и СЭМ-изображения элементов (ФГУП «ВНИИА им. Н.Л. Духова»)

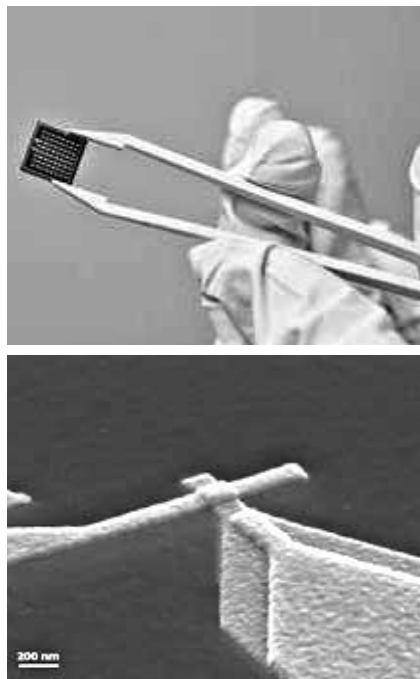


Рис. 4. Чип с массивом джозефсоновских переходов (ФГУП «ВНИИА им. Н.Л. Духова»)

Вследствие малых размеров джозефсоновского перехода и высоких требований, предъявляемых к точности воспроизведения размеров переходов и качеству электродов, отработка технологии изготовления является нетривиальной задачей. Командой ФГУП «ВНИИА им. Н.Л. Духова» разработан серийный процесс, позволяющий создавать все существующие и перспективные типы сверхпроводниковых кубитов с джозефсоновскими переходами размером от 80 до 1000 нм и широким диапазоном значений критического тока от 7 нА до 8,5 мкА.

При этом воспроизводятся электрические и геометрические параметры джозефсоновских переходов с разбросом значений менее 5% по чипу, что соответствует лучшим мировым аналогам (рис. 4). Достигнутые диапазоны значений ключевых параметров позволили обеспечить гибкость проектирования



Рис. 5. Квантовый чип с высокодобротными СВЧ-резонаторами

многокубитных квантовых схем, а также возможность создания криогенных параметрических усилителей с квантовым уровнем шумов.

## Копланарные СВЧ-резонаторы

Взаимодействие между сверхпроводниковыми кубитами и схемой считывания информации обычно построено на базе сверхпроводниковых высокочастотных копланарных СВЧ-резонаторов с частотой 0,5–8 ГГц. Чтобы информация, записанная в кубите, не «утекла» в измерительную схему, применяют методику так называемого дисперсионного считывания. Его суть заключается в измерении частоты резонатора, которая зависит от состояния кубита ( $|0\rangle$  или  $|1\rangle$ ). Сдвиг частоты копланарного резонатора при изменении состояния кубита называется дисперсионным (рис. 5).

Ключевым параметром копланарных резонаторов для квантовых приложений является их добротность в однофотонном режиме, характеризующем в том числе и качество изготовления многокубитных квантовых сверхпроводниковых интегральных схем. Нашими специалистами разработана технология изготовления сверхпроводниковых микроволновых копланарных резонаторов с показателем более 4 млн, что превышает все опубликованные ранее значения. Для достижения столь высоких результатов используется собственная технология осаждения сверхпроводящего эпитаксиального SCULL-алюминия (патенты РФ и США) и серии специальных микротехнологий травления.

Стоит отметить, что универсальные квантовые вычисления и связь на больших расстояниях требуют многокубитной памяти, которая предназначена для хранения перепутанного квантового состояния нескольких кубитов и его возвращения по требованию.

Разработка квантовой памяти на основе сверхпроводниковых копланарных резонаторов во ФГУП «ВНИИА им. Н.Л. Духова» ведется совместно с учеными из казанского университета КНИТУ КАИ. В результате совместных исследований создано устройство интегральной сверхпроводниковой квантовой памяти, которое позволяет сохранять одиночные фотоны с эффективностью  $60\pm 3\%$ , а 2–3 фотона – с эффективностью  $73\pm 3\%$ , что в 10 раз превышает известные результаты.

Однако предложенная схема может быть изменена для хранения по требованию, над чем сейчас активно работают ученые кооперации. Достигнутые результаты могут изменить

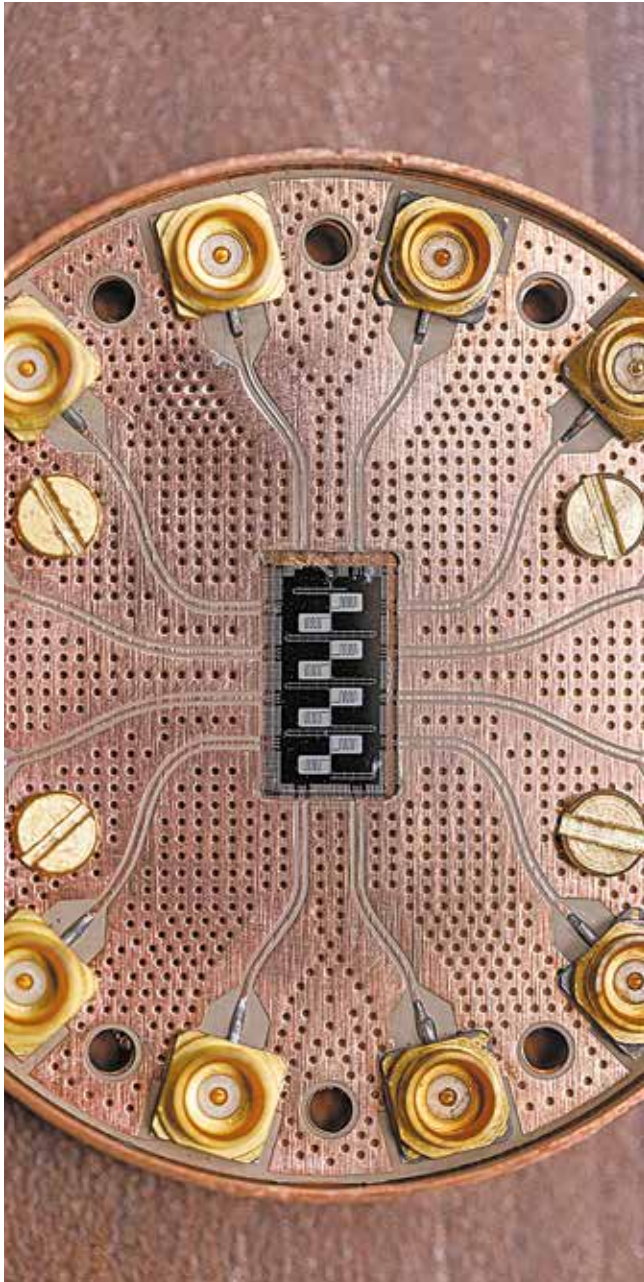


Рис. 6. Чип квантовой памяти в оснастке для проведения экспериментов (ФГУП «ВНИИА им. Н.Л. Духова»)

подходы к построению архитектуры практически полезных квантовых процессоров (рис. 6).

### **Криогенный параметрический усилитель**

Создать практически полезный квантовый компьютер невозможно без криогенных параметрических усилителей с квантовым уровнем шумов. Устройство позволяет увеличить соотношение «сигнал – шум» при измере-

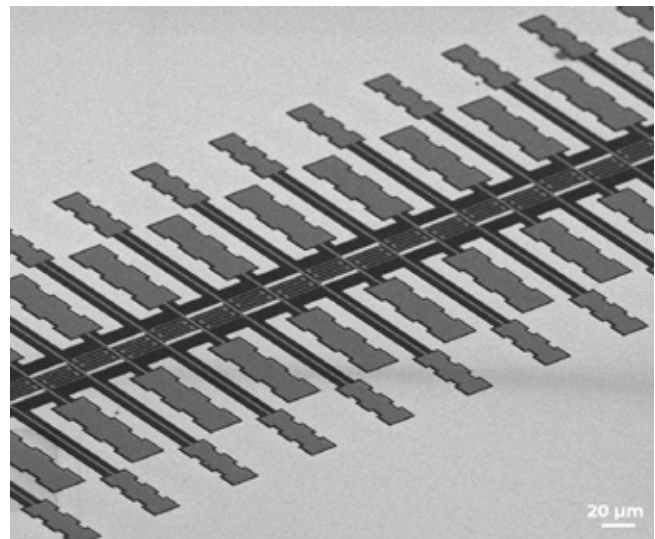
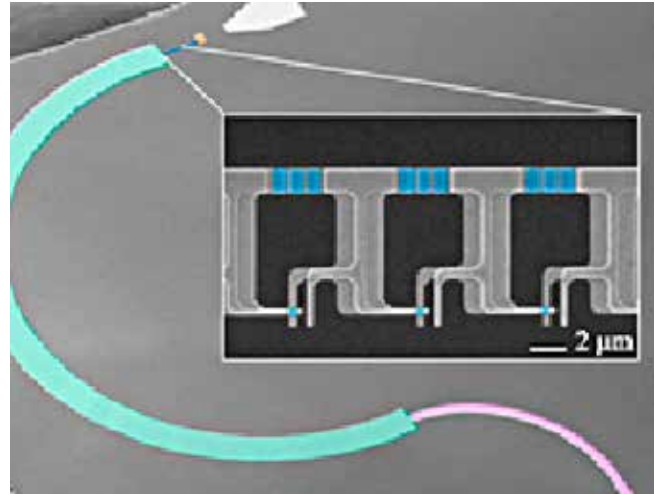


Рис. 7. Чип широкополосного квантового усилителя (ФГУП «ВНИИА им. Н.Л. Духова»)

ниях и повысить точность считывания состояния кубитов. Уникальность такого усилителя заключается в малом привносимом шуме в сигнал, получаемый от квантовой схемы. Основная сложность при его изготовлении – формирование массива джозефсоновских переходов, количество которых может достигать нескольких тысяч с одинаковыми характеристиками.

ФГУП «ВНИИА им. Н.Л. Духова» разработана технология и реализованы широкополосные джозефсоновские параметрические усилители, позволяющие, в отличие от узкополосных устройств, считывать сигналы с квантовой схемы, содержащей множество кубитов. Именно такой класс устройств сегодня используется ведущими мировыми группами, включая IBM, Google и др.

Рис. 8. Двухкубитный квантовый процессор для демонстрации квантового алгоритма Гровера (МИСиС, ФГУП «ВНИИА им. Н.Л. Духова»)

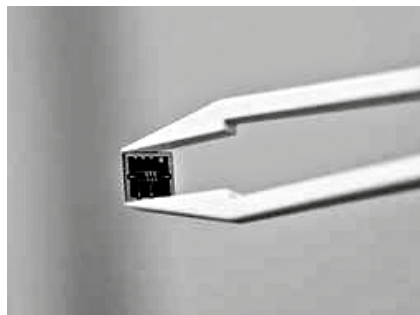
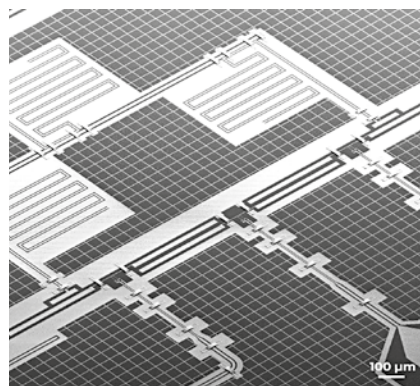


Рис. 9. Пятикубитный квантовый симулятор (МИСиС, ФГУП «ВНИИА им. Н.Л. Духова»)



Рис. 10. Квантовая схема на базе трех кубитов-флакониумов (МИСиС, ФГУП «ВНИИА им. Н.Л. Духова»)



С помощью математического моделирования создана конструкция широкополосного усилителя, а также разработаны методики его калибровки. Проведены экспериментальные криогенные исследования, в рамках которых продемонстрирована ширина полосы усиления выше 600 МГц, усиление более 17 дБ и уровень шума, близкий к квантовому пределу (рис. 7).


## ИЗ ЧИСТОЙ КОМНАТЫ В ЭКСПЕРИМЕНТАЛЬНОЕ ПОЛЕ: РОССИЙСКИЕ КВАНТОВЫЕ ПРОЦЕССОРЫ

Технологические успехи ФГУП «ВНИИА» в производстве отдельных элементов сверхпроводниковых квантовых процессоров и формирование экспериментальной базы

позволили российским командам создать ряд первых отечественных квантовых процессоров и, что важно, выполнить на них отдельные однокубитные и двухкубитные операции, а также квантовые алгоритмы. На базе разработанных технологий изготовлен первый российский двухкубитный квантовый процессор, на котором в 2019 г. был продемонстрирован полный набор квантовых логических операций и реализован квантовый алгоритм Гровера (решение задачи перебора) (рис. 8). С использованием этого процессора экспериментально показаны однокубитные и двухкубитные логические вентили с точностью операций от 80 до 99%.

Кроме того, активное развитие получили квантовые симуляторы на основе цепочек из 5, 11 и 25 кубитов для изучения фундаментальных явлений динамики коллективных состояний. Пятикубитный квантовый симулятор продемонстрировал эффективность для решения специфических физических задач, просчитав поведение фотонов в модели Бозе-Хаббарда быстрее 138-ядерного вычислительного кластера (рис. 9).

Флакониумы – один из прорывных типов сверхпроводниковых кубитов в мире, которые могут полностью вытеснить квантовую элементную базу (кубиты-трансоны), используемую сегодня технологическими лидерами (Google, IBM, Intel). Командой ФГУП «ВНИИА» совместно с МИСиС разработана технология производства сверхпроводниковых интегральных схем на базе кубитов-флакониумов, на которых впервые реализованы двухкубитные логические операции с рекордной точностью до 99,23% (рис. 10).

Сверхпроводниковые квантовые схемы заслуженно занимают одну из лидирующих позиций среди платформ для реализации вычислений нового поколения. Российское научное общество отстает от мировых лидеров в данном направлении, однако быстрое наращивание технологических компетенций позволяет делать оптимистичные прогнозы. Приоритетные задачи ближайших лет: повышение точности однокубитных и двухкубитных операций, масштабирование сверхпроводниковых квантовых схем, развитие аппаратного и программного обеспечения и организация облачного доступа к российским квантовым процессорам на различных платформах. 





# КВАНТОВЫЕ СЕНСОРЫ



**Сергей Кулик,**  
научный руководитель  
Центра квантовых  
технологий физического  
факультета МГУ  
имени М. В. Ломоносова,  
доктор физико-  
математических наук,  
профессор

Бурное развитие новой области знаний, получившей в последнее десятилетие название квантовой обработки информации, привело к появлению сквозной технологии – «Квантовые технологии», передовые научно-технические решения, создающие высокотехнологичные продукты и сервисы и оказывающие значительное влияние на рост экономики и формирование новых рынков. К таким относятся те технологии, которые одновременно охватывают несколько трендов или отраслей. Традиционно эта технология делится на три субтехнологии: *квантовые вычисления, квантовые коммуникации и квантовые сенсоры*, которые тесно связаны между собой. Прежде всего их связь определяется общими законами квантовой физики, а также возможностями, которые в последнее время получили экспериментаторы в виде обширного инструментария – единого для трех субтехнологий. Именно эти возможности доступа к индивидуальным квантовым объектам (атомам, ионам, молекулам, фотонам, базовым сверхпроводниковым элементам) стали отличительной особенностью так называемой *второй квантовой революции*.

Существенной чертой квантовых технологий является значительная доля фундаментальных исследований в цепочке продвижения по уровню технологической готовности создаваемых продуктов; в целом он пока невысок. Такая цепочка включает следующие этапы: фундаментальная научно-исследовательская работа – прикладная НИР – опытно-конструкторская работа – технология – продукт. Однако ряд разработок уже сегодня доведен до конкретных изделий, которые вышли на рынок. Речь идет об инновациях в области квантовой коммуникации и квантовых сенсорах.

**Под квантовой сенсорикой понимается создание измерительных устройств, основанных на квантовых эффектах.** Предполагается, что квантовые сенсоры будут иметь параметры, намного превышающие имеющиеся у классических аналогов. К числу таких характеристик относятся не только чувствительность (в смысле минимального значения регистрируемого сигнала) и пространственное/временное разрешение, но и рабочий диапазон измеряемых значений, время отклика или анализа, относительная воспроизводимость (например, частоты в стандартах времени), энергопотребление, габариты, сложность обслуживания, срок службы, стоимость производства и эксплуатации и т.д.

К основным инструментам, позволяющим реализовать такие характеристики, относят:

- фундаментальные наработки в области взаимодействия света и вещества, выполненные во второй половине XX – начале XXI вв.;
- специфические свойства квантовых состояний, такие как суперпозиции, перепутывание;
- особенности квантовых систем, проявляющиеся при квантовых измерениях.

Именно использование свойств суперпозиции, перепутывания обеспечит в перспективе максимально возможную чувствительность измерения за счет преодоления стандартного квантового предела (под ним понимается предел точности измерений, к которому подошли классические методы, не использующие свойства суперпозиции, перепутанности или сжатия; например, для фотонов стандартным квантовым пределом является предел «дробового шума»). Эти свойства лежат в основе ряда разрабатываемых сенсоров.

## СУПЕРПОЗИЦИИ (квантовая когерентность)

Волновые функции квантовых объектов представляют собой линейную комбинацию (суперпозицию) базисных состояний  $|0\rangle$  и  $|1\rangle$  с амплитудами  $c_1$  и  $c_2$ :

$$|\Psi\rangle = c_1|0\rangle + c_2|1\rangle, |c_1|^2 + |c_2|^2 = 1.$$

## ПЕРЕПУТЫВАНИЕ

$$|\Psi_{1,2}\rangle = \frac{1}{\sqrt{2}}\{|0_1\rangle|1_2\rangle + |1_1\rangle|0_2\rangle\}$$

Квантовое состояние составной системы «1, 2» определено лучше, чем состояния подсистем «1» и «2»; для широкого класса двухкомпонентных квантовых систем состояние составной системы является чистым и описывается волновой функцией, в то время как состояния подсистем оказываются смешанными и описываются

матрицей плотности. Соответственно, энтропия совместного состояния оказывается равной нулю, в то время как энтропия подсистем максимальна.

## ИЗМЕРЕНИЕ

Измерение квантовой системы приводит к классическим вероятностным исходам (постулат Борна).

Если над квантовой системой, находящейся в состоянии  $|\Psi\rangle$ , производится измерение, которое описывается оператором  $M_m$ , то вероятности исходов различных измерений определяются по правилу  $p_m = \langle\Psi|E_m|\Psi\rangle$ , где введены положительно определенные операторы – они известны в квантовой механике как POVM-элементы (positive operator valued measure), связанные с измерениями:

$$E_m = M_m^\dagger M_m, \sum_m E_m = I.$$

Сегодня известно большое количество сенсоров различных физических величин, начиная от магнитных и электрических полей, заканчивая датчиками времени, частоты, вращения, температуры и давления. Парадоксально, но принцип действия их квантовых аналогов (квантовых сенсоров) зачастую основан на глобальном недостатке квантовых систем – их чрезвычайной чувствительности к внешним возмущениям. Фактически квантовый сенсор представляет собой зонд (рис. 1), который благодаря этому свойству извлекает информацию о том или ином свойстве физического мира.

Например, если в качестве зонда использовать спин примесного атома (его ядра) в твердотельной матрице, то внешнее магнитное поле будет его поворачивать. Зависимость магнитного поля от времени приведет к аналогичной зависимости спина. Измерение и обработка результатов измерения его направления позволит оце-

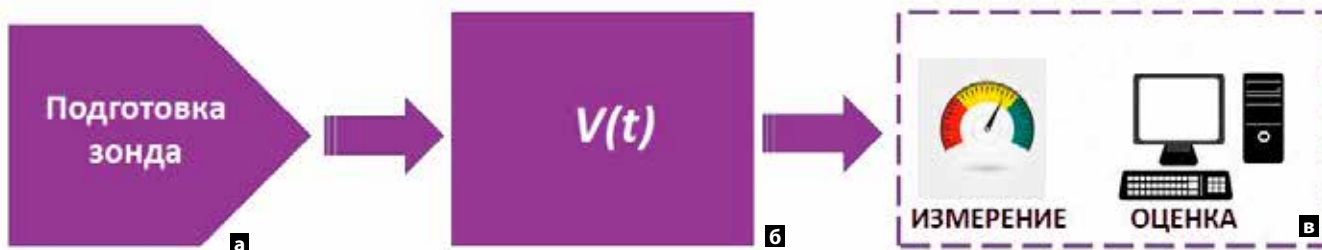


Рис. 1. Принцип действия квантового сенсора-зонда: а) подготовка зонда; б) воздействие на зонд внешнего возмущения  $V(t)$ ; в) измерение состояния зонда и математическая обработка результатов для оценки измеряемого воздействия

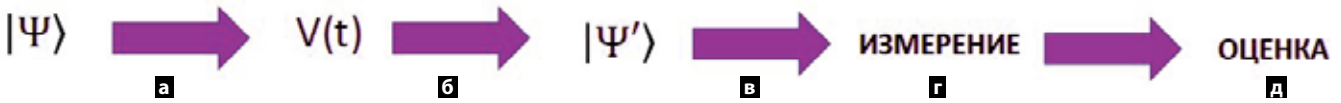


Рис. 2. Эволюция процесса преобразования состояния квантового объекта (зонда) от начального состояния (а), его взаимодействие с измеряемым физическим объектом (б) посредством оператора  $V(t)$ , преобразование в результате взаимодействия к новому состоянию (в) вплоть до измерения (г) и оценки (д)

нить эволюцию внешнего магнитного поля. Такие сенсоры востребованы, например, в медицине.

Несмотря на то, что квантовая сенсорика как отдельная область исследований появилась совсем недавно, многие подходы к решению задач квантового зондирования были хорошо известны и являются результатом развития таких направлений физики, как спектроскопия высокого разрешения, квантовая оптика, взаимодействие излучения с веществом и др. Эти подходы используют эффекты атомной интерферометрии, ядерного магнитного резонанса, лазерного охлаждения, метрологии, магнитометрии. Однако существенные надежды возлагаются на зондирование посредством отдельных квантовых объектов – например, на уровне одиночных атомов.

Как определить, что такое квантовый сенсор помимо того, что это «измерительное устройство, основанное на квантовых эффектах»? (В качестве дополнительного материала рекомендуем прекрасный обзор по технологии квантовой сенсорики [1]). Постараемся выделить и перечислить отличительные признаки квантовых сенсоров – иногда их называют критериями, аналогично известным критериям Ди Винченцо в квантовых вычислениях.

1. *Использование квантового объекта (зонда) для измерения физической величины (классической или квантовой).* При этом сам объект характеризуется квантованной структурой энергетических уровней – это электронные, магнитные, колебательные состояния сверхпроводящих или спиновых кубитов, нейтральных атомов или ионов.

2. *Применение квантовой когерентности* (например, в виде пространственной или временной суперпозиции) для измерения физической величины.

3. *Использование свойства перепутанности* для улучшения чувствительности измерений, то есть с более высокой точностью/чувствительностью, чем это имеет место при классических измерениях.

4. *Возможность приготовления (инициализации) квантовой системы* в известных состояниях и выполнения операции считывания (измерения) этих состояний.

5. *Когерентное манипулирование* (обычно с помощью полей, зависящих от времени). Это условие не строго обязательно для всех протоколов; примеры, выходящие за рамки этого критерия – измерение времен релаксации.

Далее неизменно возникает вопрос: как же работает квантовый сенсор? Приведем расширенную, по сравнению с изображенной на рис. 1, схему (рис. 2).

Квантовая система (зонд) взаимодействует с соответствующим физическим объектом  $V(t)$ , например электрическим или магнитным полем.

Взаимодействие количественно оценивается параметром вида  $\gamma = \partial^q E / \partial V^q$ , который связывает изменения энергии перехода  $E_k$  с изменением внешнего параметра  $V(t)$ . В большинстве ситуаций связь либо линейная ( $q = 1$ ), либо квадратичная ( $q = 2$ ). Взаимодействие с  $V(t)$  приводит к сдвигу энергетических уровней квантовой системы, что и подлежит измерению.

Введенный параметр  $\gamma$  тесно связан с так называемой внутренней чувствительностью сенсора – величиной, пропорциональной фактору

$$\frac{1}{\gamma \sqrt{T_\chi}}$$

где  $T_\chi$  – время релаксации системы. Из формулы следует, что для оптимизации чувствительности необходимо, чтобы параметр  $\gamma$  был достаточно большим. Например, этого можно добиться путем выбора соответствующей физической системы в качестве сенсора.

Также очевидно, что время релаксации  $T_\chi$  должно быть достаточно длительным.

Следуя логике схем, показанных на рис. 1, 2, остановимся на работе типичного (но не единственного) протокола квантового сенсора (под ним в квантовой обработке информации понимают последовательность действий,

необходимых для достижения результата). Этот протокол состоит из следующих этапов (рис. 3):

1. Инициализация зонда в известном базисном состоянии  $|0\rangle$ .

2. Преобразование к удобному начальному состоянию  $|\psi_0\rangle$ .

3. Эволюция под действием преобразования за время  $t$ :

$$|\psi(t)\rangle = \hat{U}_H(0, t)|\psi_0\rangle = c_0|\psi_0\rangle + c_1|\psi_1\rangle.$$

4. Преобразование в суперпозицию наблюдаемых состояний

$$|\alpha\rangle = \hat{U}_b|\psi(t)\rangle = c'_0|0'\rangle + c'_1|1'\rangle.$$

5. Измерение конечного состояния по дихотомной схеме Бернулли с вероятностями  $p$  и  $1-p$ .

6. Повторение шагов 1–5  $N$  раз для оценки вероятности измерения.

7. Измерение вероятности  $p$  как функции времени для оценки величины сигнала  $V(t)$ .

Приведенный пример протокола квантового сенсора – не единственно возможный. Например, полупроводниковый сенсор одиночных фотонов на основе лавинных фотодиодов работает совершенно по другому сценарию: здесь слабое электромагнитное поле является «затравкой» для лавинообразного процесса в полупроводниковой гетероструктуре. Лавина формирует макроскопический импульс напряжения, который регистрируется классическим счетчиком; при этом каждый импульс ассоциируется с приходом отдельного фотона. Вероятность возникновения лавины – это одна из базовых характеристик такого сенсора, отклик которого на предельно слабое световое поле и регистрируется соответствующим прибором – «счетчиком фотонов».

Развитие рынка квантовых сенсоров предполагает создание основного количества инновационных продуктов, технологий и отдельных отраслевых решений в рамках трех основных групп:

- часы, гравиметры, гироскопы, акселерометры;
- сенсоры электрического и магнитного поля;
- квантовая метрология.

Использование сенсоров, входящих в первые две группы, сводится к задачам в области создания инерциальных навигационных и магнитометрических систем для навигации в условиях отсутствия сигнала GPS. Действительно, гравитационные и магнитные поля Земли характеризуются небольшими аномалиями, которые варьируются от места к месту. Чувствительный гравиметр или магнитометр может проводить точные измерения локальных полей и сравнивать их



Рис. 3. Пример протокола квантового сенсора

с картами этих аномалий, чтобы позволить ориентироваться на местности без задействования каких-либо систем связи. По аналогии в основу автономных инерциальных навигационных систем могли бы лечь и квантовые акселерометры.

Другие варианты использования этого типа сенсоров:

- высокоточные часы и квантовые стандарты частоты могут найти коммерческое применение, например, для коррекции финансовых сделок и динамического регулирования потребления энергии электрическими сетями;
- с помощью гравиметров можно проводить сейсмографическое прогнозирование землетрясений и извержений вулканов, подземную разведку запасов нефти и газа, оценивать прочность грунта под крупными строительными объектами без необходимости бурения скважин;

- *квантовые акселерометры перспективны для обеспечения беспилотного режима движения транспортных средств;*
- *квантовые магнитометры могут оказаться востребованными в биомедицине, например, для улучшения чувствительности измерения магнитного поля в магнитной резонансной томографии.*

Квантовые сенсоры также востребованы для создания усовершенствованных образцов лидаров и радаров для решения задач разведки, наблюдения и рекогносцировки. Здесь наиболее известными разработками являются так называемые технологии скрытых (hidden) изображений и квантовой подсветки (quantum illumination). Однако несмотря на то, что соответствующие демонстрационные эксперименты были выполнены более 10 лет назад, существенного прогресса в продвижении к конечным продуктам к настоящему времени не наблюдается. По оценке специалистов, навигационные устройства из первых двух групп квантовых сенсоров будут созданы в пределах нескольких лет, а радарные и лидарные системы – в течение 10 и более лет. По объему рынка квантовые сенсоры уступают двум другим субтехнологиям: если в 2020 г. он оценивался в 414 млн долл., то к 2030 г., по оценкам OSA Industry Development Associates, он достигнет уровня 2 млрд долл. (соответственно, квантовые вычисления – 33 млн и 50 млрд долл., квантовые коммуникации – 84 млн и 7 млрд).

Мировые лидеры по квантовой сенсорике – США и Великобритания; исследования также ведутся в Австралии, Канаде, странах Евросоюза и Китае. В Российской Федерации в рамках реализации соглашения о намерениях между правительством и государственной корпорацией «РОСТЕХ» в 2019 г. была разрабо-

тана дорожная карта по развитию этой высокотехнологичной области. Однако в силу ряда причин она так и не была запущена, несмотря на то, что ряд предлагаемых в ней сенсоров имел высокий уровень готовности – прежде всего в области навигации и метрологии.

Что касается устройств квантовой метрологии, то в эту группу преимущественно вошли сенсоры, которым не нашлось место в первых двух. Наиболее перспективными и востребованными представляются счетчики фотонов в видимом и ближнем ИК-диапазонах, квантовые датчики случайных чисел, а также устройства абсолютной квантовой фотометрии. Последние представляют собой пример технологии, разработанной и апробированной в СССР и РФ, – создание нового поколения фотометрических устройств и эталонов на принципах квантовой механики [2].

В качестве примера квантового сенсора, основанного на перепутанных состояниях фотонов, приведем элегантную идею, предложенную Д.Н. Клышко [3] и доработанную группой Л.А. Кривицкого [4]. Перепутанные пары фотонов рождаются в двух (1 и 2) макроскопических областях толщиной  $L$ , разделенных зазором толщиной  $d$  (рис. 4).

Квантовая интерференция возникает как результат когерентного сложения амплитуд  $F^{(1)}$  и  $F^{(2)}$  пар фотонов:  $F = F^{(1)} + F^{(2)} \exp(i\Delta\phi)$ , где  $\Delta\phi \equiv \phi_p - (\phi_s + \phi_i)$  – фазовый набег между сигнальными ( $s$ ), холостыми ( $i$ ) фотонами, а также фотонами на частоте лазерной накачки ( $p$ ).

В результате интенсивность регистрируемого поля на сигнальной частоте оказывается

$$I_s(\omega_s, \theta_s) \propto \sin^2 \left[ \frac{\Delta_z L}{2} \right] \times \cos^2 \left[ \frac{\Delta_z L + \Delta_z^2 d}{2} \right].$$

Здесь  $\Delta_z = k_{z_p} - k_{z_s} - k_{z_i}$  – т.н. волновая расстройка, пропорциональная фазовому сдвигу  $\Delta\phi$ .

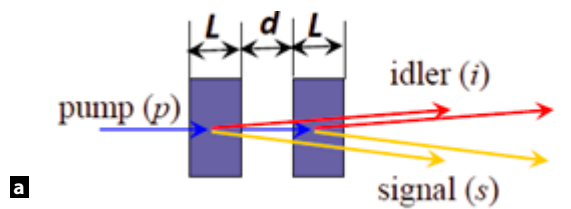
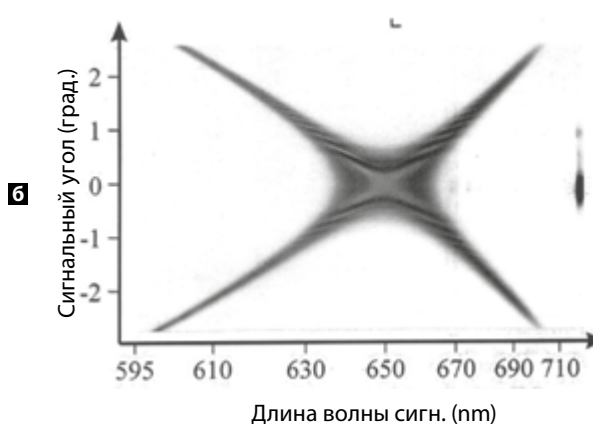


Рис. 4: а) схема для наблюдения квантовой интерференции пар фотонов, испущенных из двух макроскопических областей толщиной  $L$  (прямоугольники голубого цвета), разделенных зазором  $d$ ; б) распределение интенсивности сигнальных и холостых фотонов при трехфотонной интерференции (эксперимент)



Физическая система/тип	Кубит	Измеряемая величина	Хар. частота	Инициализация	Чтение
<b>Нейтральные атомы</b>					
Атомный пар II-III	Атомный спин	Магнитное поле, Вращение, Частота/Время	DC-10ГГц	Оптическая	Оптическое
Холодные атомы II-III	Атомный спин	Магнитное поле, Ускорение, Частота/Время	DC-10ГГц	Оптическая	Оптическое
<b>Ионы в ловушках</b>					
II-III	Долгоживущее электронное состояние, Колебательная мода	Электрическое поле, Сила, Вращение, Частота/Время	МГц	Оптическая	Оптическое
			ТГц	Оптическая	Оптическая
<b>Ридберговские атомы</b>					
II-III	Ридберговские состояния	Электрическое поле	DC, ГГц	Оптическая	Оптическое
<b>Твердотельные спины (ансамбли)</b>					
ЯМР-сенсоры II	Ядерный спин	Магнитное поле	DC	Температурная	Pick up coil
NV-сенсоры (ансамбли) II	Электронный спин	Магнитное поле, Электрическое поле, Температура, Давление, Вращение	DC-ГГц	Оптическая	Оптическое
<b>Твердотельные спины (одиночные спины)</b>					
P донор в Si II	Электронный спин	Магнитное поле	DC-ГГц	Термическая	Электрическое
Полупроводниковые квантовые точки II	Электронный спин	Магнитное поле	DC-ГГц	Электрическая, Оптико-электрическая, Оптическая	
Одиночный NV-центр II	Электронный спин	Магнитное поле, Электрическое поле, Температура, Давление, Вращение	DC-ГГц	Оптическая	Оптическое
<b>Сверхпроводящие цепи</b>					
SQUID II	Ток сверхпроводимости	Магнитное поле	DC-10ГГц	Термическая	Электрическое
Потоковый кубит II	Циркуляционный ток	Магнитное поле	DC-10ГГц	Термическая	Электрическое
Зарядовый кубит II	Зарядовые соб. состояния	Магнитное поле	DC-10ГГц	Термическая	Электрическое
<b>Элементарные частицы</b>					
Мюон II	Мюонный спин	Магнитное поле	DC	Радиоактивный распад	Радиоактивный распад
Нейтрон II	Ядерный спин	Магнитное поле, Гравитация	DC	Брагговское рассеяние	Брагговское рассеяние
<b>Другие сенсоры</b>					
Одноэлектронный транзистор I	Зарядовые соб. состояния	Электрическое поле	DC-100 МГц	Термическая	Электрическое
Оптомеханика I	Фононы	Сила, ускорение, Масса, Магнитное поле	нГц-МГц	Термическая	Оптическое
Интерферометр II-III	Фотоны, Атомы, Молекулы	Смещение, Показатель преломления			

Таблица. Классификация квантовых сенсоров

Это выражение по структуре очень похоже на известную формулу, которая описывает дифракцию плоской волны на двух щелях в классической оптике – огибающая  $\sin c^2 \left[ \frac{\Delta_x L}{2} \right]$  промодулирована функцией  $\cos^2 \left[ \frac{\Delta_x L + \Delta_x^2 d}{2} \right]$ . Только роль модуляционной функции играет фазовый вклад  $\Delta\phi$ , сформированный на трех частотах в зазоре  $d$  между двумя кристаллами. На рис. 4б четко видна интерференционная модуляция частотно-углового распределения интенсивности пар фотонов, структура которой позволяет измерять дисперсионные свойства среды-зазора в широком спектральном диапазоне. В частности, возможно проводить прецизионные измерения на частоте холостых фотонов в далеком ИК-диапазоне, измеряя распределение интенсивности на частоте сигнальных фотонов в видимой области спектра [3].

В заключение сравним известные на сегодняшний день сенсоры (таблица). Они отсортированы по таким признакам, как физическая платформа реализации сенсора (кубита), измеряемой величине (тип физического поля), харак-

терному времени отклика и/или диапазону частот, способу реализации начального и конечного состояний сенсора. Римскими цифрами I, II и III показаны перечисленные группы. Таблица представляет прежде всего методический интерес, поскольку показывает широту функционального охвата измеряемых величин и многообразие предлагаемых реализаций сенсоров. ■

Работа выполнена при поддержке Программы развития МГУ имени М.В. Ломоносова, проект №23А-Ш06-05.

#### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. C. L. Degen, F. Reinhard, P. Cappellaro. Quantum sensing. *Reviews of Modern Physics*. 2017. V. 89. P. 035002.
2. Д.Н. Клышко, А.Н. Пенин. Перспективы квантовой фотометрии // *Успехи физических наук*. 1987. Т. 152. №4. С. 653–665.
3. Д.Н. Клышко. Интерференция Рамзея при двухфотонном параметрическом рассеянии света // *Журнал экспериментальной и теоретической физики*. 1993. №104. P. 2676-2684.
4. D.A. Kalashnikov, A.V. Paterova, S.P. Kulik, L. Krivitsky. Infrared Spectroscopy with Visible Light // *Nature Photonics*. 2016. №10. С. 98–101.



# КВАНТОВЫЕ РАДАРЫ

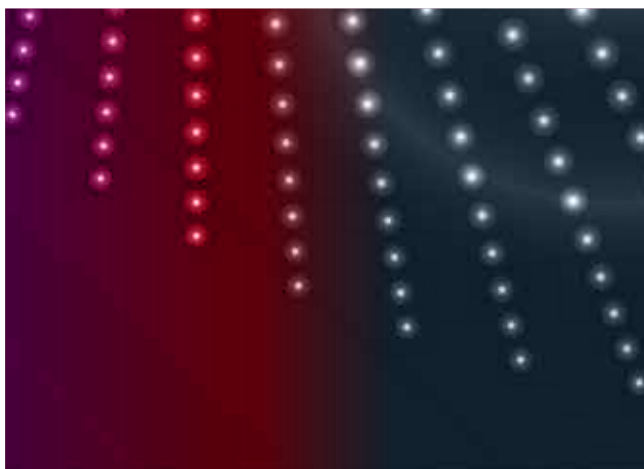


**Дмитрий Могилевцев,**  
зам. заведующего  
Центром «Квантовая  
оптика и квантовая  
информатика»  
Института физики  
НАН Беларуси,  
член-корреспондент

Первой квантовой революцией называют фундаментальный прорыв в понимании свойств вещества и излучения, произошедший в первой половине XX в. Результатом стало многое, без чего мы уже не мыслим свою повседневную жизнь: полупроводниковые технологии, принесшие нам мобильные телефоны и телевидение, компьютеры и навигаторы, лазеры, атомная энергетика и высокоточная медицинская диагностика.

**Н**ачало XXI в. ознаменовалось второй квантовой революцией, в основе которой лежит применение квантовых корреляций вещества и поля, в частности квантовой перепутанности (quantum entanglement) – явления, на заре развития квантовой механики казавшегося парадоксальным (свидетельство тому – знаменитый парадокс Эйнштейна-Подольского-Розена), приводящего к трудно вообразимому «мгновенному действию на расстоянии». Методологические трудности были разрешены в достаточной степени для того, чтобы породить и практически осуществить главный феномен: квантовую информатику, умение использовать для вычислений квантовые корреляции и получать необыкновенные результаты. Квантовые машины способны за доли секунды справиться с задачами, которые традиционные компьютеры не разрешили бы и за миллионы лет.

В числе детищ второй квантовой революции (наряду с квантовыми компьютерами, методами квантовой коммуникации и микроскопии) – новые методы диагностики удаленных объектов, так называемые квантовые радары – приборы, позволяющие улучшать возможности обнаружения и распознавания движущихся либо стационарных целей за счет неклассических свойств электромагнитного излучения, в частности квантовых корреляций.



## Рождение квантового радара

Традиционные радары – приборы, основанные на испускании направленного электромагнитного излучения, регистрации и анализе рассеянного/отраженного объектом излучения – уже давно перешли в область прикладной науки и инженерии. Основные принципы их функционирования и дизайн появились почти 100 лет назад (а прототип и вовсе был создан и продемонстрирован немцем Кристианом Хьюльсмейером в 1904 г.). Разумеется, непрерывно развиваются новые схемы и методы, улучшающие направленность пучка и контроль над его формой, используются новые материалы для антенн (разработанные недавно метаматериалы нашли широкое применение в радарной практике), создаются новые методы обработки сигналов. Примером последнего может служить так называемый фотонный радар, когда излучается сигнал по-прежнему длинноволнового диапазона, но в радарной системе обрабатывается уже оптический, модулированный на радарной частоте. Это дает возможность резко ускорить процесс обработки, генерировать импульсы недостижимой ранее спектральной ширины, и, соответственно, получить пространственное разрешение, сопоставимое с длиной волны радарного излучения.

Но все эти методы, пусть и изощренные, позволяли лишь приблизиться к хорошо известным пределам, но не превзойти их. Отношение сигнала к шуму накладывает фундаментальный предел на возможность обнаружения объектов на фоне шума, рэлеевский дифракционный предел ограничивает возможность распознавания рассеивающих объектов. Традиционные способы так или иначе подразумевают увеличение мощности для повышения отношения сигнала к шуму, использование более коротких импульсов и узконаправленных пучков для улучшения пространственного разрешения и регистрации перемещения объекта.

Потому изобретенный американским профессором Сефом Ллойдом в 2008 г. квантовый радар [1], сулящий обнаружение объектов на фоне шума при невероятно низких интенсивностях испущенного излучения, произвел ошеломляющее впечатление на радарное сообщество. Усилило эффект еще и то, что сам принцип был в достаточной мере прост и понятен: генерируется двухкомпонентное излучение, одна часть посылается к объекту, вторая сохраняется, чтобы затем интерферировать с отражен-

ным от него излучением. Результат интерференции измеряется и позволяет извлечь информацию о присутствии либо отсутствии объекта. Подобный же принцип применен, например, в шумовом радаре, разработанном еще в 50-е гг. прошлого века. Но коренным отличием предложенной Сефом Ллойдом схемы, названной «квантовой иллюминацией» было то, что посылаемая и сохраняемая части излучения были квантово коррелированными, а точнее, перепутанными. Это обещало прирост чувствительности, то есть уменьшение вероятности ошибки обнаружения объекта на фоне шума на несколько порядков при интенсивности сигнала на уровне одиночных фотонов. Она, согласно описанному протоколу [1], при использовании 2D-модового двухфотонного перепутанного состояния падает в  $D$  раз по сравнению с распределенным среди этих же мод однофотонным начальным состоянием, которое просто посылается на объект. Притом вероятность верного детектирования присутствующего объекта на фоне шума в обоих случаях одинакова. Простое увеличение  $D$ , то есть расширение частотной полосы сигнала, сулило огромный прирост отношения сигнала к шуму.

Этот поразительный факт открывал новую перспективу разработки стелс-радаров, работу которых не смогут засечь приемные устройства, предназначенные для обнаружения активных излучающих устройств. Само собой, как коммерческие предприятия, так и правительственные/военные организации заинтересовались подобными перспективами [2]. В результате научные группы, занимающиеся квантовыми радарными, получили весомую финансовую и организационную поддержку (краткий популярный обзор этого «квантово-радарного бума» можно видеть, например, в недавней работе [3]). В особенности военных подстегнуло заявление Китая в 2016 г. о создании квантового радара, способного обнаруживать самолеты, скрытые от классических радаров при помощи стелс-технологий.

## Расцвет и крах квантовой иллюминации

В начале 2010-х гг. исследовательские группы по всему миру активно занялись темой квантовых радаров на основе протокола квантовой иллюминации. Были проведены демонстрационные эксперименты в оптической области, доказавшие возможность выигрыша в отношении сигнала к шуму для квантовых перепутанных состо-



аний, началась работа по осуществлению протокола для микроволнового диапазона. На этом пути наметился существенный прогресс в разработке двухчастотной схемы. В ее рамках генерация перепутанного состояния осуществлялась в оптической области, затем электромеханический преобразователь перепутывал микроволновое и оптическое поля. Первое посылалось к объекту, а рассеянное поле преобразовывалось обратно в оптический диапазон и измерялось совместно с сохраненной частью изначального поля [4]. Также были разработаны схемы, где перепутанные состояния создавались сразу в микроволновой области при помощи сверхпроводящих параметрических усилителей, предложили возможность использования не только пространственных, но и временных корреляций. Появился ряд экспериментальных реализаций, где декларировалось многократное, и даже порядковое превосходство разработанных квантовых радарных схем над классическими [5, 3].

Декада оптимизма завершилась, когда аккуратный теоретический анализ схемы квантовой иллюминации был сопоставлен с практическими реализациями, и было оценено, сколько потребуется ресурсов для производства практически действующего радара. Для гауссовых перепутанных состояний, доступных для создания практически действующего радара, максимальная выгода по отношению сигнала к шуму при наилучшем возможном детектировании достигает всего 6 децибел. При практически удобном детектировании, когда не нужно перепутывания прошедшего и сохраненного сигнала, выгода ограничивается всего 3 децибелами. Но даже и это умеренное, но вполне ощутимое и полезное преимущество исчезает в существующих реализациях схем квантовой иллюминации [6]. К сожалению, для оригинальной схемы нужны знание о расстоянии до объекта, сохранение поляризации поля, отсутствие потерь у части поля, остающейся у экспериментатора, и высокоэффективные измерения. При усилении поля, осуществляемом при преобразовании из оптического в микроволновой диапазон, неизбежно добавляется шум, негативно сказывающийся на квантовых корреляциях. Кроме того, оказалось, что улучшение на порядок демонстрировалось при сравнении с радарными схемами, далекими от оптимальной классической модели.

В сентябре 2020 г. журнал «Сайнс» разместил заметку, название которой переводится как «Короткая странная жизнь квантового

радар», с подзаголовком «Вопреки интересам военных, квантовая механика не победит стелс-технологии» [7]. В публикации подверглось вполне обоснованному сомнению заявление Китая о создании квантового радара, и был поставлен жирный знак вопроса на принципиальной осуществимости квантового радара, по крайней мере, на основе протокола квантовой иллюминации.

## Дальнейшее развитие квантовых радаров

Разочарование в квантовой иллюминации, однако, не поставило крест на работах по нахождению и использованию квантовых преимуществ в обнаружении и распознавании удаленных объектов. В методологически схожих протоколах квантовой микроскопии и визуализации, в квантовой метрологии существование преимущества за счет квантовых корреляций и самой неклассичности излучения, которым высвечивается объект, – уже устоявшийся факт. Так, например, использование перепутанных состояний позволяет достичь предельно допустимой квантовой механикой точности, так называемого гейзенберговского предела в случае измерения фазы, а применение фоковских состояний, то есть собственных состояний оператора энергии, обеспечивает достижение гейзенберговского предела в оценке поглощения [8]. Тщательное изучение квантовой иллюминации помогло определить источник квантового преимущества и продолжить работу как над новыми квантово-радарными схемами, так и над применением наработок в области создания радара на квантовой иллюминации.

Здесь надо отметить, что квантовая перепутанность не является необходимой для достижения преимуществ в схеме квантовой иллюминации. На самом деле от объекта возвращается и попадает на детектор лишь малая часть испущенного излучения. Подобные потери неизбежно разрушают квантовую перепутанность. Было показано, что за квантовое преимущество в протоколе квантовой иллюминации отвечает другой, гораздо более устойчивый к потерям вид квантовых корреляций – «квантовый дискорд» [9].

Также было показано, что использование в квантовой иллюминации корреляций не по одной, а по нескольким степеням свободы, например по поляризации и частоте, увеличивает предельно достижимые значения выигрыша в отношении сигнала к шуму по сравнению

с оптимальной классической схемой. Этот выигрыш составляет 6 дБ на дополнительную степень свободы (хотя реализация этого преимущества требует более сложной схемы детектирования) [10]. Применение неклассических негауссовских состояний, в частности ограниченных по числу фотонов, вкуче с детекторами, различающими числа фотонов, также позволяет значительно сдвинуть предел выигрыша по отношению сигнала к шуму [11].

Неожиданные результаты дало применение квантовой иллюминации не для обнаружения объекта, а для расчета расстояния до него при использовании перепутанных по частоте состояний: выигрыш по сравнению с классическим радаром той же мощности и спектра может составлять десятки децибел [12]. Использование многомодовых перепутанных состояний, как и в квантовой микроскопии, может значительно улучшить локализацию объекта. Так,  $N$ -фотонные перепутанные состояния позволяют в  $\sqrt{N}$  раз улучшить точность определения пространственного положения точечного объекта по сравнению с  $N$ -фотонным некоррелированным состоянием [13]. Также квантовые корреляции существенно улучшают точность распознавания объекта. Так, пространственно-временные корреляции, произведенные, например, парой взаимодействующих и спонтанно испускающих квантовых диполей, могут преодолеть рэлеевский предел при определении расстояния между малыми рассеивателями [14]. Квантовые корреляции позволяют и существенно увеличить точность определения скорости объекта [15].

## Перспективы

Быстрый рост популярности и последующий крах квантовых радаров, основанных на квантовой иллюминации, несомненно, нанес значительный вред данной области квантовых технологий. Фактически, он вернул ее на уровень экспериментальных демонстраций самой возможности предсказанного теоретиками эффекта. Тем не менее экспериментаторами уже совершены уверенные первые шаги в данном направлении. Так, совсем недавно был продемонстрирован чисто микроволновой радарный прибор, действительно дающий квантовое преимущество при обнаружении объекта [16]. Микроволновые квантовые технологии быстро развиваются, и уже доступны однофотонные детекторы в данной области длин волн,

равно как и новые способы генерации неклассических состояний вкуче с малошумящими усилителями, позволяющие с оптимизмом смотреть на перспективы квантовых радаров [17].

Следует также заметить, что в Республике Беларусь, в частности в Центре «Квантовая оптика и квантовая информатика» Института физики НАН Беларуси, с 2018 г. ведутся исследования в области квантовой визуализации и сенсинга, в том числе и в сфере квантовых радаров, приведшие к ряду публикаций в высокорейтинговых физических журналах [3, 14]. Подобные исследования планируется продолжить с перспективами экспериментальной реализации. ■

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. S. Lloyd. Enhanced sensitivity of photodetection via quantum illumination / S. Lloyd // *Science*. 2008. Vol. 321. №5895. P. 1465.
2. M. Høijer, T. Hult and P. Jonsson. Quantum Radar. Quantum Radar – A survey of the science, technology and literature // <https://www.foi.se/rest-api/report/FOI-R-4854-SE>.
3. G. Slepian. Quantum Radars and Lidars: Concepts, realizations, and perspectives / G. Slepian, S. Vlasenko, D. Mogilevtsev and A. Boag // *IEEE Antennas and Propagation Magazine*. 2022. Vol. 64. №1. P. 16–26.
4. S. Barzanjeh. Microwave Quantum Illumination / S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J.H. Shapiro, and S. Pirandola // *Phys. Rev. Lett.* 2015. Vol. 114, P. 080503.
5. G. Sorelli. Detecting a Target With Quantum Entanglement / G. Sorelli, N. Treps, F. Grosshans and F. Boust // *IEEE Aerospace and Electronic Systems Magazine*. 2022. Vol. 37. №5. P. 68–90.
6. J.H. Shapiro. The Quantum Illumination Story / J.H. Shapiro // *IEEE Aerospace and Electronic Systems Magazine*. 2020. Vol. 35. №4. P. 8–20.
7. A. Cho. The short, strange life of quantum radar / A. Cho // *Science*. 2020. Vol. 369, №6511 P. 1556–1557.
8. M. Barbieri. Optical Quantum Metrology / M. Barbieri // *PRX Quantum* 2022. Vol. 3. P. 010202.
9. C. Weedbrook. How discord underlies the noise resilience of quantum illumination / C. Weedbrook, S. Pirandola, J. Thompson, V. Vedral, and M. Gu // *New J. Phys.* 2016. Vol. 18, №4. P. 043027.
10. A. Varadaraj Prabhu. Hyperentanglement-enhanced quantum illumination / A. Varadaraj Prabhu, B. Suri, and C.M. Chandrasheka // *Phys. Rev. A*. 2021. Vol. 103. P. 052608.
11. L. Cohen. Thresholded Quantum LIDAR: Exploiting Photon-Number-Resolving Detection / L. Cohen, E.S. Matekole, Y. Sher, D. Istrati, H.S. Eisenberg, and J.P. Dowling // *Phys. Rev. Lett.* 2019. Vol. 123. P. 203601.
12. Q. Zhuang. Ultimate Accuracy Limit of Quantum Pulse-Compression Ranging / Q. Zhuang and J.H. Shapiro // *Phys. Rev. Lett.* 2022. Vol. 128. P. 010501.
13. L. Maccone and C. Ren. Quantum Radar / L. Maccone and C. Ren // *Phys. Rev. Lett.* 2020. Vol. 124. P. 200503.
14. I. Peshko. Quantum noise radar: superresolution with quantum antennas by accessing spatiotemporal correlations / I. Peshko, D. Mogilevtsev, I. Karuseichyk, A. Mikhalychev, A.P. Nizovtsev, G. Ya. Slepian, and A. Boag // *Opt. Express* 2019. Vol. 27. P. 29217–29231.
15. M. Reichert. Quantum-enhanced Doppler lidar / M. Reichert, R. Di Candia, M.Z. Win [et al.] // *Npj. Quantum. Inf.* 2022. Vol. 8. P. 147.
16. R. Assouly. Quantum advantage in microwave quantum radar / R. Assouly, R. Dassonneville, T. Peronin [et al.] // <https://doi.org/10.1038/s41567-023-02113-4>.
17. M. Casariego. Propagating quantum microwaves: towards applications in communication and sensing / M. Casariego [et al.] // *Quantum Sci. Technol.* 2023. Vol. 8 P. 023001.

# КВАНТОВЫЕ СЕНСОРЫ НА БАЗЕ ЦЕНТРОВ ОКРАСКИ В АЛМАЗЕ



**Алексей Акимов,**  
руководитель группы «Квантовые симуляторы» Российского квантового центра, старший научный сотрудник Физического института им. П. Н. Лебедева, научный руководитель ООО «Сенсор Спин Технолоджис», кандидат физико-математических наук

Квантовые сенсоры и метрология — одно из важных направлений в развитии квантовых технологий будущего. Сенсоры используют квантовые объекты и алгоритмы для достижения рекордных показателей чувствительности, пространственного разрешения и других характеристик. Одним из популярных векторов стали изыскания на базе центров окраски в алмазе.

Внимание исследователей привлекают квантовые вычисления, обещающие решить все сложные для классического компьютера задачи, а также линии связи, которые предлагают новый и удобный метод надежно защищенной передачи данных. В ходе развития квантовых вычислений, однако, много проблем, связанных с тем, что единичные квантовые объекты, используемые в качестве элементарных битов информации — кубитов, — оказываются крайне чувствительными к различным внешним факторам и легко теряют полезную информацию из-за взаимодействия с внешним миром. Здесь и появляется идея квантовых сенсоров. А что, если развернуть задачу и использовать чувствительность кубитов к внешним воздействиям и, собственно, измерять их за счет оценки состояния кубита? Эта простая на первый взгляд идея оказалась очень эффективной. Следуя данному подходу, ученые разных стран разработали множество сенсоров, обладающих высокой точностью, малым дрейфом, высоким пространственным разрешением, которые уже начали внедрять в коммерческие продукты. Часто для измерения тех или иных величин применяют последовательности измерения, очень близкие к традиционно разработанным для квантовых вычислений, и по возникающим в этих последовательностях ошибкам делается вывод. Такой подход используется и в метрологии, в частности при определении времени. Однако было бы странно остановиться только на алгоритмах для вычислений: в конце концов, квантовая механика — наука о единичных объектах, фактически о шумах, позволяющая понять пределы, достижимые в точности измерений, и преодолеть многие, казалось бы, фундаментальные шумы в процессе измерения. Остановимся лишь на некоторых ярких примерах развития квантовых сенсоров, в основном фокусируясь на использовании центров окраски в прозрачных кристаллах.

## Сенсоры на базе центров окраски в алмазе

Центры окраски получили свое название благодаря тому, что придают кристаллам цвет. По сути же, это дефекты специального вида в структуре кристалла. Чистый алмаз прозрачен, однако при добавлении примесей он может стать практически любого цвета. Эта особенность активно используется ювелирной индустрией, но в рамках статьи ограничимся

описанием наиболее полезных центров окраски. Самый известный из них – азот-вакансия. Азот – самая распространенная примесь как в естественном, так и в искусственном алмазе, прежде всего потому, что его очень много в атмосфере Земли. Азот-вакансия представляет собой дефект в кристаллической решетке алмаза, в котором один атом углерода замещен азотом, а еще один, соседний с азотом атом углерода, отсутствует. Такой дефект должен быть электрически нейтральным, но если ему удастся захватить электрон, то такой заряженный вариант оказывается энергетически более выгодным. Именно отрицательно заряженный центр и используется в сенсорных приложениях, поэтому далее мы будем называть центром азот-вакансия (NV-центр) такую его версию. Основная его особенность – зависимость свечения от направления электронного спина. Линия, соединяющая положение азота и отсутствующего атома азота-вакансии, определяет выделенное направление, или ось центра. Суммарный собственный механический момент или спин всех электронов, имеющих в центре окраски, составляет 1, но вектор спина может иметь разные проекции на ось, а именно  $-1$ ,  $0$ ,  $1$ . Эти выделенные состояния обладают существенно разной светимостью: если облучить зеленым одиночный центр окраски азот-вакансия с проекцией спина  $0$ , он будет примерно на 30% ярче, чем центр с проекциями  $+1$  или  $-1$ . Более того, если NV-центр подвергнуть облучению зеленого света (чаще всего используется длина волны 532 нм), то спин электрона поляризуется перпендикулярно оси. Эти два свойства оказываются ключевыми в приложениях NV-центров. Если поляризованный с помощью зеленого света NV-центр подвергнуть облучению микроволн на частоте, соответствующей разнице частот уровней энергии, сообразных проекциям спина, то он перевернется, и свечение центра упадет. В результате в спектре свечения NV-центра при сканировании частоты прилагаемых к нему микроволн возникнет провал, получивший название оптически детектируемого магнитного резонанса.

Оказывается, что в отсутствие внешних полей и напряжений в алмазе разными энергиями обладают только проекции спина  $0$  и  $\pm 1$ , а проекции  $\pm 1$  оказываются вырождены. Однако при приложении внешнего магнитного поля они расщепляются, позволяя независимо управлять микроволновым полем состояниями с проекциями спина  $+1$  и  $-1$ , а следовательно, кубитами на переходах  $|0\rangle \rightarrow |1\rangle$  и  $|0\rangle \rightarrow |-1\rangle$ . Время когерентности таких кубитов определяется взаимодействием спина электрона

с окружением. Он обладает магнитным моментом, а потому крайне чувствителен к полям, создаваемым другими парамагнитными примесями в алмазе. Для устранения этого влияния были разработаны сложные последовательности, самая простая из которых – Хан-эхо – представляет собой очень близкую к эхо-последовательности, привычной в области электронного парамагнитного резонанса, что позволяет за счет переворота кубита посередине ее в существенной степени учесть влияние внешнего магнитного поля на состояние кубита, поскольку во второй половине последовательности кубит будет подвержен той же динамике, но с обратным знаком.

В 2008 г. группа Михаила Лукина в Гарварде предложила использовать эхо-последовательность с обратной целью – для измерения магнитного поля [1]. Если оно прикладывается на той же частоте, что и эхо-последовательность, то есть меняет знак в тот же момент, когда эхо-последовательность переворачивает спин, то последовательность не сработает и сигнал когерентности упадет по величине. Сравнительная оценка влияния поля на частоте с сигналом измерения когерентности в отсутствие поля, можно определить его величину. Такой метод очень похож на синхронное детектирование. Оценки, приведенные в оригинальной работе, были очень оптимистичны, обещая с помощью ансамбля NV-центров достичь чувствительности в единицы фемтотесла (фТл) (сопоставимой с наиболее сенсорными из промышленно доступных магнитометров) сверхпроводящих квантовых интерферометров СКВИД. Важная особенность предложенного магнитометра – высокое пространственное разрешение, ведь сенсором может являться одиночный центр окраски, а методы его наблюдения уже были разработаны! По сути, разрешение ограничивается лишь тем, насколько близко можно подойти к NV-центру, что в ряде случаев составляет единицы нанометров, и при этом обладать чувствительностью, достаточной для измерения как спина единичного электрона, так и единичного ядерного спина с гораздо меньшим магнитным моментом. В той же работе указывалось, что возможно измерение и постоянного поля, хотя при этом должны быть задействованы другие последовательности.

С момента появления первого предложения измерение магнитного поля на базе NV-центров в алмазе активно развивалось. Электронный парамагнитный резонанс и ядерный магнитный резонанс, более известный как магнитный резонанс, получили распространение в ряде областей, включая медицину. В частности, широко известна повсе-



местно распространенная МРТ. В традиционной реализации, однако, эти методы часто используют огромные магнитные поля, создаваемые сверхпроводящими магнитами, или сверхпроводящие сенсоры СКВИД. Обычно их пространственное разрешение не велико и требует относительно большого объема материала для измерений.

Более компактные сенсоры на базе алмазов быстро привлекли внимание биологов и материаловедов. Чувствительность сенсоров на базе NV-центров еще не достигла первоначально предсказанного предела, и пока рекордное измерение позволило достигнуть лишь  $70 \text{ фТл}/\sqrt{\text{Гц}}$  по переменному полю на частоте  $0,35 \text{ МГц}$  [2] и  $195 \text{ фТл}/\sqrt{\text{Гц}}$  [3] по постоянному полю за счет применения ферритных концентраторов магнитного поля на алмазе. Тем не менее даже реализации в 100–1000 раз меньшей чувствительности, чем теоретический предел, уже хватило для привлечения индустрии и создания целого семейства молодых компаний.

Спектр исследований с использованием NV-центров в качестве магнитометров крайне широк. Совершенствуются интегральные версии, в которых все микроволновое управление, фотодетектор и сам алмаз умещаются в один чип [4], по размерам не превышающий обычный операционный усилитель. Его точность пока невелика, но исследования находят лишь в начале пути.

Получили развитие сканирующие устройства, похожие на атомно-силовой или магнитно-силовой микроскоп, в которых щупом выступает выполненный из алмаза параллелепипед с небольшим чувствительным цилиндром, также из алмаза, содержащего NV-центры. Такие устройства сочетают большое пространственное разрешение с хорошей чувствительностью к магнитному полю и уже используются для анализа дефектов в микросхемах и биологических исследованиях [5].

Продолжают совершенствоваться сканирующие микроскопы с алмазным щупом. Рассматривая кубит NV-центра на вершине щупа как диполь, ученые реализовали ближнепольную передачу энергии между молекулами на поверхности благодаря методу диагностики молекул FRET. Он используется для изучения биомолекулярной динамики, включающей изменение структуры молекул. В сочетании с пространственным разрешением NV-центров он теперь может применяться для контроля излучения единичных молекул аналогично тому, как это было продемонстрировано для плазмонных щупов. Интересно отметить, что ближнепольному взаимодействию подвержены только центры окраски

на самой вершине в нескольких последних нанометрах цилиндрической части щупа, в то время как весь цилиндр составляет в высоту около 1 мкм, поэтому с помощью остальных NV-центров, лежащих выше над поверхностью, можно по-прежнему измерять магнитное поле. И хотя разрешение в таком приборе несколько ниже, возможность одновременного измерения, безусловно, представляет существенный интерес.

Все более и более активное развитие получает применение наноалмазов в биологии. Химически и биологически они инертны, поэтому могут относительно легко быть внедрены в клетки. В идеальном случае алмазы могут служить сенсорами, однако профессор Куан Ли из Китая использует магнитометрию на алмазах в специально приложенном внешнем поле для определения ориентации и положения самого алмаза, внедренного в клетку, измеряя тем самым ее внутреннюю динамику. Сочетая такой сенсор с алмазным щупом, который в данном случае служит также для деформации стенки клетки, оцениваются ее эластичные свойства и влияние деформаций на внутреннюю динамику [6].

Волоконные магнитометры, которые хотя и уступают по чувствительности магнитометрам на основе больших алмазных пластин, благодаря гибкости волокна могут быть полезны во многих областях медицины и биологии, в частности для измерения магнитных полей в головном мозге или сердце [7].

Двигаясь в сторону практических приложений, группа профессора Рональда Валсворта разработала обеспечивающие широкопольное изображение магнитных полей над поверхностью алмазной пластины устройство, достаточно удобное для применения. Оно было использовано как для фундаментальных целей, таких как измерение распределения токов в графене, так и для более практических, а именно детектирования отдельных молекул в растворе. При этом они не обязательно должны быть магнитными. Данный метод опирается на два типа магнитных частиц, покрытых антителами, которые адресно прикрепляются к исходной молекуле. Магнитометр на NV-центрах последовательно опрашивает каждый тип частиц и определяет количество искомым молекул по числу совпадений двух магнитных частиц, приклеившихся друг к другу через молекулу и свое покрытие из антител. Метод позволяет детектировать десятки микромолей вещества и постоянно развивается [8].

Группа работает над повышением чувствительности, включая разработку способов поляризации обладающих ядерным спином примесей в алмазе

(в первую очередь 13-го изотопа углерода). Не менее важная задача – совершенствование методов ядерного магнитного резонанса, который позволяет анализировать химический состав окружения алмаза [9]. Повышение чувствительности магнитометров возможно за счет нескольких подходов. Прежде всего могут быть оптимизированы сами алмазные пластины, а также алгоритмы считывания магнитного поля. С точки зрения алмазных пластин важными параметрами являются время когерентности, концентрация NV-центров и доля поглощения излучения накачки ими. Увы, в современных алмазах, даже искусственно выращенных для приложений в магнитометрии, только малая доля их поглощения (часто менее 1%!) приходится на NV-центры, поэтому активно ведутся исследования по увеличению этого коэффициента, в частности повышению конверсии содержащегося в алмазе азота в полезные NV-центры. Достигнут рекорд конверсии азота в NV-центры в 37% [10].

Азот необходим в алмазе как источник электронов для NV-центров, но в то же время он – один из основных источников декогерентности, а следовательно, ограничивает чувствительность магнитометров. Поэтому методы диагностики и минимизации содержания бесполезного для измерений азота активно развиваются. В частности, недавно предложен способ внедрения в алмаз фосфора для выполнения зарядовой функции азота с надеждой увеличить время когерентности NV-центров и повысить конверсию азота в полезные NV-центры [11].

Исходное предложение магнитометрии с NV-центрами ограничивалось лишь постоянным полем и полем на частоте в несколько кГц. Однако на практике интерес могут представлять и большие частоты. Совершенствование методов измерения позволило расширить диапазон детектируемых магнитных полей сначала на диапазон до 10 МГц благодаря более сложным последовательностям динамической отвязки окружения (CPMG), а также на диапазон 1–10 ГГц за счет измерения времени продольной релаксации. Недавно был перекрыт и диапазон 10 МГц–1 ГГц за счет применения самого NV-центра как миксера частот, гетеродинирующего входящую частоту к частотам, удобным NV-центру как сенсору магнитного поля [12].

Магнитометры на NV-центрах применяют и в ряде других направлений научных исследований, в частности для детектирования намагниченности антиферромагнитных материалов и необычных магнитных состояний – скирмионов. Из интересных приложений магнитометров на NV-центрах

следует упомянуть измерение намагниченности метеоритов и других геологических образцов, которое может пролить свет на историю развития нашей планеты. Имеются предложения об использовании сенсоров на базе алмаза в составе детекторов темной материи [13].

Однако измерение магнитного поля – далеко не единственное применение NV-центров в алмазе. Той же группой Михаила Лукина в 2013 г. было предложено с помощью NV-центра измерять температуру в живых клетках. Метод совершенствовался для термометрии как внутри клетки, так и в ее окрестностях. С помощью NV-центров был получен новый результат в биологии, объясняющий процессы термочувствительности змей, активации нейронов и других связанных вопросов [14]. Несмотря на колоссальный успех NV-центров, их приложения в термометрии живых систем имеют сложности, связанные с необходимостью использования микроволнового излучения, близкого по частоте к показателю обычной микроволновой печи, для работы сенсора. Этот недостаток требует большой осторожности от исследователей, которым приходится ломать голову над тем, как при этом не поджарить клетку. Для устранения данного недостатка учеными из Техасского университета и Гарварда почти одновременно были предложены новые сенсоры на основе других кандидатов в кубиты – центров окраски *германий-вакансия* и *кремний-вакансия*. Позже к ним присоединились центры *олово-вакансия*. На их основе удалось реализовать полностью оптические сенсоры температуры, позволяющие измерять ее с высоким разрешением и чувствительностью около  $0.3 \text{ K}/\sqrt{\text{Гц}}$ . Эти сенсоры также были реализованы в волоконном варианте и сегодня используются в исследованиях мозга и клеток [15].

Наличие ядерного спина у азота, входящего в NV-центр, позволяет еще более расширить его применение в качестве сенсора. В частности, долгое время стоял рекорд чувствительности магнитного поля в субпикотесла (лучше, чем  $10^{-12}$  Тесла), использующий ядерный спин в качестве памяти и таким образом повышающий чувствительность магнитометра [16]. Другим возможным применением ядерного спина является измерение вращения, теоретически предложенное в 2012 г. и экспериментально реализованное российскими [17] а затем и американскими учеными в 2021 г. Идея гироскопа заключается в использовании спина ядра как механического момента, который должен прецессировать при вращении. К сожалению, наличие у элементарных частиц спина сопровождается присут-



ствием магнитного момента. Однако у электрона спин также обладает и механическим моментом, и магнитным, который в  $10^4$  раз больше, чем у ядра. Поэтому можно измерять вращение ядерным спином, компенсируя его чувствительность к магнитному полю за счет параллельного его измерения с помощью электронного спина того же NV-центра. Оказывается, что уровни энергии как электронного, так и ядерного спинов чувствительны к температуре, поэтому первый используется еще и как сенсор температуры. Его преимущество – отсутствие фундаментальных дрейфов базовой линии, так как чувствительность завязана на параметры одиночного атома и, следовательно, не зависит ни от времени, ни от того, какой атом взят. Сегодня она сопоставима с хорошими образцами микроэлектромеханических гироскопов (MEMS), обладающих заметным дрейфом нуля и требующих периодической калибровки.

Одна из проблем современных магнитометров на NV-центрах – неоднородность управляющего микроволнового поля. Есть несколько методов решения этой проблемы: размещение пластины алмаза в ближнем поле микроволновой чип-антенны, которое на несколько порядков снижает необходимое энергопотребление антенны, использование антенн специальной формы или выполненных из диэлектрического резонатора [18]. Последний подход недавно привел к идее нового метода измерения магнитного поля, основанного на наблюдении за дисперсией микроволнового сигнала в диэлектрическом резонаторе, содержащем алмазные образцы. Магнитометр тогда еще реализован не был, но первые оценки показывают, что его теоретический предел на 2 порядка лучше, чем первоначальный [19].

Несколько ранее было продемонстрировано измерение вращения на электронном спине. При этом чувствительность оказалась невысокой, однако этот способ получил развитие в качестве метода измерения постоянных магнитных полей. Дело в том, что, как правило, переменное магнитное поле удается измерить заметно точнее, чем постоянное. Вращение же алмаза делает постоянное в лабораторной системе координат поле переменным, таким образом решая вопрос переноса чувствительности переменного поля на постоянное [20]. Пока продемонстрирован лишь тестовый эксперимент, но в ближайшее время можно ожидать реализации подобного устройства уже с рекордной чувствительностью.

Центры окраски в алмазе, главным образом NV-центр, стали основой ряда разнообразных сенсоров магнитного поля, температуры и вращения. Они

широко применяются в исследованиях в физике, химии, биологии, геологии, идет речь об их использовании в астрономии, в частности для поиска темной материи. Возможно, центры окраски будут полезны в инерционной навигации. На их основе уже создаются научные приборы, и весьма вероятно, что очень скоро они найдут себе путь в область бытового приборостроения. ■

Работа поддержана грантом №21-42-04407  
Российского научного фонда.

#### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. J.R. Maze. Nanoscale Magnetic Sensing with an Individual Electronic Spin in Diamond / J.R. Maze [et al.] // *Nature*. 2008. №455. P. 644.
2. Y. Silani. Nuclear Quadrupole Resonance Spectroscopy with a Femtotesla Diamond Magnetometer / Y. Silani [et al.] // *Sci Adv*. 2023. №9. P.21.
3. Y. Xie. A Hybrid Magnetometer towards Femtotesla Sensitivity under Ambient Conditions / Y. Xie [et al.] // *Sci Bull (Beijing)*. 2021. №66. P. 127.
4. D. Kim. A CMOS-Integrated Quantum Sensor Based on Nitrogen–Vacancy Centres / D. Kim [et al.] // *Nat Electron*. 2019. №2. P. 284.
5. Y. Ninio. High-Sensitivity, High-Resolution Detection of Reactive Oxygen Species Concentration Using NV Centers / Y. Ninio [et al.] // *ACS Photonics*. 2021. №8. P. 1917.
6. K. Xia. Nanometer-Precision Non-Local Deformation Reconstruction Using Nanodiamond Sensing / K. Xia [et al.] // *Nature Communications*. 2019. №10, P. 1.
7. S. Blakley. Vectorial Magnetic Field Sensing with a Dual-Core Photonic-Crystal Fiber: Toward Fiber-Optic Stereomagnetometry / S. Blakley [et al.] // *AIP Conference Proceedings*. 2018 Vol. 1936 (American Institute of Physics Inc., 2018).
8. N. Aslam. Quantum Sensors for Biomedical Applications / N. Aslam [et al.] // *Nature Reviews Physics*. 2023. №5. P. 157.
9. N. Arunkumar. Micron-Scale NV-NMR Spectroscopy with Signal Amplification by Reversible Exchange / N. Arunkumar [et al.] // *PRX Quantum*. 2021. №2. P. 010305.
10. S.V. Bolshedvorskii. The Study of the Efficiency of Nitrogen to Nitrogen-Vacancy (NV)-Center Conversion in High-Nitrogen Content Samples, *Physica Status Solidi (RRL)* / S.V. Bolshedvorskii [et al.] // *Rapid Research Letters*. 2023. №17. P. 2200415.
11. J. Geng. Dopant-Assisted Stabilization of Negatively Charged Single Nitrogen-Vacancy Centers in Phosphorus-Doped Diamond at Low Temperatures / J. Geng [et al.] // *Cornell University*. 2023. 2305.15160v1.
12. G. Wang. Sensing of Arbitrary-Frequency Fields Using a Quantum Mixer / G. Wang, Y.X. Liu, J.M. Schloss, S.T. Alsid, D.A. Braje, P. Cappellaro // *Phys Rev*. 2022. №12. P. 021061.
13. S. Baum. Mineral Detection of Neutrinos and Dark Matter. A Whitepaper / S. Baum [et al.] // *Physics of the Dark Universe*. 2023. №41. P. 101245.
14. Y.G. Ermakova. Thermogenetic Neurostimulation with Single-Cell Resolution / Y.G. Ermakova [et al.] // *Nat Commun*. 2017. №8. P. 15362.
15. I.V. Fedotov. All-Optical Brain Thermometry in Freely Moving Animals / I.V. Fedotov, M.A. Solotenko, M.S. Pochechuev, O.I. Ivashkina, S.Ya. Kilin, K.V. Anokhin, A.M. Zheltikov // *ACS Photonics*. 2020. №7. P. 3353.
16. T. Wolf. Subpicotesla Diamond Magnetometry / T. Wolf, P. Neumann, K. Nakamura, H. Sumiya, T. Ohshima, J. Isoya, J. Wrachtrup // *Phys Rev*. 2015. №5. P. 041001.
17. V.V. Soshenko. Nuclear Spin Gyroscope Based on the Nitrogen Vacancy Center in Diamond / V.V. Soshenko, S.V. Bolshedvorskii, O. Rubinas, V.N. Sorokin, A.N. Smolyaninov, V.V. Vorobyov, A.V. Akimov // *Phys Rev Lett*. 2021. №126. P.197702.
18. P. Kapitanova. 3D Uniform Manipulation of NV Centers in Diamond Using a Dielectric Resonator Antenna / P. Kapitanova, V.V. Soshenko, V.V. Vorobyov, D. Dobrykh, S.V. Bolshedvorskii, V.N. Sorokin, A.V. Akimov // *JETP Lett*. 2018. №108. P. 588.
19. J. Ebel. Dispersive Readout of Room-Temperature Ensemble Spin Sensors / J. Ebel, T. Joas, M. Schalk, P. Weinbrenner, A. Angerer, J. Majer, and F. Reinhard // *Quantum Sci Technol*. 2021. №6, 03LT01.
20. A. Wood. DC Magnetometry below the Ramsey Limit with Rapidly Rotating Diamonds / A. Wood, A. Stacey, A. Martin // *Bulletin of the American Physical Society*. 2023.

# КВАНТОВЫЕ ТЕХНОЛОГИИ НА ОСНОВЕ ЦЕНТРОВ ОКРАСКИ АЗОТ-ВАКАНСИЯ В АЛМАЗЕ

## **Александр Низовцев,**

главный научный сотрудник Центра «Квантовая оптика и квантовая информатика» Института физики им. Б.А. Степанова НАН Беларуси, доктор физико-математических наук

## **Александр Пушкарчук,**

старший научный сотрудник лаборатории ионного обмена и сорбции Института физико-органической химии НАН Беларуси, кандидат физико-математических наук

## **Дмитрий Филимоненко,**

научный сотрудник Центра «Квантовая оптика и квантовая информатика» Института физики им. Б.А. Степанова НАН Беларуси

## **Сергей Килин,**

заведующий Центром «Квантовая оптика и квантовая информатика» Института физики им. Б.А. Степанова НАН Беларуси, академик

В современном мире все более широкое применение находят квантовые технологии второго поколения [1], основанные на практическом использовании *индивидуальных квантовых систем* – атомов, молекул, примесных центров, фотонов и т.п., являющихся физическими носителями *квантовых бит (кубит)*, которые, в отличие от обычных бит  $|0\rangle$  и  $|1\rangle$ , могут находиться в *суперпозиционных состояниях*  $\alpha|0\rangle + \beta|1\rangle$ , а также, в случае нескольких квантовых бит, в *перепутанных состояниях*, которые с учетом принципиально вероятностного характера квантовых измерений и обеспечивают качественно новый уровень квантовых технологий. В ходе их разработки продемонстрированы принципиально новые методы обработки

информации и безопасной ее передачи на большие расстояния, созданы метрологические и сенсорные системы для потребностей нанотехнологий и биомедицины на уровне индивидуальных клеток, мембран, нервных волокон и т.д.

Перспективные объекты для этих целей – одиночные квантовые системы в твердых телах, поскольку для них применим обширный технологический потенциал, накопленный в современной микроэлектронике. В частности, кубитами здесь могут быть *электронные и ядерные спины*, методы управления и манипулирования которыми с помощью микроволновых (МВ) и радиочастотных (РЧ) полей хорошо отработаны в области физики, изучающей электронные парамагнитный и ядерный магнитный резонансы (ЭПР и ЯМР). В системах

взаимодействующих электронных и ядерных спинов электроны играют роль быстрых кубит, а ядерные спины могут хранить квантовую информацию в течение долгого времени, благодаря их исключительно высокой изоляции от окружения. Кроме того, электронные кубиты могут использоваться в качестве интерфейсов с «летающими» кубитами – фотонами. В этом контексте интерес представляют парамагнитные *центры окраски* в твердых телах, которыми, в частности, являются различные дефекты в кристаллах, имеющие локализованные на них электронные состояния с энергетическими уровнями, лежащими в запрещенной зоне, что делает их подобными изолированным атомам или молекулам.

Наиболее известный и активно изучаемый в последние десятилетия представитель таких систем – центр окраски *азот-вакансия* (NV-центр) в алмазе, который состоит из замещающего атома азота (N) и вакансии (V), расположенной в соседнем узле решетки алмаза [2] (рис. 1А). В нем электронным кубитом является спин  $S=1$  NV-центра в основном триплетном электронном состоянии, а ядерными спинами – спин  $I^{(N)}=1$  атома  $^{14}\text{N}$ , принадлежащего NV-центру, и – потенциально – ядерные спины  $I^{(C)}=1/2$  изотопических атомов  $^{13}\text{C}$ , распределенных случайно в решетке алмаза и замещающих бесспиновые атомы  $^{12}\text{C}$  с вероятностью 1,1% (в природных образцах алмаза).

Центр обладает уникальным набором взаимосвязанных фотофизических и спиновых свойств, обеспечивающих оптическую инициализацию элек-

тронного спина  $S=1$  в состоянии с определенной проекцией  $m_S=0$  и считывания его посредством измерения интенсивности испускаемой центром флуоресценции, которая в состоянии  $m_S=0$  на ~30% больше, чем с проекциями  $m_S=\pm 1$ . Сверхтонкие взаимодействия (СТВ) электронного спина NV-центра с ядерными спинами, используемыми в качестве дополнительных кубит, обеспечивают возможность выполнения многокубитных операций с помощью последовательности оптических, МВ- или РЧ-импульсов для инициализации, манипулирования и считывания состояний электронно-ядерных спиновых систем NV- $^{13}\text{C}$ . Стандартно для этих целей применяется конфокальная микроскопия в комбинации с методом оптически детектируемого магнитного резонанса (ОДМР), повышающего чувствительность на ~7 порядков в сравнении с ЭПР, что и делает возможным наблюдение одиночных систем NV- $^{13}\text{C}$  и их применение в квантовой информатике в качестве квантовых регистров и квантовой памяти, реализации квантовой коррекции ошибок при квантовых вычислениях и т.п. Концептуально такие перспективы гибридных систем NV- $^{13}\text{C}$  в алмазе были предсказаны в нашей работе [3]. В настоящее время можно счи-

тать хорошо отработанными методы экспериментальной работы с ними [4]. В частности, недавно была продемонстрирована [5] возможность визуализации, идентификации и когерентного манипулирования 27 различными ядерными спинами  $^{13}\text{C}$ , составляющими специфическое окружение некоторого одиночного NV-центра.

В последние годы активно развивается еще одна область работы с одиночными NV-центрами и их комплексами с ядерными спинами, связанная с их использованием в качестве сенсоров для измерения магнитных и электрических полей, а также температуры и давления с *нанометровым пространственным разрешением* [6]. Физически такие нанометрологические применения основаны на изменении расщепления состояний NV-центра с проекциями электронного спина  $m_S=\pm 1$  (рис. 1Б), величина которого напрямую связана с напряженностями действующих на центр полей. Для биологических приложений исключительно важным является то обстоятельство, что такие измерения можно проводить при комнатных температурах. Кроме того, использование одиночных NV-центров в качестве сенсоров позволяет идентифицировать ядерные спины одиночных молекул, расположенных на поверхности алмаза,

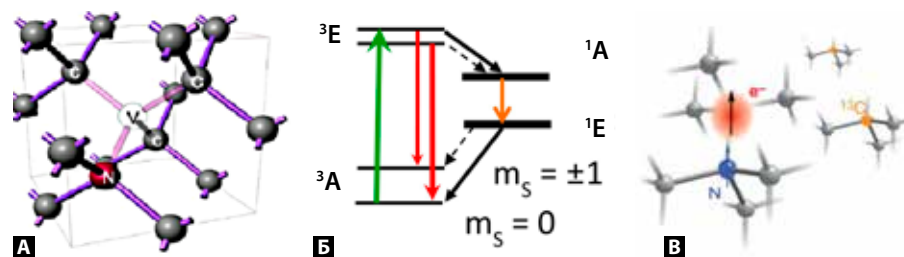


Рис. 1. Структура NV-центра в алмазе (А), энергетические уровни и переходы NV-центра (Б), сверхтонкое взаимодействие NV-центра с ядерными спинами  $^{13}\text{C}$  (В)

что открывает новое чрезвычайно перспективное направление магнитно-резонансной томографии наноразмерных объектов для широкого круга задач (от определения молекулярной структуры неорганических и биологических молекул до визуализации биопроцессов и терапии в медицине) [7].

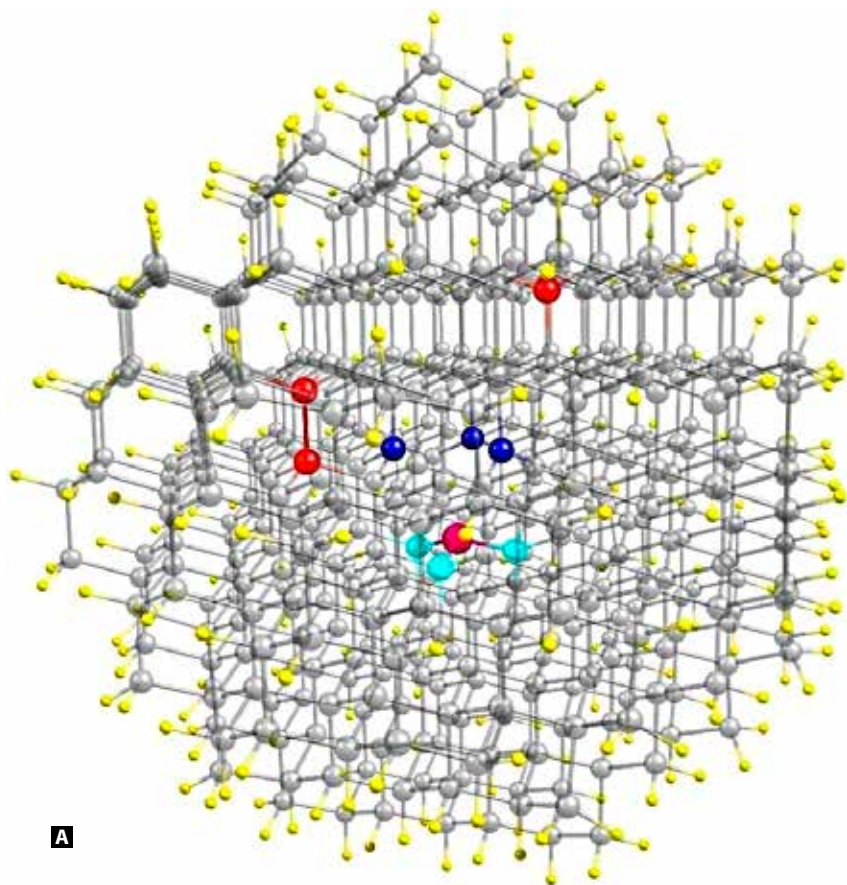
Для всех этих приложений необходимо детально знать характеристики электронно-ядерных спиновых систем  $NV^{13}C$ , их изменений под влиянием внешних воздействий, понимать их динамику под влиянием постоянных или

импульсных оптических, МВ- и РЧ-полей. Наряду с экспериментальным их изучением для этих целей широко применяются современные методы компьютерного моделирования, позволяющие с высокой точностью рассчитывать пространственные, электронные и спиновые характеристики наноразмерных кластеров/суперъядер алмаза, содержащих NV-центры.

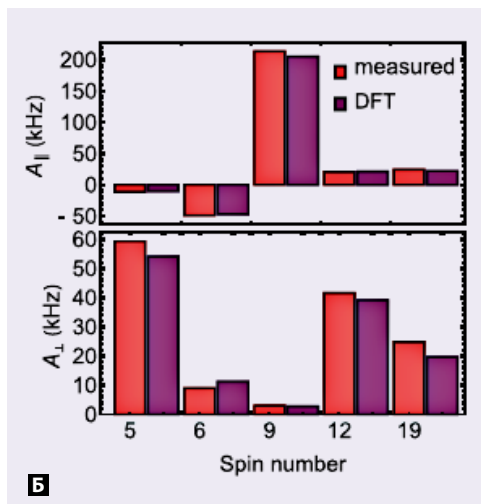
В частности, недавно нами был выполнен [8] систематический расчет матриц  $A_{kl}$ , описывающих СТВ электронного спина NV-центра с различным образом расположенными ядер-

ными спинами  $^{13}C$  посредством моделирования методом функционала плотности пассивированного водородом и содержащего NV-центр кластера алмаза  $C_{510}[NV]-H_{252}$  (рис. 2А). Результаты расчетов хорошо согласуются с данными, полученными экспериментально (рис. 2Б). Используя полученные в [8] расчетные данные в спин-гамльтонианах конкретных систем  $NV^{13}C$ , можно получить практически без подгоночных параметров различные экспериментально наблюдаемые характеристики и зависимости, а также предсказывать оптимальные условия для получения нужных результатов при постановке планируемых экспериментов. Примеры и результаты нашей деятельности в этом направлении кратко представлены ниже.

Для большинства приложений желательно использовать системы  $NV^{13}C$ , в которых ядерные спины имеют большое



**А**



**Б**

Рис. 2А. Изученный в [8] кластер  $C_{510}[NV]-H_{252}$  (А). Атомы углерода показаны серым цветом, атом N-азота NV-центра – фиолетовым, ближайшие к нему атомы углерода – голубым, а ближайшие к вакансии V – синим. Красным цветом выделен некоторый произвольно выбранный одиночный атом  $^{13}C$ , а также димер  $^{13}C-^{13}C$ , входящий в состав изучаемых экспериментально систем. Атомы водорода, пассивирующие оборванные связи на поверхности кластера, показаны желтым цветом

Рис. 2Б. Сравнение экспериментально измеренных в [6] значений элементов  $A_{kl}$  матриц, описывающих СТВ в 5 различных системах  $NV^{13}C$  с соответствующими значениями, предсказанными теоретически в [8]

время когерентности. Одним из важных механизмов нарушения когерентности ядерных спинов выступают их стохастические перевороты, инициируемые анизотропной составляющей СТВ, описываемой недиагональными элементами матриц  $A_{KL}$  СТВ. Экспериментальный поиск стабильных спиновых систем NV- $^{13}\text{C}$  осуществляется обычно рутинным перебором большого количества различных систем NV- $^{13}\text{C}$ . До недавнего времени считалось, что стабильны только NV- $^{13}\text{C}$  системы с расположением ядерного спина  $^{13}\text{C}$  на оси симметрии  $C_{3V}$  NV-центра, поскольку матрица СТВ является диагональной, и ось квантования ядерного спина всегда параллельна оси NV-центра. В [8] на основе использования найденных матриц СТВ был выполнен систематический расчет индуцированных СТВ скоростей переворотов ядерных спинов в кластере  $C_{510}[\text{NV}]-\text{H}_{252}$  и впервые было предсказано наличие большого количества неосевых стабильных систем NV- $^{13}\text{C}$ , в которых ядерные спины  $^{13}\text{C}$  расположены в бислое алмаза, перпендикулярном оси NV-центра.

Согласно сделанным в [8] предсказаниям, для большинства систем NV- $^{13}\text{C}$  анизотропная составляющая СТВ не является малой. Это обстоятельство можно использовать для управления состояниями ядерных спинов  $^{13}\text{C}$  в системах NV- $^{13}\text{C}$ , в которых обычно манипулирование электронным спином NV-центра осуществляется с помощью коротких импульсов МВ-излучения, а ядерным спином  $^{13}\text{C}$  – с помощью РЧ-импульсов, вынужденно имеющих существенно большую длительность вследствие малости

магнито-дипольного переходного момента ядерного спина. В [9] на основе численного моделирования нестационарной динамики систем NV- $^{13}\text{C}$  под действием МВ-импульсов было показано, что можно эффективно манипулировать ядерными состояниями системы с помощью только МВ-импульсов, обладающих характеристиками (отстройка частоты и частота Раби), при которых имеют место резонансы в спиновой системе, «одетой» микроволнами. На основе рассчитанных в [8] матриц СТВ мы численно проанализировали динамику ряда конкретных спиновых систем NV- $^{13}\text{C}$  и нашли оптимальные характеристики МВ-импульсов, выполняющих с высокой вероятностью (~1) переворот ядерного спина  $^{13}\text{C}$ .

Недавно была реализована [10] идея получения наноразмерных алмазов с NV-центрами в результате роста из затравки, в качестве которой используются алмазоподобные молекулы азаадамантана  $C_9H_{15}N$ . Химическими методами можно создавать такие прекурсоры с замещением в них в определенных позициях обычных бесспиновых атомов  $^{12}\text{C}$  изотопическим углеродом  $^{13}\text{C}$ . Это позволит выращивать нанокристаллы алмаза, содержащие спиновые системы NV- $^{13}\text{C}$  с заданным расположением ядерных спинов  $^{13}\text{C}$  относительно NV-центра. Контролировать результаты такого роста и устанавливать корреляции полученных спиновых систем NV- $^{13}\text{C}$  с исходным прекурсором можно посредством измерения спектров ОДМР. При этом в качестве индикатора для идентификации различных систем NV- $^{13}\text{C}$  может применяться величина индуцирован-

ного СТВ расщепления подуровней  $m_s = \pm 1$  NV-центра в нулевом магнитном поле, которая зависит от взаимного расположения атома  $^{13}\text{C}$  и атома N в прекурсор. Очевидно, для этих целей желательно знать эти величины заранее. Такой предсказательный расчет характерных величин индуцированного СТВ расщепления подуровней  $m_s = \pm 1$  NV центра в нулевом магнитном поле выполнен нами в [11, 12] на основе расчетных данных о характеристиках СТВ, полученных в [8] для кластера  $C_{510}[\text{NV}]-\text{H}_{252}$ .

Недавние эксперименты [13, 14] на димерах  $^{13}\text{C}-^{13}\text{C}$  в алмазе с NV-центрами, а также впечатляющий прогресс в увеличении (до ~ Гц) спектрального разрешения односпинового сенсора на основе NV-центра [15] создали запрос на расчет полных тензоров  ${}^nJ_{KL}(K, L=X, Y, Z)$  непрямого, через электроны связей, взаимодействия (так называемый *J-coupling*) ядерных спинов  $^{13}\text{C}$  в алмазе. Недавно такой расчет был впервые выполнен нами [16] посредством моделирования пассивированного водородом кластера алмаза  $C_{35}H_{36}$ , а также аналогичного кластера  $C_{33}[\text{NV}]-\text{H}_{36}$ , содержащего NV-центр. Согласно полученным результатам, центр влияет на ближайшие к нему ядра  $^{13}\text{C}$ , что приводит к существенному изменению характеристик их непрямого взаимодействия со своими соседями. Расчетные данные о тензорах  ${}^nJ_{KL}$ , дополненные данными работы [8] о характеристиках СТВ различных ядерных спинов  $^{13}\text{C}$  с NV-центром, а также о пространственном расположении ядерных спинов  $^{13}\text{C}$  относительно NV-центра (рис. 1А),

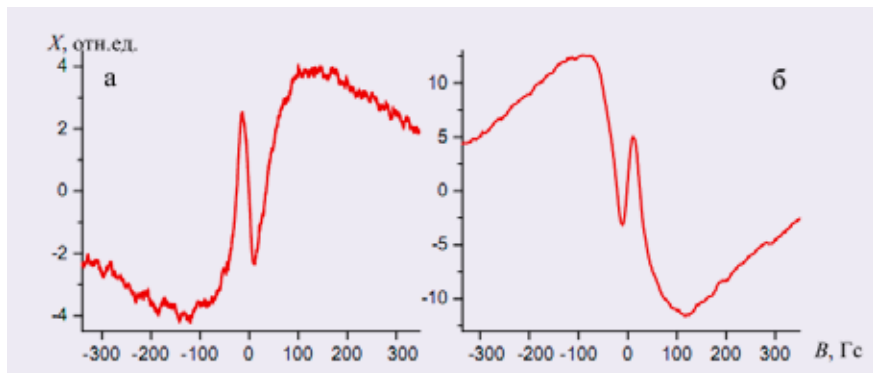


Рис. 3. Магнитные спектры ансамбля NV-центров в микрокристалле алмаза в инфракрасном (ИК) (а) и видимом диапазоне (б)

были использованы нами [17] в спин-гамилтониане конкретной тестовой системы  $NV-^{13}C-^{13}C$  для анализа возможности создания димера  $^{13}C-^{13}C$  в синглетном состоянии, которое перспективно в качестве долгоживущей квантовой памяти [14, 18]. Для рассмотренной системы найдены характеристики МВ и РЧ-импульсов, обеспечивающие перевод димера  $^{13}C-^{13}C$  в синглетное состояние.

Как отмечалось выше, обычно магнитометрические измерения с помощью NV-центров выполняются на основе измерения и последующего анализа спектров ОДМР. В случае использования в качестве сенсоров одиночных NV-центров вследствие симметрии  $S_{3V}$ -центра теряется информация об азимутальном угле вектора магнитного поля. Недавно нами был проанализирован [19] метод полной векторной магнитометрии, реализуемой с помощью одиночной спиновой системы  $NV-^{13}C$ , имеющей более высокую симметрию  $S_6$ . Метод основан на экспериментальном измерении положений линий в спектре ОДМР и их анализе с учетом априорного знания характеристик СТВ

в такой системе, полученных в [8]. В [19] метод экспериментально апробирован на системе  $NV-^{13}C$ , в которой атом  $^{13}C$  был расположен в третьей координационной сфере NV-центра.

Наряду с одиночными  $NV/NV-^{13}C$  центрами, позволяющими получать сверхвысокое пространственное разрешение благодаря нанометровым размерам сенсора, активно ведутся разработки [20] датчиков, в которых в качестве сенсора используются ансамбли NV-центров, поскольку последние обеспечивают лучшее отношение «сигнал – шум» (правда, за счет пространственного разрешения) благодаря статистическому усреднению по многим спином. Кроме того, поскольку типично в ансамбле NV-центры равномерно распределены по четырем возможным кристаллографическим ориентациям так, что каждая их группа «чувствует» различные проекции магнитного поля, то такие «ансамблевые» сенсоры автоматически обеспечивают измерение всех векторных характеристик внешнего магнитного поля.

Одним из практически важных направлений реализации «NV-ансамблевой» магнитометрии является интегрирова-

ние сенсора с другими (излучательными и регистрирующими) частями измерительной установки с помощью оптоволокна, что позволяет миниатюризировать ее и создать компактные портативные устройства, пригодные для внелабораторного применения. С использованием такого подхода был создан и апробирован [21] квантовый сенсор для высокочувствительной векторной градиентометрии магнитного поля при комнатной температуре. Разработанная методика дифференциальных пространственно-временных ОДМР-измерений позволяет эффективно подавлять шум и обеспечивает чувствительность магнитоградиентометрии на уровне  $10^{-7} \text{нТ}/(\text{нм Гц}^{1/2})$ .


Во всех указанных методах магнитометрия с помощью NV-центров реализовалась посредством измерения и последующего анализа чувствительных к магнитному полю спектров ОДМР. Между тем под действием внешнего магнитного поля происходит не только зеемановский сдвиг спиновых подуровней NV-центров, но и перемешивание их спиновых состояний, которое при оптическом возбуждении приводит к перераспределению заселенностей состояний NV-центров и напрямую влияет на интенсивность фотолуминесценции, испускаемой их ансамблем. Очевидно, данный метод, в котором не используются микроволны, гораздо более практичен с точки зрения затрат, упрощения и компактизации конструкции магнитометра. Следуя этому подходу, в наших работах [22–24] экспериментально и теоретически исследовано влияние внешнего магнитного поля на интен-

сивность флуоресценции ансамбля NV-центров в алмазе.

На рис. 3 представлены магнитные спектры (производные от интенсивности люминесценции X-образца как функции магнитного поля  $B$ ) ансамбля NV-центров в алмазе для области слабых магнитных полей, полученные при регистрации люминесценции в ИК (а) и видимом диапазоне (б) при оптическом возбуждении образца: YAG-лазером с  $\lambda=532$  нм. Амплитуда и форма резонанса определяются концентрацией NV-центров в алмазе, а также мощностью и поляризацией возбуждающего лазерного излучения. Наличие линейного участка (в пределах  $\pm 4$  Гс, с переходом через 0) на дисперсионной кривой, связывающей приложенное магнитное поле с выходом фотодетектора, позволяет использовать этот сигнал для магнитных измерений. С учетом того, что магнитные спектры ансамбля NV-центров для видимого и ИК-диапазона носят противофазный характер, такие измерения можно осуществлять и путем регистрации люминесценции в области наибольшей прозрачности биологических тканей (1–1,5 мкм). Экспериментальные данные хорошо описываются в рамках 8-уровневой фотофизической модели NV-центра [22–24], в которой учтена кросс-релаксация центров с определенной пространственной ориентацией с другими электронными спинами (NV-центрами, имеющими другую ориентацию, спинами замещающих атомов азота и т.п.).

Таким образом, в данной статье представлен краткий обзор результатов компьютерного моделирования характеристик NV-центров в алмазе и их комплексов с ядерными

спинами  $^{13}\text{C}$ , а также использования полученных данных для описания экспериментов и предсказания оптимальных условий реализации различных квантовых технологий на основе алмаза с NV-центрами. Пред-

ставленные результаты получены в рамках выполнения Белорусской государственной программы научных исследований «Конвергенция-2025», задание 3.01, а также при поддержке РНФ, проект 21–42–04416. 

#### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. С.Я. Килин. Впереди времени и технологий // Наука и инновации. 2023. №8. С. 10–17.
2. M. W. Doherty. The nitrogen-vacancy color centre in diamond / M. W. Doherty [et al.] // Physics Reports. 2013. Vol. 528. P. 1.
3. J. Wrachtrup. Quantum computation using the  $^{13}\text{C}$  nuclear spins nearby the single NV defect center in diamond / J. Wrachtrup, S. Ya. Kilin, A. P. Nizovtsev // Оптика и Спектроскопия. 2001. Т. 91. №3. С. 460–467.
4. S. Pezzagna. Quantum computer based on color centers in diamond / S. Pezzagna, J. Meijer // Applied Physics Reviews. 2021. Vol. 8 (1). P. 011308.
5. M. H. Abobeih. Atomic-scale imaging of a 27-nuclear-spin cluster using a single-spin quantum sensor / M. H. Abobeih [et al.] // Nature. 2019. Vol. 576. P. 411.
6. R. Schirhagl. Nitrogen-Vacancy Centers in Diamond: Nanoscale Sensors for Physics and Biology / R. Schirhagl [et al.] // Annu. Rev. Phys. Chem. 2014. Vol. 65. P. 83–105.
7. Y. Wu. Diamond Quantum Devices in Biology / Y. Wu, F. Jelezko, M. B. Plenio, T. Weil // Angew. Chem. Int. Ed. 2016. Vol. 55. P. 6586–6598.
8. A. P. Nizovtsev. Non-flipping  $^{13}\text{C}$  spins near NV center in diamond: Hyperfine and Spatial Characteristics by Density Functional Theory Simulation of the  $\text{C}_{510}[\text{NV}]\text{H}_{252}$  Cluster / A. P. Nizovtsev [et al.] // New J. Phys. 2018. Vol. 20. P. 023022.
9. А.П. Низовцев, С.Я. Килин. Микроволны для эффективного манипулирования ядерными спинами в системах NV- $^{13}\text{C}$  в алмазе / А.П. Низовцев, С.Я. Килин // Известия РАН, серия физическая. 2020. Т. 84. №3. С. 310–316.
10. M. Alkahtani. Growth of high-purity low-strain fluorescent nanodiamonds / M. Alkahtani [et al.] // ACS Photonics. 2019. Vol. 6. P. 1266.
11. A. P. Nizovtsev. Hyperfine Characteristics of Quantum Registers NV- $^{13}\text{C}$  in Diamond Nanocrystals Formed by Seeding Approach from Isotopic Aza-Adamantane and Methyl-Aza-Adamantane / A. P. Nizovtsev [et al.] // Semiconductors. 2020. Vol. 54. №12. P. 1689–1691.
12. A. P. Nizovtsev. Hyperfine interactions in the NV- $^{13}\text{C}$  quantum registers in diamond grown from the azaadamantane seed / A. P. Nizovtsev [et al.] // Nanomaterials. 2021. Vol. 11. P. 1303.
13. M. H. Abobeih. One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment / M. H. Abobeih [et al.] // Nat. Commun. 2018. Vol. 9. P. 2552.
14. H. P. Bartling. Entanglement of Spin-Pair Qubits with Intrinsic Dephasing Times Exceeding a Minute / H. P. Bartling [et al.] // Phys. Rev. X. 2022. Vol. 12. P. 011048.
15. S. Schmitt. Submillihertz Magnetic Spectroscopy Performed with a Nanoscale Quantum Sensor / S. Schmitt [et al.] // Science. 2017. Vol. 356. P. 832–837.
16. A. Nizovtsev. Simulation of Indirect  $^{13}\text{C}$ - $^{13}\text{C}$  J-Coupling Tensors in Diamond Clusters Hosting the NV Center. A. Nizovtsev [et al.] // Mater. Proc. 2022. Vol. 9. P. 4.
17. А.П. Низовцев. Квантовая память на димерах  $^{13}\text{C}$ - $^{13}\text{C}$  в алмазе с NV-центрами: моделирование методами квантовой химии / А.П. Низовцев [и др.] // ЖПС. 2023. Т. 90. №5.
18. Q. Chen. Steady-state preparation of long-lived nuclear spin singlet pairs at room temperature / Q. Chen, I. Schwarz, M. B. Plenio // Phys. Rev. B. 2017. Vol. 95. P. 224105.
19. А.П. Низовцев. Векторная магнитометрия с помощью одиночного комплекса NV- $^{13}\text{C}$  в алмазе / А.П. Низовцев [и др.] // ЖПС. 2022. Т. 89. №6. С. 807–814.
20. E. Bauch. Sensitivity optimization for NV-diamond magnetometry / E. Bauch [et al.] // Rev. Mod. Phys. 2020. Vol. 92. P. 015004.
21. S. M. Blakley. Fiber-optic vectorial magnetic-field gradiometry by a spatiotemporal differential optical detection of magnetic resonance in nitrogen-vacancy centers in diamond / S. M. Blakley [et al.] // Optics Letters. 2016. Vol. 41. P. 2057–2060.
22. D. S. Filimonenko. Weak magnetic field resonance effects in diamond with nitrogen-vacancy centers / D. S. Filimonenko [et al.] // Semiconductors. 2018. Vol. 52, №14. P. 1865–1867.
23. D. S. Filimonenko. Weak magnetic field effects on the photoluminescence of an ensemble of NV centers in diamond: experiment and modelling / D. S. Filimonenko [et al.] // Semiconductors. 2020. Vol. 54. P. 1730–1733.
24. Д.С. Филимоненко. Проявления в ИК-люминесценции процессов кросс-релаксации NV-центров в слабых магнитных полях / Д.С. Филимоненко [и др.] // ЖПС. 2021. Т. 88. №6. С. 858–871.

# МАТЕМАТИЧЕСКИЕ АСПЕКТЫ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ



**Геннадий Матвеев,**  
доцент факультета  
прикладной математики  
и информатики БГУ,  
кандидат физико-  
математических наук

Криптография, представляющая собой практику безопасного общения, предполагает использование математических алгоритмов для преобразования обычного текста в нечитаемый, зашифрованный формат. После чего он пересылается через сеть Интернет, и расшифровывается получателем в обычный текст с помощью ключа.

## Преимущества криптосистем с открытым ключом

Понять, что такое криптография, позволяет следующий пример. Алиса и Боб – имена условных персонажей, которые хотят обмениваться сообщениями так, чтобы их содержание оставалось в секрете. Очевидно, что у каждой из сторон должен быть свой ключ. На практике используются два вида криптосистем. К первому относятся симметричные криптосистемы. При этом для шифрования и расшифровывания при-

меняется один и тот же криптографический ключ, который должен храниться в секрете обеими сторонами. Алгоритм шифрования выбирается ими до начала обмена сообщениями. Однако если этот ключ будет скомпрометирован, всякая попытка защитить секретную информацию с его помощью потеряет смысл.

Криптосистема с открытым ключом – это асимметричная схема, в которой применяется пара ключей: открытый (public key), с помощью которого зашифровывают данные, и соответствующий ему

закрытый (private key), который применяют при расшифровке. Алиса размещает свой открытый ключ в открытом доступе, в то время как закрытый держит в тайне. Любой человек с копией ее открытого ключа может зашифровать информацию, которую только она и сможет прочитать. Это могут сделать даже люди, с которыми она прежде никогда не встречалась. Для более детального знакомства с этими и другими криптографическими понятиями можно рекомендовать книгу [2].

Исследования по основным направлениям современной криптографии ведутся с 2000 г. в НИИ прикладных проблем математики и информатики БГУ под руководством академика НАН Беларуси Юрия Харина.

Хотя ключевая пара математически взаимосвязана с помощью некоторого уравнения, вычислить закрытый ключ, владея данными об открытом, должно быть практически невыполнимо. Современная математика умеет решать такие задачи. Каждый, у кого есть ваш

открытый ключ, сможет зашифровать данные, но только пользователь, обладающий соответствующим закрытым ключом, может прочитать сообщение.

Главное преимущество асимметричного шифрования в том, что оно позволяет лицам, не имеющим предварительной договоренности о безопасности, обмениваться конфиденциальной информацией. Таким образом, Алисе и Бобу не надо согласовывать секретный ключ по специальному защищенному каналу. Все коммуникации затрагивают только открытые ключи, тогда как закрытые хранятся в безопасности. Примерами криптосистем с открытым ключом являются RSA (названная в честь изобретателей Рона Ривеста, Ади Шамира и Леонарда Адлемана) и Elgamal (названная в честь автора – Тахира Эль-Гамала) и др.

Симметричная криптография долгое время была единственным способом пересылки секретной информации, а цена надежных каналов для обмена ключами ограничивала ее применение узким кругом организаций, которые могли себе это позволить. Появление шифрования с открытым ключом стало технологической революцией, предоставившей надежную криптографию широкому кругу пользователей. Для полноты картины перечислим и некоторые недостатки асимметричных алгоритмов.

Они используют более длинные ключи, чем симметричные. Разница при этом довольно существенная. Например, 128-битный симметричный ключ и 2048-битный асимметричный обеспечивают примерно одинаковый уровень безопасности. Асимметрич-

ное шифрование сравнительно медленнее, чем симметричный алгоритм, а также требует больше вычислительных ресурсов. Поэтому оно неэффективно при передаче длинных сообщений. Эта проблема на практике решается с помощью так называемого механизма инкапсуляции ключей (КЕМ).

Его при необходимости должны поддерживать современные стандарты асимметричного шифрования. В связи с этим дадим необходимые пояснения.

Протокол КЕМ относится к классу криптографических алгоритмов, спроектированных для безопасной передачи ключей симметричных криптосистем с помощью криптосистем с открытым ключом. Это вызвано тем, что последние, как уже отмечалось, неудобны для передачи длинных сообщений, и вместо этого используются для обмена симметричными ключами, которыми в итоге шифруется текст. Для этого первоначально был предложен следующий алгоритм:

- генерируется случайное число  $w$  (ключ);
- оно шифруется открытым ключом и отправляется получателю;
- тот расшифровывает его закрытым ключом и восстанавливает симметричный ключ  $w$ .

К сожалению, данный алгоритм имеет ряд недостатков. Например, злоумышленник может отправить свое число, зашифрованное открытым ключом, и затем обмениваться сообщениями с получателем. На практике инкапсулированный ключ защищают от манипуляций путем добавления кода аутентификации.

Более надежный метод использует подход посложнее. В частности, получатель зашифрованного случайного числа  $w$  формирует материал ключа  $y = KDF(w)$  для его последующего шифрования. То же самое делает и отправитель. Key Derivation Function – функция, которая служит для получения секретных ключей из какого-то другого секретного значения для задач защиты информации.

## ЭЦП, проблема факторизации, RSA

Широко применяемая технология электронной цифровой подписи (ЭЦП) основана на современных стандартах асимметричного шифрования и опирается на следующие принципы.

- Разработаны надежные методы шифрования сообщения закрытым ключом так, что прочитать его можно только связанным открытым. При этом механизм шифрования/расшифрования является общеизвестным.

- Если электронный документ расшифрован с помощью открытого ключа, то можно быть уверенным, что он был зашифрован уникальным закрытым. Если документ прочитан благодаря открытому ключу Алисы, то это подтверждает ее авторство: зашифровать данный документ могла только Алиса, поскольку она – единственный обладатель закрытого ключа.

- Можно сгенерировать пару (открытый и закрытый ключи) так, чтобы, зная первый, нельзя было вычислить второй за разумный срок. Алгоритм генерации ключей строго определен и является общеизвестным. При этом каждому открытому ключу

соответствует закрытый. Если, например, Алиса публикует свой открытый ключ, то это означает, что соответствующий закрытый есть только у нее.

- На практике шифровать документ целиком весьма затратно, поэтому шифруется только его хеш-значение, то есть небольшой объем данных, жестко привязанный к документу с помощью математических преобразований и идентифицирующий его. Механизм хеширования строго определен и является общеизвестным. Шифрованное хеш-значение и является электронной подписью.

Термины «цифровая подпись», «электронная подпись» и «ЭЦП» – синонимы. Данное понятие было впервые предложено в 1976 г. У. Диффи и М. Хеллманом, хотя это была всего лишь идея. Годом позже был разработан алгоритм RSA, который без дополнительных модификаций можно использовать для создания цифровых подписей. Вскоре после RSA разработали другие ЭЦП, такие как алгоритмы цифровой подписи М. Рабина и Р. Меркла.

Стойкость всякой схемы ЭЦП и асимметричного шифрования основана на вычислительной сложности некоторой математической задачи. Для RSA это факторизация целого числа. Определенно можно сказать, что при наличии ее эффективного алгоритма не составит труда найти секретный ключ RSA.

Неизвестно, есть ли эффективный неклассический алгоритм факторизации целых чисел. Однако доказательств того, что не существует решения этой задачи за полиномиальное время, также нет. Первая большая распределенная

факторизация касалась числа RSA-129, имеющего 129 десятичных знаков (426 бит). В 1977 г. его использовали Р. Ривест, А. Шамир и Л. Адлеман, зашифровав фразу из нескольких слов. Они утверждали, что на расшифровку понадобится триллионы лет, однако ключ к самому сложному на тот момент шифру был найден за 17 лет. Над дешифрованием работали 600 ученых и добровольцев на 5 континентах при помощи 1600 компьютеров. Это число было разложено на два сомножителя в период с сентября 1993 г. по апрель 1994 г. Фактической целью этого проекта было стимулирование изучения проблемы факторизации больших чисел и надежности RSA-криптосистемы в частности.

## Квантовые вычисления

Впервые они были предложены независимо Ю.И. Маниным и Р. Фейнманом в начале 1980-х гг. для моделирования сложных квантово-механических систем [1, 5].

Оказалось, что квантовые вычисления могут дать значительное ускорение для решения ряда сложных математических задач, таких как факторизация чисел и дискретное логарифмирование. В 1994 г. П. Шор разработал алгоритм, способный справиться с этими задачами. Он имеет полиномиальную сложность для разложения числа на простые множители и дискретного логарифмирования на квантовом компьютере [6].

В отличие от обычных устройств, работающих на основе полупроводниковых технологий, мощность квантовых значительно выше. Их воз-

можности превосходят любые инструменты, которые сегодня применяют хакеры. Квантовый компьютер использует вместо классических битов (бинарных переменных, единиц и нулей) кубиты – систему с двумя уровнями. Они, в отличие от битов, могут находиться в состоянии 0, 1 и в суперпозиции 0 и 1. На практике это означает, что при наличии квантового компьютера из приблизительно 3 тыс. кубитов криптографическая система RSA с ключом длиной 2048 битов может быть эффективно взломана за время, лишь ненамного превосходящее то, что требуется для шифрования. Это стало существенной проблемой для криптографии, так как безопасность распространенных стандартизированных систем зависит от сложности решения задач разложения числа на простые множители и дискретного логарифмирования.

Квантовые вычисления могут применяться не только в криптографии. С их помощью эффективно решается ряд алгоритмических задач в алгебре, а также предложен протокол генерации общего ключа на квантовом компьютере. Уточним, что лучший классический алгоритм факторизации числа  $N$  требует времени, экспоненциально зависящего от  $n$ , где  $n = \log N$ , а алгоритм Шора [6] на квантовом компьютере – полиномиально зависящего от  $n$ , а именно  $O(n^2 \log_2 n (\log_2 \log_2 n))$  операций. Отсюда следует возможность экспоненциального ускорения решения проблемы факторизации: на квантовом компьютере для компрометации схемы RSA вместо тысяч лет потребуется несколько часов, дней,

недель, месяцев. Разумеется, сказанное носит пока условный характер, а станет актуальным лишь с появлением работающих квантовых компьютеров.

Для более детального знакомства с квантовыми вычислениями можно рекомендовать книгу [3].

Задача дискретного логарифмирования, как и задача факторизации большого натурального числа, – одна из основных вычислительно трудных, на которых базируется современная криптография. Это обусловлено предположительно высокой сложностью обращения дискретной показательной функции. Хотя задача вычисления дискретной показательной функции решается достаточно эффективно, даже самые современные алгоритмы вычисления дискретного логарифма имеют очень высокую степень сложности, которая сравнима со сложностью факторизации целого числа. Классическими криптографическими схемами на основе задачи дискретного логарифмирования являются схема выработки общего ключа Диффи-Хеллмана, схемы электронной подписи Эль-Гамала, DSA, EdDSA и др.

Еще одна возможность эффективного решения задачи вычисления дискретного логарифма связана с квантовыми вычислениями. Теоретически доказано, что с помощью алгоритма Шора он вычисляется за полиномиальное время. Можно утверждать, что в случае, если полиномиальный алгоритм нахождения дискретного логарифма будет реализован, криптосистемы на его основе станут практически непригодными для долговременной защиты данных. Квантовые алгоритмы с начала 1980-х гг.

остаются лишь потенциальной возможностью, которую пока невозможно технически реализовать в полной мере.

Перспектива создания квантовых компьютеров стимулировала Национальный институт стандартов и технологий США (NIST) объявить открытый конкурс по разработке постквантовых криптографических алгоритмов. Точнее говоря, NIST заинтересован в новых стандартах асимметричного шифрования (Public-Key Encryption) и цифровой подписи (Digital Signatures). Основное требование для алгоритмов постквантовой криптографии состоит в том, что они должны быть основаны на задачах с математически доказанной вычислительной сложностью (NP-сложных). Такие алгоритмы называют постквантовыми или квантово-устойчивыми.

Первоначально на участие в конкурсе подали заявки 69 команд со всего мира. Уже проведены три этапа, определены перспективные направления и произведен конкурсный отбор участников.

В настоящее время разработка алгоритмов постквантовой криптографии ведется по 4 направлениям, используемым: теорию решеток (Lattice based cryptography), коды, исправляющие ошибки (Code based cryptography), многочлены в конечных полях (Multivariate, quadratic equations cryptography), теорию хэш-функций для больших данных (Hash-based cryptography).

К асимметричным системам шифрования в рамках конкурса NIST предъявляются требования по обеспечению стойкости к следующим угрозам различения шифртекстов относительно атак на основе:

- *подобранного открытого текста (Indistinguishability Against Chosen Plaintext Attack, IND-CPA);*
- *подобранного зашифрованного текста (Indistinguishability Against Chosen Ciphertext Attack, IND-CCA);*
- *неадаптивно подобранного открытого текста (Indistinguishability Against (non-adaptive) Chosen Plaintext Attack, IND-CPA1);*
- *адаптивно подобранного открытого текста (Indistinguishability Against Adaptive Chosen Plaintext Attack, IND-CPA2).*

## Криптосистема Мак-Элиса

Как показал третий этап конкурса NIST, криптосистема Мак-Элиса Classic McEliece [7] со встроенным кодом Гоппы является одним из кандидатов для последующей стандартизации. Она относится к семейству квантово-устойчивых криптографических алгоритмов, стойкость которых основывается на предположении о вычислительной сложности задачи декодирования случайного линейного кода. В частности, на этой задаче основан не только алгоритм Classic McEliece, но и альтернативные финалисты – алгоритмы BIKE и HQC. Код Гоппы в 1970 г. разработал советский математик В.Д. Гоппа.

Алгоритм Classic McEliece – криптосистема с открытым ключом на основе теории алгебраического кодирования, созданная в 1978 г. Р. Мак-Элисом. Это первая схема, использующая рандомизацию в процессе шифрования. Алгоритм ранее не получил широкого признания в криптографии, но в то же

время является кандидатом для постквантовой криптографии, так как устойчив к атакам на основе алгоритма Шора.

Криптосистема Мак-Элиса строится на тех же принципах, что и криптосистема Г. Нидеррайтера, разработанная последним в 1986 г. и основанная на сложности декодирования полных линейных кодов [8]. Несмотря на то, что данная криптосистема была взломана В. Сидельниковым и С. Шестаковым, некоторые ее модификации остаются криптостойкими [9]. Одна из них лежит в основе алгоритма ВКЕ-2 – альтернативной схеме асимметричного шифрования и цифровой подписи.

Рассмотрим вариант криптосистемы Мак-Элиса [7, 10], который вошел в третий этап конкурса. Основная идея состоит в маскировании линейного кода под код, не обладающий видимой алгебраической и комбинаторной структурой. Есть 2 разновидности данной криптосистемы: основанная на кодах Гоппы и на БЧХ-кодах. В нашем случае алгоритм построения выглядит следующим образом.

Закрытый ключ состоит из:

- матрицы  $G$  размером  $k \times n$ , необходимой для генерации кода Гоппы, исправляющего  $t$  ошибок;
- матрицы перестановок  $P$  размером  $n \times n$ ;
- случайной невырожденной матрицы  $S$  размером  $k \times k$ .

Матрицы  $P$  и  $S$  необходимы для сокрытия структуры открытого ключа, коим является матрица  $G_{pub}$  размером  $k \times n$ , вычисляемая исходя из матриц закрытого ключа:  $G_{pub} = SGP$ . Легко заметить, что в открытом ключе содержится информация о закрытом, но она скрыта. Поэтому невозможно

восстановить по открытому ключу закрытый атакой грубой силы за разумное время.

При шифровании случайным образом выбирается вектор длины  $r$  над полем  $GF(2)$  с весом Хэмминга не более  $t$ . Затем идет вычисление шифртекста:  $C = mG_{pub} + r$ .

Расшифровка производится в три этапа:

- вычисляется вектор  $c' = cG_{pub}^{-1}$ ;
- при помощи алгоритма быстрого декодирования кода Гоппы находится  $m'$ , для которого  $d_H(m'G_{pub}c) \leq t$ ;
- находится открытый текст  $m = m' S^{-1}$ .

Достоинство данного алгоритма состоит в том, что он работает значительно быстрее RSA. Недостатком является большой размер открытого ключа, вследствие чего данная система была ранее мало распространена. Имеется ряд работ, посвященных анализу этой криптосистемы, благодаря чему она считается хорошо изученной.

Геометрические свойства решетки позволяют рандомизировать еще одного участника конкурса NIST – алгоритм NTRU при помощи преобразования  $e = r \otimes h + m \text{mod} q$ .

То есть на определенном этапе используется случайный вектор ошибок  $r$ .

Рандомизация считается преимуществом, поскольку она применяется еще и в системах ВКЕ и SABER.

Современные квантовые компьютеры пока не обладают мощностью, достаточной для взлома систем на основе асимметричного шифрования.

Анализ зарубежной литературы показывает, что полно-

ценный квантовый компьютер можно ожидать лишь в ближайшие десятилетия, а первые случаи квантовых атак могут быть зафиксированы примерно в 2030 г. Наиболее уязвимыми к подобным угрозам считаются персональные и финансовые данные, а также данные, касающиеся блокчейн-экономики [4].

Большинство зарубежных экспертов оценивают квантовую угрозу как реальную. Поэтому назрела необходимость привести систему криптографической защиты информации республики в соответствие с новыми постквантовыми требованиями. Недавно завершившийся международный конкурс постквантовых криптографических алгоритмов выявил общие схемы построения надежных квантово-устойчивых криптосистем, а значит, непреодолимых препятствий для их разработки не существует. ■

#### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Манин Ю. И. Вычислимое и невычислимое / Ю. И. Манин. – М., 1980.
2. Харин Ю. С. Криптология: учебник / Ю. С. Харин, С. В. Агиевич, Д. В. Васильев, Г. В. Матвеев. – Минск, 2013, 2023.
3. Квантовая криптография: идеи и практика / под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. – Минск, 2008.
4. И. Голдовский. Постквантовая криптография. Готовимся сегодня? // ПЛАС. 2023. №2 (288).
5. Bernstein D., Lange T. Post-quantum cryptography // <https://doi.org/10.1038/nature23461>.
6. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring. In Proc. 35th Ann. Symp. on Foundations of Computer Science (FOCS'94) 124–134 (IEEE, 1994).
7. McEliece R.J. A Public-Key Cryptosystem based on Algebraic Coding Theory. Deep Space Network Progress Report. P. 42–44.
8. H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory (англ.) / H. Niederreiter // Problems of Control and Information Theory. 1986. Vol. 15. Iss. 2. P. 159.
9. V.M. Sidelnikov, S.O. Shestakov. On insecurity of cryptosystems based on generalized ReedSolomon codes // Discrete Mathematics and Applications. 1992. №2 P. 439–444.
10. E. Persichetti. Code-based Key Encapsulation from McEliece's Cryptosystem // arXiv:1706.06306v1, Jun. 2017.

# ДОВЕРИЕ К ТЕХНОЛОГИЯМ

Криптография как наука о защите информации насчитывает тысячелетия своего развития. Системы шифрования сообщений существовали еще у древних цивилизаций – в Египте, Китае, Греции и Риме. В средние века появились новые шифры и коды, которые использовались для дипломатической переписки и переговоров, передачи секретных сведений. В конце XIX в. все большую роль в криптографии стала играть математика, что привело к зарождению математической криптографии, а компьютерные технологии подтолкнули последующее усовершенствование методов шифрования и криптоанализа. Разработанный алгоритм открытого ключа, получивший название алгоритма Диффи-Хеллмана, был дополнен криптосистемой Ривеста-Шамира-Адлемана, что позволило не только шифровать сообщения, но и подписывать их с помощью закрытого ключа.

С развитием технологий и потребностей в безопасности данных криптография продолжает свое победное шествие. Так, принципы квантовой механики стали базой квантовой криптографии, которая, основываясь на квантовых явлениях, таких как квантовая суперпозиция и квантовая измеримость, защищает от перехвата информации, обнаруживает любые попытки взлома. Можно сказать, что сегодня это важный инструмент обеспечения безопасности государственных, персональных и финансовых данных, промышленных и научных секретов. Действительно ли квантовая криптография – критически важный аспект защиты от различного уровня информационных угроз и рисков? В чем ее преимущества и недостатки, каковы перспективы? На эти и другие вопросы мы попросили ответить специалистов центра «Квантовая оптика и квантовая информатика» Института физики имени Б.И. Степанова НАН Беларуси.



**Дмитрий Хорошко,**  
старший научный сотрудник центра,  
приглашенный научный сотрудник лаборатории  
лазерной, атомной и молекулярной физики  
Национального центра научных исследований  
Франции, доктор физико-математических наук

– Квантовое шифрование для записи передаваемого символа состоит в использовании так называемых взаимно дополнительных физических величин. Каждая из них требует определенной настройки измерительного аппарата для распознавания ее значения. Если он настроен на измерение величины  $Q$ , а значение передаваемого символа несет дополнительная к ней величина  $P$ , то показание аппарата будет случайным, никак не связанным с  $P$ . Таким образом, квантовое шифрование происходит на уровне физического носителя информации, которым, как правило, выступает импульс света в оптической линии связи. Примерами взаимно дополнительных физических величин являются частота и время прибытия отдельного фотона, линейная и круговая поляризация света и т.п. Квантовое шифрование дает доступ к записанному символу только тому участнику, чей аппарат настроен на измерение правильной физической величины. Фундаментальное свойство неклонирования квантовых объектов не позволяет создать две копии исходного носителя квантовой информации для того, чтобы измерить величину  $Q$  у одной и  $P$  – у другой. Следствием квантового принципа дополнительности является также искажение величины  $Q$  при измерении  $P$  и наоборот. Таким образом, любой перехват информации, записанной с использованием квантового шифрования, во-первых, дает результат только при случайном совпадении измеряемой величины с величиной записи, и во-вторых, вносит искажения в передаваемый сигнал

каждый раз, когда эти величины не совпадают. В технологии, известной как квантовое распределение ключей, это позволяет установить верхнюю границу информации  $J$ , доступной для перехвата, по уровню ошибок и потерь в оптической линии связи. В том случае, когда эта информация не превышает информацию  $I$ , переданную за сеанс связи, пользователи могут создать криптографический ключ длины  $K=I-J$ . Основные области приложения квантового шифрования – те, в которых применяется криптография с открытым ключом: распределение ключей, цифровые подписи, электронное голосование.

– *Дмитрий Борисович, не могли бы вы очертить горизонты развития квантовых технологий для криптографии?*

– Современная криптография успешно справляется с задачей защиты информации от угроз, существующих сегодня, однако развитие информационных технологий требует постоянного обновления ее методов. Основной вид криптографии нашего времени – криптография с открытым ключом, основанная на так называемых односторонних функциях  $y=f(x)$ , которые требуют малого числа шагов алгоритма для вычисления  $y$  по известному  $x$ , но большого числа этих шагов для вычисления  $x$  по известному  $y$ . Понятия «малого» и «большого» в данном контексте имеют строгие значения – полиномиальный и экспоненциальный законы роста числа шагов при увеличении длины числа  $x$  в двоичной записи. Эта длина подбирается таким образом, чтобы вычисление прямой функции занимало доли секунды, а обратной – большой временной промежуток, за который секрет успеет устареть, например сотни лет. С ростом вычислительной мощности обычных классических компьютеров длину блока необходимо увеличивать, чтобы держать время вычисления обратной функции на уровне



времени устаревания секрета. При этом работа с блоками большей длины не представляет серьезной проблемы ввиду возросшей вычислительной мощности ЭВМ. Основные угрозы для криптографии будущего связаны с развитием теории чисел, которое может привести к открытию более быстрых алгоритмов расчета обратных функций, и с появлением универсальных квантовых компьютеров, когда все современные односторонние функции становятся «двусторонними», так как расчет прямой и обратной функций занимает одинаково «малое» число шагов квантового алгоритма. Потенциально существует два решения проблемы защиты информации в грядущую эпоху. Первое известно как постквантовая криптография и состоит в поиске новых односторонних функций, но представляется временным, так как в любой момент могут возникнуть новые квантовые алгоритмы для быстрого обращения этих функций. Второе решение дают те же квантовые информационные технологии, что привели к созданию квантовых компьютеров. Оно называется квантовой криптографией и основано на квантовом шифровании, которое обеспечивает безусловную защиту информации в том смысле, что она не ставит условием ограниченность вычислительной мощности противника.

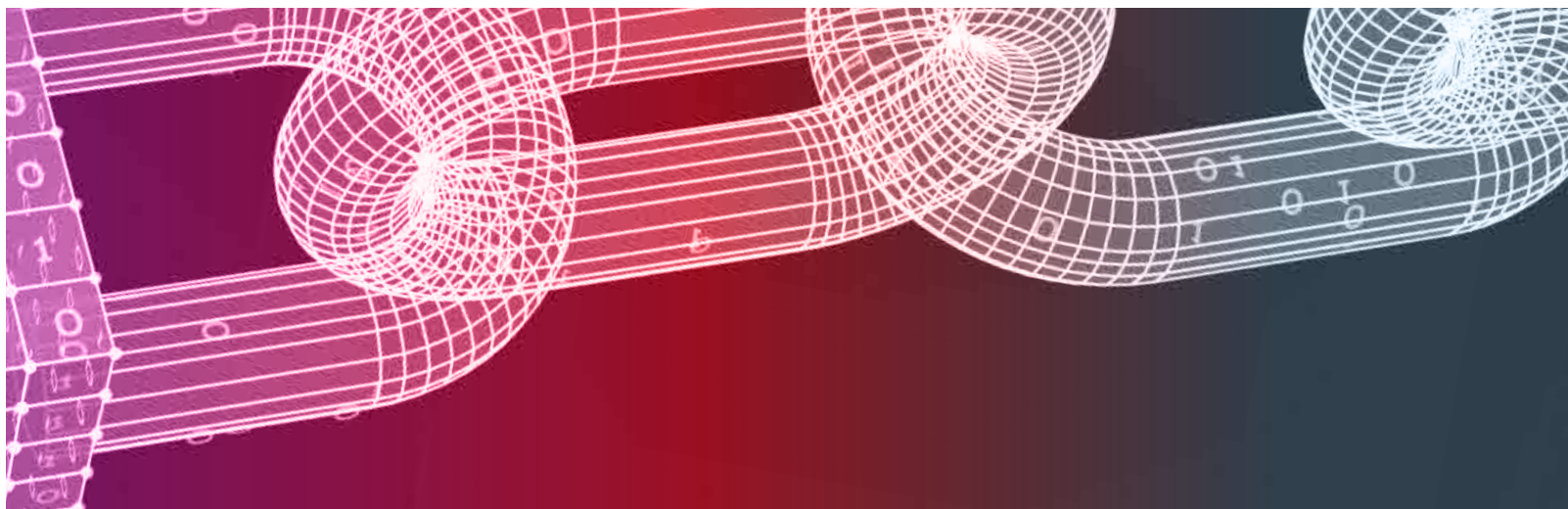
— Насколько широко и где используется квантовая криптография?

— Из всех ее разновидностей только квантовое распределение ключей получило массовое применение. Оптоволоконные линии связи, обеспечивающие генерацию безусловно защищенных ключей на дистанции порядка 100 км, доступны на рынке от производителей из Швейцарии, США, Франции и других стран. Основными покупателями являются частные компании, желающие обезопасить свои коммуникации от атаки в будущем, когда квантовые

компьютеры смогут расшифровывать криптограммы, созданные на основе криптографии с открытым ключом. Эти криптограммы можно без особого труда перехватить сегодня и сохранить для расшифровки в будущем с помощью квантового алгоритма. Компании, оценивающие срок секретности своих коммуникаций выше, чем ориентировочный срок создания универсальных квантовых компьютеров (10–50 лет), — основной потребитель рынка квантового распределения ключей. Другой пример применения квантовой криптографии — квантовые сети, составленные из «доверенных узлов», соединенных оптоволоконными линиями квантового распределения ключей. Они существуют во многих городах мира (например, квантовые сети Бостона, Женева, Вены, Токио, Кембриджа, квантовые линии связи Пекин — Шанхай и Москва — Санкт-Петербург) и, как правило, финансируются научными фондами или правительствами этих стран. Небольшая квантовая линия связи, дальностью до 50 км, была создана и в НАН Беларуси при выполнении задания программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006–2010 гг.».

— Одна из главных проблем существующих криптографических методов — возможность их взлома с ростом вычислительных мощностей, которые становятся все более доступными с каждым годом, а также появление квантовых компьютеров. Не повлияют ли эти факторы на взлом квантовых криптографических систем и существующих криптографических методов и, соответственно, безусловную безопасность? Насколько серьезна эта угроза?

— Квантовая криптография не использует математическое шифрование и, как следствие, совершенно не чувствительна к вычислительной



мощности противника. Качественный перехват в квантовой линии связи реализуется при помощи высокоточного измерения импульсов света, а не решения сложных математических задач. Даже для самых точных измерительных приборов квантовые принципы дополнительности и неклонированности определяют фундаментальный предел количества извлекаемой информации при заданном уровне внесимого шума и потере. Этот предел не может быть превышен с использованием компьютеров любой мощности, в том числе квантовых.

– С какими препятствиями могут столкнуться конечные пользователи?

– Основная проблема современных систем квантового распределения ключей – ограниченная дальность, исчисляемая сотнями километров. Создание крупных сетей с безусловной защитой информации связано с использованием «доверенных узлов», где информация записана обычным классическим образом и может быть скопирована и прочитана противником. Хотя они предполагаются хорошо защищенными от несанкционированного проникновения, сам факт их применения означает, что защита информации больше не основана исключительно на законах квантовой физики, а включает предположение о защищенности узлов. Создание подлинно квантовой сети, в которой сигнал существует в квантовой записи на всем пути от клиента к серверу и обратно, требует разработки квантовых повторителей, способных усиливать квантовый сигнал без его клонирования. К сожалению, прогресс в данной области идет сравнительно медленно, несмотря на наличие проработанного теоретического обоснования подобных устройств. Некоторое неудобство также может быть связано с необходимостью использования волоконно-оптического входа в персональном компьютере для защищенной связи, так как сверхвысокочастотные волны, на которых передается сигнал Wi-Fi, пока не удастся сделать носителями квантовой информации должного качества. Хорошим решением может оказаться технология Li-Fi, обеспечивающая беспроводную связь в помещениях на основе оптической связи через открытое пространство, что позволит естественным образом интегрировать системы квантовой криптографии и беспроводной связи.



**Вячеслав Чижевский,**  
ведущий научный сотрудник Центра «Квантовая оптика и квантовая информатика» Института физики им. Б.И. Степанова НАН Беларуси,  
кандидат физико-математических наук

– Какую функцию в криптографии выполняет квантовая генерация случайных чисел?

– Случайные числа играют важную роль в различных областях науки и техники, и прежде всего в системах защиты информации, в задачах математического моделирования методом Монте-Карло, программировании, в ряде коммерческих приложений. Получение высококачественных случайных чисел критически значимо как для криптографии – математической, стохастической, квантовой, так и в схемах цифровой подписи, алгоритмов шифрования. Они должны обладать свойством истинной случайности, то есть демонстрировать отсутствие каких-либо закономерностей. Для чего, как правило, создаются устройства, в основе работы которых лежат измерения некоторой характеристики физического стохастического процесса с внутренне присущей случайностью и преобразование полученных данных по заданным алгоритмам в последовательность случайных чисел. Существует достаточно большое количество различных физических явлений со сложной динамикой, используемых в качестве источника энтропии для генерации случайных чисел. Прежде всего можно отметить применение хаотической лазерной динамики полупроводниковых лазеров, которые позволяют получить скорости генерации в гигабитном и терабитном диапазоне. Однако подобные генераторы являются устройствами с детерминированной, хотя и сложной динамикой. Это ограничивает их применение для криптографических систем, где противник может использовать суперкомпьютер для расчета этой сложной динамики, установления закономерности в числовой последовательности и как следствие – раскрытия шифра. Подлинная случайность, которую невозможно просчитать на компьютере, свойственна внутренним качествам квантовых процессов, которые лежат в основе реализации ряда квантовых генераторов случайных чисел. Эти устройства создают случайный битовый поток чисто физических явлений с квантовой неопределенностью. В этом контексте генераторы случайных чисел обладают преимуществом безусловной слу-

чайности, что делает их наиболее востребованными для различных применений, к примеру, в медицинской диагностике, банковском секторе для шифрования финансовых транзакций, квантовой физике для тестирования квантовых систем, в различных приложениях, связанных с искусственным интеллектом, робототехникой и другими технологиями. То есть квантовый генератор случайных битов – физическое устройство, генерирующее последовательность классических бит таким образом, что их значение не содержит никакой информации ни о ранее созданных, ни о последующих битах.

**|** – Существует немало методов генерации случайных бит, в том числе на основе физических и квантовых процессов, блокчейна и пр. Какие из них наиболее востребованы?

– Выбор конкретного метода зависит от требуемой степени случайности, скорости генерации и других факторов, связанных с конкретным применением, большинство из них оптические, хотя есть и неоптические методы, основанные, например, на радиоактивном распаде, электронном шуме элементов электронных схем (резисторы, диоды). Среди оптических реализаций можно отметить такие физические явления, как выбор пути одиночным фотоном на светоделителе 50/50, регистрации времени прихода одиночного или ослабленного до уровня одиночных фотонов лазерного излучения. При этом регистрация фотонов производится с помощью детекторов одиночных фотонов либо массивов детекторов. Наличие мертвого времени и послеимпульсов ограничивает скорость генерации случайных бит с использованием подобных детекторов. Тем не менее она может достигать сотен Мбит/с даже в получаемых на лабораторных установках.

Достаточно большое количество исследований квантовых генераторов случайных бит основано на измерении характеристик квантовых случайных процессов с помощью макроскопических детекторов. К ним можно отнести такие процессы, как вакуумные флуктуации, люминесценция в волоконно-оптическом усилителе, фазовый шум в одномодовых полупроводниковых лазерах, флуктуации излучения светоизлучающих суперлюминесцентных диодов, фазовые флуктуации в спонтанно индуцированном вынужденном комбинационном рассеянии, спонтанное параметрическое преобразование частоты, поляризационный шум в одномодовых вертикально-излучающих лазерах и др. Использование макроскопических быст-

родействующих фотодетекторов позволяет получать скорости генерации значительно выше, чем в работе с дискретными детекторами одиночных фотонов, которые могут достигать десятков Гбит/с.

В последнее время появился ряд коммерческих предложений квантовых генераторов случайных бит, основанных на различных физических принципах, со скоростями генерации от 1 Мбит/с до 1 Гбит/с. Однако, несмотря на значительные успехи в разработке квантовых генераторов случайных бит, дальнейшие исследования направлены на разработку устройств, сочетающих в себе надежность, простоту реализации, высокие скорости, долговечность, низкую стоимость и компактность. Помимо перечисленных свойств, одной из важнейших характеристик квантовой генерации случайных чисел является наличие системы самотестирования генерируемых данных, что позволяет оценивать в реальном масштабе времени энтропию источника случайности и качество генерируемых последовательностей. Это направление исследований – одно из наиболее актуальных в настоящее время. В Центре «Квантовая оптика и квантовая информатика» Института физики им. Б.И. Степанова НАН Беларуси проводились исследования по генерации случайных бит на основе многомодового вертикально-излучающего полупроводникового лазера, в котором интенсивность света на заданной поляризации меняется случайно со временем. В результате был разработан и изготовлен квантовый генератор случайных бит со скоростью генерации до 100 Мбит/с в реальном масштабе времени.

Квантовые генераторы случайных чисел имеют большой потенциал для использования в различных областях, включая криптографию, статистику, моделирование и тестирование программного обеспечения.

Исходя из задач, которые решает квантовая криптография благодаря надежности, базирующейся на использовании фундаментальных законов квантовой механики, она может стать одной из основных технологий будущего в области защиты конфиденциальности информации, в том числе передачи метаданных. Безусловно, сегодня квантовые криптосистемы требуют дорогостоящего оборудования и высокой технической квалификации сотрудников для работы с ними, но возможно, вскоре появятся более простые и дешевые методы реализации квантовых криптосистем, что позволит использовать эту технологию в широком спектре приложений. ■

Жанна КОМАРОВА



### Наша даведка

Яна Шаўчэнка — навуковы супрацоўнік аддзела нарадазнаўства Цэнтра даследаванняў беларускай культуры, мовы і літаратуры (з 2017 г.). Нарадзілася 1 жніўня 1991 г. у г. Наваполацку. Скончыла гісторыка-філалагічны факультэт Полацкага дзяржаўнага ўніверсітэта (2013 г.) па спецыяльнасці «гісторык, выкладчык гісторыі і сацыягуманітарных дысцыплін»; магістратуру Полацкага дзяржаўнага ўніверсітэта па спецыяльнасці «айчынная і ўсеагульная гісторыя» (2014 г.); аспірантуру пры Інстытуце мастацтвазнаўства, этнаграфіі і фальклору Цэнтра даследаванняў беларускай культуры, мовы і літаратуры (2017 г.). Са студэнцкіх гадоў актыўна ўдзельнічае ў палявых этнаграфічных даследаваннях як у складзе навуковых экспедыцый, у тым ліку інтэрнацыянальных (Беларусь — Эстонія), так і самастойна. Аўтарка навукова-папулярнай кнігі «Дзікарослы раслінны свет у традыцыйных уяўленнях і сучасным жыцці беларусаў». Лаўрэат прэміі для маладых навукоўцаў імя акадэміка У.М. Ігнатойскага НАН Беларусі (2022 г.).

# МОЦ КАРАНЁЎ, БЕЗДАНЬ НЯБЁСАЎ

Як маладая беларуская даследчыца расшыфравала наш культурны код праз шолах лістоты

«І насадзіў Бог лес. І насяліў яго птушкамі і звярамі. І толькі потым стварыў чалавека. . .».  
Прыкладна так пачынаюцца некаторыя старадаўнія беларускія паданні, што праз стагоддзі захавалі ў сабе ключ да нашага калектыўнага падсвядомага.

Сёння, калі над Беларуссю часта пануе спёка і веюць небывалыя сухавеі, многія з нас хвалююцца за флору роднай краіны: за лясы, доступ у якія абмежаваны з-за небяспекі пажараў, палі, дзе трэці месяц не можа напіцца жыта, ды і за іх насельнікаў — звяроў і птушак. . . Розум кажа: гэта перажыванні за ўраджай, будучыя цэны на прадукты, біязнастайнасць, магчымасць збіраць суніцы і баравікі. Але душа пытаецца, адкуль ва ўсім гэтым няўлоўная нотка цеплыні. Можа, унутры нас гаворыць голас продкаў, нават калі розум лічыць гэта містычнай выдумкай?



Для шмат якіх пакаленняў людзей тысячы гадоў таму свет пачынаўся з зялёнага акіяну лясоў, які ўвасябляў жыццё ва ўсіх яго праявах: даваў не толькі ежу, вопратку, лекі і дах над галавой, але і абарону ад ворагаў, душэўны спакой, натхненне для вынаходніцтваў і іншых творчых пошукаў.

Ці шмат змянілася? Вобразы раслін дагэтуль з намі на карцінах, сукенках, гербах, нават на айфоне і кампутары, з якіх можна хоць з лесу пісаць любы тэкст. А, галоўнае, паміж намі і раслінамі – усё тая ж «хімія» ва ўсіх сэнсах. Пачынаючы ад літаральнага: дзякуючы абменным працэсам у арганізмах прадстаўнікоў флоры мы можам фізічна існаваць, дыхаючы паветрам з неабходным працэнтам кіслароду. Пра парадаксальную і жыватворную павязь усяго непадобнага – чалавека з дрэвам, біялогіі з культурай, этналогіі з маркетынгам і шмат чым яшчэ – мы пагутарым сёння з навукоўцам, што імкнецца абагуліць тысячагадовыя веды аб раслінах.

## Адзін корань і тры сцяблінкі

Усё пачалося з цікавасці да мінуўшчыны. Яна Шаўчэнка ўпэўнена: сам факт з'яўлення на свет у гістарычна значнай мясцовасці

гэтаму спрыяў: «Уявіце: Наваполацк – адзін з самых маладых беларускіх гарадоў, але побач – самы старэйшы з іх, Полацк. Розніца паміж гадамі іх заснавання – 1958 і 862 – проста каласальная!». Ад асэнсавання гэтай бездані часу літаральна дух захоплівала.

Бацькі, людзі творчыя і адукаваныя, падзялялі захапленне дзяўчынкі. Тага, мастак у музеі гісторыі і культуры, і мама, дырэктар універсітэцкай навуковай бібліятэкі, любілі вандроўкі па родным краі. «У мяне натуральным чынам сфармавалася разуменне, што мы маем вялікі пласт гісторыі, якая павінна быць прэзэнтавана, бо мы не горшыя за іншых – мы ўнікальныя», – успамінае суразмоўца сваё станаўленне, дадаючы, што гэта «заахвоціла заняцца гісторыяй прафесійна».

Калі ў старэйшых класах школы прыйшоў час выбіраць спецыялізацыю, ваганняў не было. Паступленне ў 2008 г. у Полацкі дзяржаўны ўніверсітэт на спецыяльнасць «сусветная і айчынная гісторыя» стала лагічным працягам. Вучылася з вялікім задавальненнем і цікавасцю.

– Пяць гадоў – гэта былі незабыўныя прыгоды. Экспедыцыйныя, – прыгадвае Яна. – Жыццё ў намётах, сустрэчы з вялікай колькасцю інфармантаў... У той перыяд я атрымала свой першы вопыт паля-

вых даследаванняў у якасці этнолага. І, канечне, мяне гэта захапіла. Гэта аказалася менавіта тое, чым я хацела б займацца. Той пласт спадчыны, які адкрыўся для мяне і для маіх калег-навукоўцаў, – проста неабсяжны! І настолькі прыцягальны, што прайсці міма і памяняць накірунак дзейнасці ўжо не ўялялася магчымым.

Паступова два адгалінаванні навуковых ведаў зліліся ў лёсе Яны ў адну плынь, фармуючы з будучага гісторыка яшчэ і этнографа. Адкуль жа ўзялася тэма раслін, калі дзяўчына быццам бы не марыла быць этнабатанікам?

А ўзялася яна з унутранага пачуцця. Паэт бы сказаў: з сэрца.

– Люблю прыроду, – прызнаецца раптам мая суразмоўца і тут жа шукае рацыянальнае тлумачэнне, – магчыма, гэта звязана з дзяцінствам. Я часта магла з бацькам наведваць лес, хадзіць па грыбы, ды і проста паблукваць.

І нападарт: «Прагулкі сярод дрэў – добры такі антыстрэсавы сродак».

Падчас навучання ў Полацкім універсітэце, у 2009 г., у першай сваёй навуковай экспедыцыі (у Докшыцкі раён, удакладняе Яна) адчуванне дзівоснасці і магіі роднай прыроды канчаткова расквітнела. І выклікала жаданне яго растлумачыць навуковымі сродкамі:

– *Калі ты ідзеш да вёскі, крочыш па лясх, па гэтых бязмежных палях – ну немагчыма проста не захапіцца хараством прыроды! Гэта настолькі зацягвае. Калі я выбірала тэму курсавой працы на першым курсе, думала: пра што ж я буду пісаць? І раптам у галаву прыйшла думка: я хачу пісаць пра лес, пра лясную прастору.*

Цікава, што ўслед за лясамі ўзнікла цікавасць да прасторы сакральнай – даследавання святых камянёў і крыніц. Яшчэ праз год Яна вырашыла пісаць работу пра дзікіх жывёл. Дыпломная праца аб'ядноўвала ўсе гэтыя кампаненты ў гістарычным развіцці народнай культуры. Але, працягнуўшы вучобу пасля ВНУ ў аспірантуры Акадэміі навук, маладая даследчыца зразумела, што трэба абіраць больш дакладны напрамак працы.

– *Жывёлы – гэта, канечне, даволі спецыфічны момант, – дзеліцца крытэрыямі выбару Яна. – Іх знайсці складаней, чым расліны, тым больш у дзікай прыродзе (а я вывучала менавіта віды, не акультураныя чалавекам). Паколькі мне было цікава менавіта ў натуральнай сферы, то і вырашыла займацца дзікарослымі раслінамі.*

Выявілася, што ў айчынай этналагічнай навуцы асобныя, не абагульняючы працы на тэму раслін былі і раней. У прыклад Яна прыводзіць даследаванні фалькларыста Вольгі Мікалаеўны Шарай, этнолагаў Леаніда Осіпавіча Мінько, Таццяны Іванаўны Кухаронак, Канстанціна Анатольевіча Шумскага і, канечне, сваёй навуковай кіраўніцы Любові Васільеўны Ракавай, якая вывучала традыцыі агародніцтва. Але папярэднікі

даследавалі асобныя аспекты ўзаемадзення з прыродай.

– *А мне былі цікавыя менавіта расліны, якія знаходзяцца на незасвоенай чалавекам прасторы, – кажа Яна. – Тое, што ён супрацьпастаўляе свайму атачэнню. Вось ёсць хата, агарод – гэта яго жыццёвая прастора, а ёсць, умоўна кажучы, чужое: поле, балота, лес – «тэра інкогніта», нязведанае.*



Працягнуўшы паглыбляцца ў дзікарослыя раслінны свет, навукоўца хутка зразумела: «Сфераў яго выкарыстання – проста процьма: гэта літаральна ўсё, што мы бачым».

– *Я паспрабавала аб'яднаць у адно розныя кірункі, якія да гэтага вывучаліся паасобку. Таму праца сама па сабе атрымалася як бы міждысцыплінарная. Тут спалучыліся і чыста этналагічны аспект, і этнабатаніка, фалькларыстыка, калі вывучаецца вусная народная творчасць, акрамя таго, і лакальныя назвы, мовазнаўства – час ад часу... Гэта вялікі спектр навук. І канечне, гістарычныя метады выкарыстоўваюцца, само сабой зразумела. Я паспрабавала гэта ўсё аб'яднаць.*

## Духоўны бок зямных раслін

Самы грунтоўны кампанент свету флары супадае з найвялікшым ярусам лесу – гэта дрэвы. Са старадаўніх часоў у розных народаў (беларусы не выключэнне) яны былі аб'ектам культуры.

– *Гэта таму, што, па ўяўленнях людзей, дрэвы, дзякуючы вышыні – найбольш набліжаныя да Бога, да боскай сферы, – тлумачыць Яна Сяргееўна. – Лічылася: чым вышэйшае дрэва, тым бліжэй яно да неба. Гэта месца, дзе пражываюць птушкі – божыя істоты. І вось паглядзіце, як цікава. Калі вы ведаеце, у розных народаў свету ёсць матыў пра Сусветнае дрэва як цэнтр Сусвету. Напрыклад, у скандынаўскай міфалогіі – дрэва Ігд-расіль, якое каранямі ўзыходзіць да іншасвету, цэнтральная частка якога – сфера людзей, а вяршыня і крона – боскі свет: птушак, багоў і ўсяго, што*

звышнатуральнае. Уяўленне пра Сусветнае дрэва – элемент фальклору шмат якіх народаў.

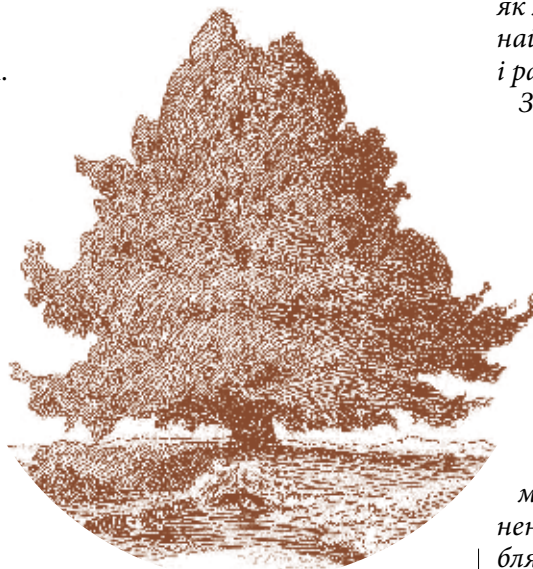
У гэтым рэчышчы выглядае цалкам арганічна, што і ў беларусаў старажытных часоў дуб, самае магутнае дрэва нашых шырот, успрымаўся як увасабленне бога Перуна. У народным мастацтве на доўга захаваўся такі архетып як аб'ект пакланення, і вельмі часта было распаўсюджана ўяўленне аб дубе – «цары дрэваў»... Слухаючы Яну, хочацца дадаць, што і ў сучаснага чалавека пры сустрэчы з гэтым зялёным волатам нярэдка ўзнікае міжвольнае захапленне – мы можам зразу мець пачуцці продкаў і пад панцырам утылітарнай цывілізацыі.

– Частка апавяданняў, легенд і паданняў у беларусаў пачынаюцца з таго, што Бог вырашыў засеяць лес. І такім чынам потым ужо з'яўляліся іншыя лакацыі, але першааснова свету – гэта лес. Дзікарослыя расліны – першае, што чалавек бачыць, калі трапляе ў дзікую прыроду. Дрэвы. Ёсць яшчэ кустоўе, тыя ж самыя ягады, у тым ліку ядомыя, якія мы выкарыстоўваем кожны дзень як ежу.

Духоўная роля раслін цесна пераплецена з матэрыяльным выкарыстаннем. Эзатэрычны свет беларусаў выбудоўваўся на тым, што аб'екты яго пакланення найперш давалі яму само жыццё як магчымасць фізічна існаваць і выжываць, і так з пакалення ў пакаленне.

– Тыя агульнавядомыя ягады, якія чалавек выкарыстоўвае ў ежу, назапашвае – гэта адна катэгорыя. Ёсць, канечне, асобныя часткі раслін і кветкі, якія выкарыстоўваліся ў штодзённасці ў якасці фарбавальнікаў

або, скажам, розных прытраў. Калі паглыбляцца, гэта процьма, процьма розных сфераў выкарыстання. І ў штодзённым побыце ў якасці ежы, у нацыянальнай, народнай кухні. Дэкаратыўнае выкарыстанне я ўжо нават не ўгадваю: у адзенні, дэкоры інтэр'ераў, мэблі. Калі браць драўніну (нават не канкрэтызуючы пра ўжытак асобных відаў дрэва), то ў нас было ўсё зроблена з яе. Хаты, мэбля, посуд, кросны, іншыя прылады працы – фактычна ўся культурная частка чалавечага жыцця.



У той жа час, падкрэслівае даследчыца, рацыянальны аспект непарушна спалучаецца з духоўным. Дзікарослыя расліны выкарыстоўваліся (і нават дагэтуль могуць выкарыстоўвацца) у сямейнай абраднасці: радзіннай, вясельнай, пахавальнай.

– Калі, напрыклад, нараджаецца дзіця, маглі яму пераразаць пупавіну на дрэве: калі нараджаўся хлопчык – на дубу, каб ён быў здаровы і моцны, як дуб.

Ёсць побытавае выкарыстанне дрэва, а ёсць абавязковае рытуальнае, якое звязана з папярэднім. Або з той ж самаю вадой, якую першы раз дзіця абмываюць, калі яно народзіцца – калі гэта дзяўчынка, зліваюць вадку пасля мыцця дзіцяці пад вішню (сімвалічна жаночае дрэва), калі хлопчык, то пад мужчынскае дрэва: дуб, ясьень або явар.

Яна тут жа прыводзіць мне прыклад такога звышцеснага адзінства народных уяўленняў – трэба сказаць, крыху нечаканы:

– Трыпутнік, які мы ведаем (па-руску «подорожник»), выкарыстоўваўся не толькі як лекавы сродак. У Цэнтральнай Беларусі ён быў яшчэ і раслінай, на якую варажылі!

Знаходзілі трыпутнік на раздарожжы і на купальскіх варожбах, калі трэба было даведацца пра свой будучы лёс, свайго суджанага, казалі: «Трыпуце, трыпуце, ты стаіш прыпуце, ты бачыш старога і малага, ці бачыш ты майго мілога?». То бок, расліна выкарыстоўвалася не толькі у народнай медыцыне (тое ж самае спыненне крывацёку), але і ўвасабляла сабой вось такога медыятара, пасрэдніка паміж гэтым светам і тым, невядомым. Тым, які можа дапамагчы даведацца аб сваім будучым лёсе. Беларуская культура вельмі сінкрэтычная па характары. Няма дакладнага размежавання на адну і другую сферы.

## Шэдэўры лістоты і квецені

Выкарыстанне расліннага арнаменту – вельмі яскравая частка беларускай прыкладной мастацкай культуры, падкрэслівае Яна.

І не толькі ў дызаіне знакамітых слупкіх паясоў або рушнікоў, а і ў аздабленні самых розных прадметаў абіходу. «Гэта быў вельмі папулярны дэкаратыўны прыём, – працягвае даследчыца, – адзінае адрозненне – у тым, што ў некаторых рэгіёнах назіраецца большае выкарыстанне расліннага кампаненту, у іншых – меншае».

– Самыя старажытныя элементы дэкору ў народнай творчасці – геаметрычныя: сімвалы зямлі, трохкутнікі, крыжы. Пазней з’яўляецца антрапаморфны арнамент, а таксама ў выглядзе раслін, жывёл. Раслінны арнамент асабліва часта прысутнічае ў упрыгожваннях: на мэблі, куфарах, ліштвах хатаў, не кажучы ўжо пра вопратку і рушнікі. Прычына навідавоку. Гэта тое, што нас атачае, што атачала нашых продкаў, было для іх важным. І, канечне, калі праз усё жыццё праходзіць бясконцы прыродны кампанент, нікуды ад гэтага не дзецца.

Прадстаўнікі расліннага свету – не толькі мастацкі фон, але і нязменныя героі беларускіх песень, казак і паданняў.

– Амаль увесь сямейны цыкл песень, асабліва вясельная лірыка, утрымлівае ў сабе процьму ўзгаданняў пра каліну, маліну, рабіну як вобразы нявесты, маладой, якая робіць крок, пераходны з незамужняга стану ў шлюбны. Вельмі часта сімволіка жаночая у беларускіх песнях прысутнічае ў вобразе «жаночых» дрэў: вішні, ці памятаеце: «шэпчуцца явар з калінаю»... Апошняя цытата – яскравы прыклад уяўлення пра мужчынскую і жаночую сімволіку: явар – дрэва «мужчынскае», а «жаночае» – каліна, вішанька... Гэта больш адносіцца да сямейна-абрадавага фальклору. Але, канечне, імат

і звычайных песень, у якіх даволі часта трапляюцца ў тэксце тыя ці іншыя расліны.

У наш час мастацтва з расліннымі матывамі і матэрыяламі драўніны, лісця, кветак прысутнічае і ў выглядзе сувеніраў і ювелірных вырабаў. Частку іх ствараюць беларускія рамеснікі, упрыгожваючы сваімі творамі турыстычныя лакацыі і ствараючы тым самым непаўторную атмасферу для цікаўных турыстаў.

## Гісторыя з этнаграфіяй

Гаворачы пра навуковыя экспедыцыі ў той або іншы рэгіён нашай краіны, немагчыма абысці тэму параўнальных асаблівасцей этнабтанікі. Напрыклад, я не змагла самастойна ідэнтыфікаваць «заштырыну» – дрэва, кару якога выкарыстоўвалі ў лекавых мэтах на радзіме продкаў, паўзмежку Палесся. Яна Сяргеёўна глумачыць: з народнымі найменнямі дзікарослых раслін не ўсё так проста:

– Тое, пра што вы пытаеце, можа быць рэгіянальнай назвай аднаго з часта выкарыстоўваемых дрэў. І самае цікавае, што ў беларускай мове, увогуле ў беларускай культуры пры даследаванні раслін навукоўцы выдзелілі такую катэгорыю, як расліны-ўніверсалы – найбольш папулярныя, якія лечаць вялікі спектр хвароб. Па народных уяўленнях, адна такая расліна можа вылечыць імат хвароб. Напрыклад, святаяннік (на-руску – «зверабой»). Альбо «крываўнік» (на руску – тысячелистник). Ці «падбел» – гэта «мать-и-мачеха» тая самая. Расліна адна, але ў кожным рэгіёне Беларусі лакальныя назвы могуць адрознівацца: напрыклад,

і «купалка», і «доля», і той жа самы «святаяннік», «зелле святога Яна» – вялікі вельмі арэал.

Яна прыводзіць іншы прыклад: «Расліна, якая лечыць хваробу стрававання, на біялагічны манер называецца «лапчатка прамастойная». Лакальны варыянт назвы – калган. Але калі пералічыць, у гэтай зёлкі ёсць з дзясятка назваў, і ў кожнай мясцовасці можа быць свая. Калган, сурмоліна, узік, вязь-трава... І пры гэтым розныя варыянты назвы ў залежнасці ад таго, дзе яна выкарыстоўваецца». Падобная сітуацыя выяўляецца нярэдка ў адносінах да самых розных траў, хмызьнякоў і дрэў, дадае Яна, таму часам бывае даволі складана высветліць, пра якую траву вядзецца гаворка. «Калі пачнеш у інфарманта выведваць, як яна выглядае, якія ў яе кветачкі, калі цвіце, то чуеш, напрыклад, што «гэта вось такая трава, а гэта вось такая». Здаецца часам, што нават у межах аднаго раёна адной вобласці адна і тая ж расліна называецца па-іншаму. Таму ў вашым выпадку можа быць такое, што гэта было нешта агульнавядомае. Але гэтая варыянтнасць назваў вельмі цікавая як з’ява і гаворыць пра тое, што ў кожным культурным асяроддзі, у кожнай мясцовасці або грамадзе была нейкая свая невялікая традыцыя, звязаная з выкарыстаннем той ці іншай зёлкі, або травы».

## Калі раніца пачыналася не з кавы

Зараз у свеце зрабілася модна пераходзіць на раслінную ежу і духоўныя практыкі, але мала хто ведае, што ў своеасаблівым выглядзе ўсё гэта існавала і ў нашых продкаў – не толькі

беларусаў, але і ўвогуле сла-  
вян альбо балтаў. І гаворка  
не толькі пра хрысціянскія  
пасты (хоць і гэта, канечне, тра-  
дыцыя). Замест цяперашніх  
гарбаты і кавы, якія прыйшлі  
да нас пазней з Усходу і Захаду,  
продкі запарвалі «скрыпень»,  
або «кіпрэй» – мы ведаем яго  
як «иван-чай». У некаторых  
вёсках яго і цяпер выкары-  
стоўваюць як прафілактычны  
сродак. Але ці шмат сучас-  
нікаў ведае, што ў продкаў  
раніца пачыналася з кіпрэю?

– *Культура назапашвання  
беларусамі раслін – гэта куль-  
тура не проста «пайсці, нар-  
ваць і пакласці», а цэлая  
навука, сістэма прадпісан-  
няў: як правільна заходзіць у лес,  
як там сябе наводзіць, як наз-  
біраць расліны, дрэва так, каб  
назапасіць і не прынесці шкоды  
прыродзе, і пры гэтым самому  
прытрымлівацца нейкіх мараль-  
ных і этычных норм, – распа-  
вядзе Яна Сяргееўна. – *Веды  
ў гэтай галіне патрэбныя для  
таго, каб гарманічныя адносіны  
«прырода – чалавек» існавалі  
і сёння, а для гэтага трэба пры-  
цягнуць людзей і да трады-  
цый захавання нашай флары,  
і да традыцый яе выкарыстання.**

Прывіванне людзям любові  
да раслін іграе ролю куль-  
турнага каталізатара, бо гэта  
крок адначасова і да заха-  
вання нацыянальнай культуры,  
і да павышэння экалагічнай  
самасвядомасці (што, безумоўна,  
у інтарэсах краіны і грамадства):

– *Традыцыі абыходжання  
з раслінным светам з’яўляліся  
важнымі складнікамі беларускага  
ладу жыцця, пры якім чалавек  
быў часткай прыроды. Цяжка  
было наводзіць сябе па-за межамі  
таго, як прадпісвала грамада,  
а згодна з яе правіламі, трэба  
было з павагай ставіцца да пры-*

*роды. Гэтану таксама можна  
навучыць і сённяшняю моладзь.*

## Папараць-кветка і глабалізацыя

Традыцыя збору зёлак вельмі  
старажытная яшчэ і таму, што  
з раслінамі былі (і застаюцца)  
звязаны ўсе значныя святы.  
Пачынаючы з Купалля, карані  
якога хаваюцца ў далёкай  
дахрысціянскай даўніне. «*Гэта  
відавочна, – разважае Яна, –  
дзень святога Іаана – на хрыс-  
ціянскі манер, але здаўна гэта  
было свята ўшанавання Сонца.*»

– *Гэта час максімальнага  
роскрытцтва прыроды, калі ноч най-  
больш кароткая ў годзе і самы  
доўгі дзень. Лічылася, што  
менавіта ў дзень летняга сон-  
цастаяння зёлкі атрымваюць  
найвялікшую лекавую моц для  
таго, каб лячыць хваробы. Або  
выкарыстоўваюцца, напрыклад,  
для акурвання хаты ад роз-  
нага негатыўнага ўздзеяння:  
упуду, калі меў месца нядобры  
ўплыў на дзіця, пасля якога яго  
крычыць, не можа супакоіцца.*

З вядомых навуцы рытуаль-  
ных духмянасцяў у беларусаў  
найпапулярнейшым быў палын,  
удакладняе Яна Сяргееўна. Паз-  
ней, з прыходам хрысціянства,  
з гэтай жа мэтай сталі выкары-  
стоўваць грамаднічныя свечкі.

– *Але абкурванне палыном –  
з’ява нашмат больш старажыт-  
ная за хрысціянства. З цягам  
часу адбылося напластаванне  
адных вераванняў на іншыя,  
і разам з уяўленнямі пра лека-  
вую моц зёлак і іх актыўнае  
выкарыстанне стала існаваць  
і павер’е пра дзень святога Іаана  
Хрысціцеля, хоць насамрэч мы  
ведаем, што прырода гэтага  
свята дахрысціянская і звя-  
зана з культуам Сонца, саяяр-  
най сімволікай. Свята і асабліва*

*сакральная ноч лічыліся аса-  
блівай кропкай часу і прасторы –  
паміж гэтым светам і інша-  
светам, калі лёгка магчыма іх  
ўзаемадзеянне з-за таго, што  
мяжа сціралася. Адсюль і гулянні,  
скокі цераз вогнішча, спробы  
змагання з мясцовымі ведзь-  
мамі, якія адваджвалі малако  
ў жывёл, збіранне крапівы, дзя-  
доўніка – гэта ўсё Купалле.*

Што датычыцца пошуку  
самай легендарнай кветкі году,  
то тут усё няпроста. Пачнем  
з таго, што вынікі даследаван-  
няў разбіваюць міф аб тым,  
што папараць-кветка выключ-  
на «наша». Хоць беларусы самі  
сталі падобныя да яе – няўлоў-  
ныя, загадкавыя, каштоўныя  
і неўміручыя ў стагоддзях.

– *Я думаю, што легенда  
пра кветку папараці – агуль-  
ная ўсходнеславянская з’ява,  
а не чыста беларуская, –  
дзеліцца высновамі сураз-  
моўца. – Яна характэрная  
і для ўкраінцаў, ёсць пэў-  
ныя праявы на частцы  
тэрыторыі Расіі.*



Мне падаецца, гэта проста агульны вобраз, звязаны з культурам раслін.

Яшчэ цікавей, што ў купальскай традыцыі расліна надзелена зусім іншым сімвалізмам, чым даследчыкам вядома ў звычайным сэнсе – як адзін з «мужчынскіх» раслінных вобразаў: «Гэта зусім іншая папараць-кветка, якую, як мы ведаем па легендзе, ніхто ніколі не бачыў, ніхто не можа знайсці, а хто знайшоў, тыя назад і не вярнуліся».

Адценне пакланення, характарыстыкі неадназначнай чароўнасці – напэўна, тут любы чытач міжволі прыгадае сюжэтныя павароты твораў Мікалая Гогаля. Яна Сяргеёўна тлумачыць, што гэта нездарма: такі сакральны аспект – «проста квінтэсэнцыя ўшаноўвання расліннага свету – часткі прыроды, якое знайшло ўвасабленне ў такіх вась легендах пра папараць-кветку».

## «Фларысты» маркетынг – рухавік прагрэсу

Адзін з напрамкаў даследаванняў Яны Сяргеёўны – тое, чым яшчэ не займаліся іншыя этнолагі: выкарыстанне народных ведаў пра расліны ў сучаснасці. Аб гэтым яна напісала ў сваёй кнізе. Гэта праца на памежжы этналогіі, гісторыі, этнаэкалогіі. «Як расліны сёння могуць рэпрэзентаваць краіну ў якасці брэндаў і яе папулярна заваць?» – вось тэма пытання, якімі задалася навукоўца.

Як удалы прыклад прыводзіць маркетынгавы ход у час Еўрапейскіх гульніў 2019 г., да якіх спецыяльна выпушчлі марожанае з валошак. «Яно блакітнага колеру ад таго, што дадавалі ў яго экстракт пярэст-

каў валошак, быццам сочыва, і атрымоўвалася блакітнае марожанае, прычым яно раскупалася на «ўра» і стала візітнай карткай спаборніцтваў і краіны, – адзначае мая суразмоўца. – Чым не прыклад таго, як можна выкарыстоўваць расліну, тым больш усім вядомы васільк? Ён настолькі папулярна заваўся і ўвайшоў у менталітэт беларусаў як расліна-маркер, як, можна сказаць, эмблема, звязаная з Беларуссю, што проста немагчыма ўявіць сабе іншае прымяненне».

Сучаснае расліннае брэндзіраванне кампаній асацыятыўна адсылае наведвальніка да беларускай культуры, напрыклад, творчасці Максіма Багдановіча, адзначае Яна: «А вось паглядзіце, нават калі выйдзеце на вуліцу: сетка рэстаранаў нацыянальнай кухні – «Васількі». А што ў нас на эмблеме айчынай авіякампаніі «Белавія»? Таксама васільк, або, па-іншаму, валошка».

Даследчыцу радуе, што ў крамах краіны, а часам і за яе межамі, становіцца ўсё больш беларускіх брэндаў, у прадукцыі якіх так ці інакш «задзейнічаны» тутэйшыя прадстаўнікі флары. Сярод мноства вядомых гандлёвых марак «наўскідку» называе беларускія:

– «Калі ласка» ёсць брэнд, «Белтеа», што выпускае гарбату беларускую, і з дадаткамі – чабарам, васільком, мятай. Вялікі такі працэнт айчынных марак. Раней неяк было не так, а цяпер цікавасць адраджаецца, людзям хочацца паспрабаваць сваё, уласнае. Канечне, гарбата гэта робіцца ў сучасным выглядзе; тое, што мы называем «гарбата», нашы дзяды, продкі проста называлі «чай». Яны валодалі ведамі пра тое, чым можна

вылечыць тую ці іншую хваробу, і такім чынам яны рыхтавалі зборы на кожны выпадак жыцця. І ў гэтым мелі вялікі поспех, таму дагэтуль вельмі папулярна ўжываць расліны ў народнай кухні і медыцыне.

Апафеозам гэтага працэсу навукоўца лічыць магчымасць «вельмі ўдала прэзентаваць краіну, задзейнічаючы раслінныя брэндзі» на яе таварах, якія ўжо сталі пазнавальнымі. «Сучасныя беларускія касметычныя брэндзі больш за ўсіх выкарыстоўваюць раслінныя экстракты, гэта зараз папулярна. Нашы майстры актыўна вырабляюць упрыгожванні на аснове засушаных кветак, лістоў дрэваў. Гэта паўнавартасны і, можна сказаць, цэлы аспект дэкаратыўна-прыкладнага мастацтва. Магчыма ажыццявіць ўсё, на што толькі здатна чалавечая фантазія».

Беларусь як краіна кветак – вобраз амаль казачны, як з дзіцячай мары ці паданняў пра зямлю абетаваную. Напэўна, кожнаму хочацца бачыць сваю Радзіму менавіта такой... Бо іхняе характава – «гэта тое, што з дзяцінства вызывае захапленне ў чалавека», з'яўляецца адной з прыемных частак яго жыцця, звязана з найлепшымі яго момантамі. Таму, лічыць Яна, зусім не дзіўна, што «на кожную расліну знойдзеца свой піар-мэнэджэр».

## Брама неўміручасці

Што чакае Яніну навуку, якая гучыць смачна, як рэцэпт стравы: гісторыю з прысмакам этнаграфіі, прыпраўленую этнабатанікай?

Магчыма, праз сто гадоў людзі будуць вандраваць па галактыках, беражна пера-

возячы з сабой парасткі зялёных сяброў, і наносіць «цвяток радзімы васілька» на борты найноўшых зоркалётаў... Мы, сучасныя дзеці асфальту, не ведаем усяго пра традыцыі мінуўшчыны, і яшчэ менш – пра нашу будучыню.

Але можна сказаць дакладна: Яна Шаўчэнка мае рацыю, кажучы:

*– Традыцыі, што складаліся тысячы гадоў, – гэта культурны «генетычны код», і нельга проста так узяць і вытравіць яго з памяці.*

Яна Сяргееўна ўпэўнена, што рознабаковае вывучэнне ўзаемакарыснага суіснавання чалавека з прадстаўнікамі флоры ніколі не спыніцца: *«Мы заўсёды будзем мець неабходнасць і патрэбу ў раслінах і раслінным свеце. Нягледзячы на тое, што ў нас – век прамысловасці, вялікіх тэмпаў урбанізацыі, калі вытворчасць ужо на хімічны, малекулярны ўзровень пераведзена, усё роўна прырода – тое, адкуль мы выйшлі. І людзі заўсёды будуць мець патрэбу ў ёй, бо гэта першае – тое, адкуль чалавек пайшоў. Таму проста немагчыма пераацаніць значэнне выкарыстання дзікарослых раслін у жыцці як сучасных беларусаў, так і нашых продкаў».*

Праца навукоўцы карысная і ў лакальным, і ў глабальным маштабе. Гаворка ідзе аб захвочванні людзей да захавання духоўнай, культурнай, прыроднай спадчыны. І імідж месца, дзе ты жывеш, пагадзіцеся, нашмат прывабнейшы з валожкамі альбо рамонкамі, чым з рэчамі, якія не нясуць у свет хараство, здароўе і квітнеючае жыццё.

*– Можна паспрабаваць прадставіць нашу краіну, зрабіць такі цікавы яе «партрэт»*

*на міжнароднай арэне: паказаць, што Беларусі насамрэч ёсць чым ганарыцца, што ёсць тысячы відаў раслін, якія могуць зацікавіць гэтай зямлёю і прыцягнуць да яе ўвагу замежных гасцей.*

У нечым наша сённяшня геранія падобная да некаторых сваіх «герояў», напрыклад моцных векавых дубоў (хоць, канечне, і пшчотных бярозак з рабінкамі). Моцна ўросшы каранямі ў родную зямлю, дрэвы не могуць яе пакінуць. Чалавек тэарэтычна можа, але... Яна Шаўчэнка раптам прызнаецца напрыканцы нашай размовы: *«Не ўяўляю жыцця без свайёй краіны».* Уся яе праца пабудавана на вывучэнні традыцый людзей, што жылі і жывуць тут, у Беларусі. І гэтыя веды яна марыць перадаць тым, хто будзе жыць пасля нас – новаму пакаленню вучоных, якія калі-небудзь працягнуць справу папярэднікаў.

## Пра што не ведаў кот Шродынгера. Замест пасляслоўя

Я хачу скончыць свой апошні крыху на іншай ноце. Знакаміты навуковец, вядомы вопытам з катом (уласна, заснаваннем квантавай фізікі і заслужанай Нобелеўскай прэміяй) яшчэ ў 1944 г. зрабіў прадказанне. І датычыцца яно не кветак і раслін, не брэндаў і гісторыкаў, а ўсёй навуцы XXI стагодзя – гэта значыць, ужо цяперашняй.

Шродынгер прадбачыў пашырэнне спецыялізацый навукоўцаў, і не проста як спецыялістаў міждысцыплінарных даследаванняў, але і больш шырокага, мультыдысцыплінарнага профілю. Вучоных,

на яго думку, у нечым будуць падобныя да Леанарда да Вінчы або Эйнштэйна – даследчыкаў, звязаных з мастацтвам, і наадварот – мастакоў, улюбёных у навуку. Як мінімум, яны будуць займацца адразу некалькімі галінамі навук, спалучаючы іх у сваіх даследаваннях, вывучаць з’явы на стыку розных сфер ведаў.

Нешта падобнае мы ўжо назіраем сярод навукоўцаў, асабліва маладых, і ў тым ліку ў нашай краіне. Праца нашай гераніі таксама стаіць у шэрагу прыкладаў, што распачынаюць гэтую з’яву. Маладыя вучоныя – людзі новай фармацыі, выхаваныя на старых акадэмічных традыцыях, і менавіта таму за імі – будучыня. ■

Таццяна ЖДАНОВІЧ





# ДТП с участием диких животных: закономерности и сравнительный анализ



**Павел Гешовт,**  
заместитель генерального директора Научно-практического центра НАН Беларуси по биоресурсам по научной и инновационной работе;  
[heshaut@mail.ru](mailto:heshaut@mail.ru)



**Степан Гузней,**  
заместитель начальника отдела Государственной инспекции охраны животного и растительного мира при Президенте Республики Беларусь;  
[stepan-pd@mail.ru](mailto:stepan-pd@mail.ru)

**Аннотация.** Приведены количественные характеристики и дан сравнительный анализ дорожно-транспортных происшествий с участием диких животных в Беларуси и других странах. Представлены закономерности распределения количества погибших в ДТП копытных по сезонам года, дням недели и половозрастной структуре. Установлено, что местами концентрации аварий такого рода являются участки автомобильных дорог, прилегающие к крупным населенным пунктам, и иные участки с высокой интенсивностью транспортного потока.

**Ключевые слова:** дорожно-транспортные происшествия с дикими животными, методы снижения аварийности, адаптивное управление популяциями.

**Для цитирования:** Гешовт П., Гузней С. ДТП с участием диких животных: закономерности и сравнительный анализ // Наука и инновации. 2023. №8. С. 70–75. <https://doi.org/10.29235/1818-9857-2023-08-70-75>

Дорожно-транспортные происшествия (ДТП) с участием диких животных представляют опасность для людей и приводят к ощутимому материальному ущербу. В результате увеличения интенсивности транспортного потока, сети автомобильных дорог, скорости движения, а также плотности населения копытных как в Европе, так и в Северной Америке

наблюдается увеличение количества таких ДТП. По экспертным оценкам, на территории Европейского союза общее количество копытных, ежегодно погибающих на дорогах, составляет около 1 млн особей, а в США – более 1,5 млн [1].

Достаточно сложно дать точную оценку масштабу проблемы, так как официальная статистика ведется только в некоторых странах Европы. Так, в 2022 г. в Германии в резуль-

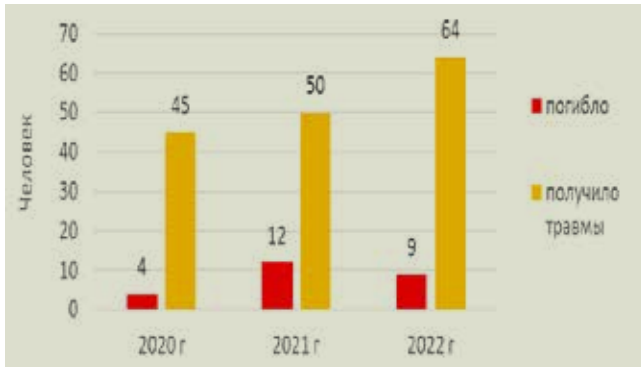


Рис. 1. Количество людей, погибших и получивших травмы в результате ДТП с участием диких животных

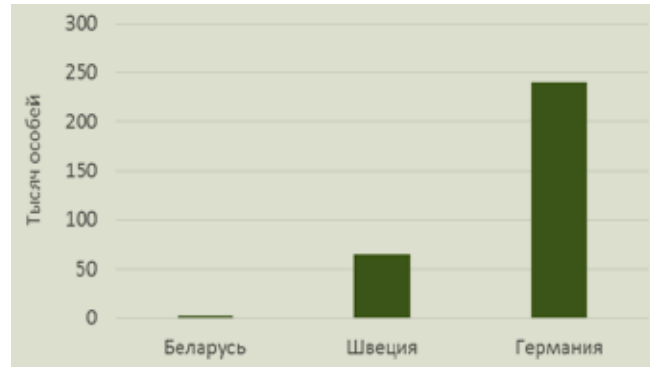


Рис. 2. Количество диких животных, погибших в результате ДТП в Беларуси и некоторых странах Европы в 2022 г.

тате столкновений с автомобилями погибло 240 388 диких животных, в том числе 209 300 косуль, 23 808 кабанов, 4 315 ланей, 2 965 оленей благородных. В Швеции по этой же причине пало 65 660 диких животных, в том числе 47 603 косули, 5 638 лосей, 5 852 кабана, 5 406 ланей, 437 оленей благородных.

Данные ДТП приводят как к прямому материальному ущербу, связанному прежде всего с повреждением транспортных средств, так и к косвенному: затратам на работу аварийно-спасательных служб, медицинское обслуживание, потере доходов. Прямой ущерб от столкновений копытных с транспортными средствами в Германии оценивается примерно в 450 млн евро в год, в Швеции и Франции – по 100 млн евро в год [2]. Общий ущерб в Словении составляет около 15 млн евро в год [3]. По мнению экспертов, в Европе только ежегодный ущерб от повреждения транспортных средств в результате столкновений с дикими животными (исключая компенсацию за телесные повреждения и работу экстренных служб) превышает 1 млрд евро [1].

В 2022 г. в Австрии произошло 298 ДТП с дикими животными, в которых люди получили серьезные травмы. В Польше было зафиксировано 257 случаев столкновения с объектами и животными на дорогах (отдельная статистика по диким животным не представлена), в результате чего погибли 50 человек и 289 получили серьезные ранения [4]. Статистические данные по Соединенному Королевству Великобритании и Ирландии показывают, что в период с 2000 по 2005 г. в результате дорожно-транспортных происшествий с участием копытных в среднем погибало 12 человек в год, при этом 100 происшествий приводили к серьезным травмам и 450 – к легким.

В последние годы в Республике Беларусь также наблюдается рост количества погибших и травмированных людей в результате ДТП с участием диких животных (рис. 1).

До 2021 г. сбор информации о ДТП такого рода носил децентрализованный характер, в результате чего достоверность предоставляемой информации была достаточно низкой. После введения требования об обязательном сообщении

о факте обнаружения травмированного или погибшего в результате ДТП дикого животного в Государственную инспекцию охраны животного и растительного мира при Президенте Республики Беларусь начался этап централизованного сбора указанной информации, что позволило получать точные данные о месте и дате происшествий, а также о виде погибшего животного, его поле и возрасте.

В течение 2021 г. в Беларуси в результате ДТП погибло 3050 диких копытных, в том числе 878 лосей, 81 олень благородный, 1907 косуль, 178 кабанов, 3 пятнистых оленя, 3 лани. Всего было зарегистрировано 2978 фактов ДТП с участием диких животных.

На протяжении 2022 г. погибло или было травмировано 3075 диких копытных, в том числе 850 лосей, 86 благородных оленей, 1992 косули, 142 кабана, 5 ланей. Общее количество зафиксированных фактов ДТП с участием диких животных составило 3021. Это значительно меньше, чем в странах Европы (рис. 2).

Как правило, существенный ущерб здоровью и имуществу причиняется в результате столкновения с дикими

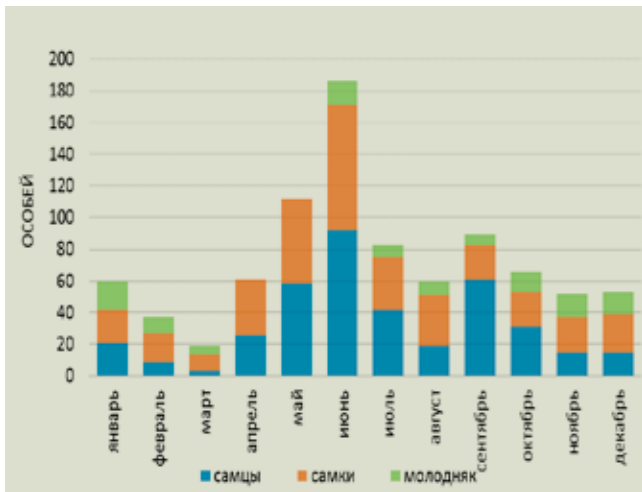


Рис. 3. Количество лосей, погибших в ДТП в 2021 г.

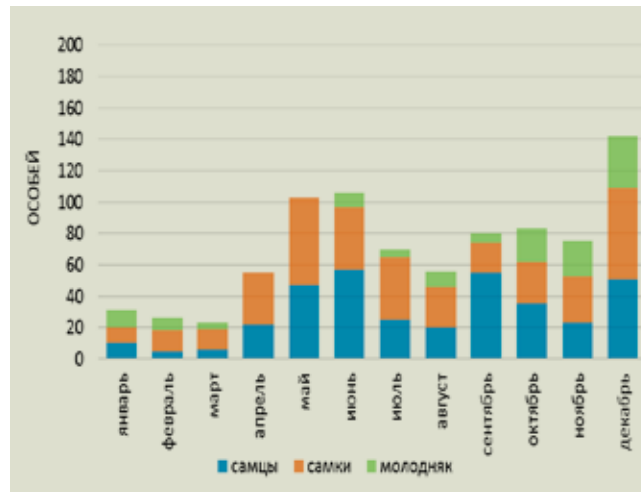


Рис. 4. Количество лосей, погибших в ДТП в 2022 г.

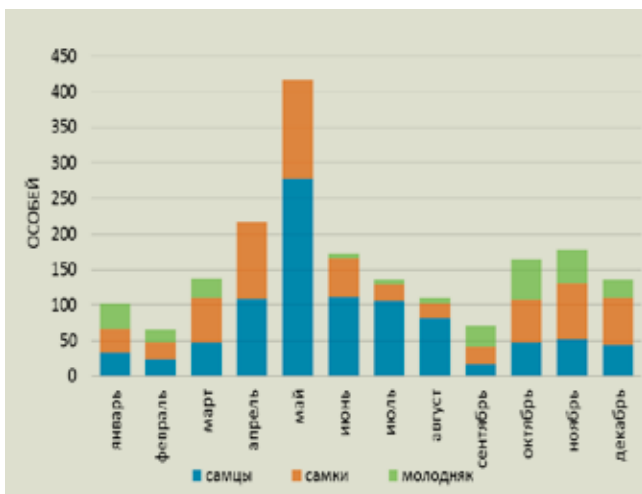


Рис. 5. Количество косуль, погибших в ДТП в 2021 г.

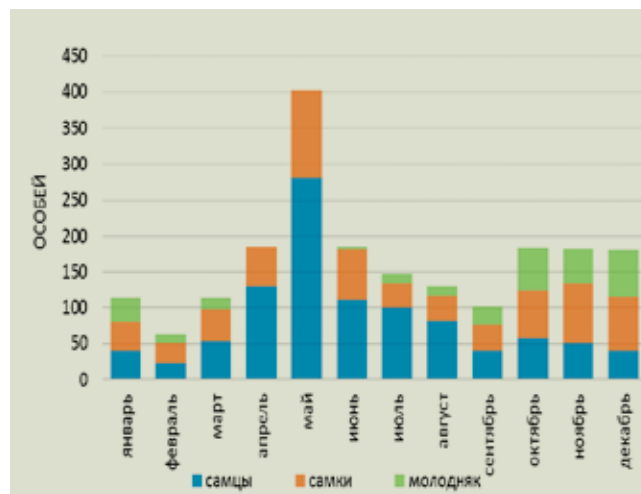


Рис. 6. Количество косуль, погибших в ДТП в 2022 г.

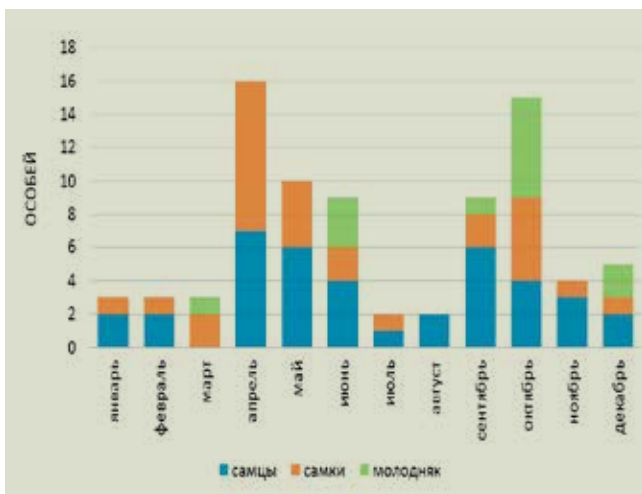


Рис. 7. Количество оленей благородных, погибших в ДТП в 2021 г.

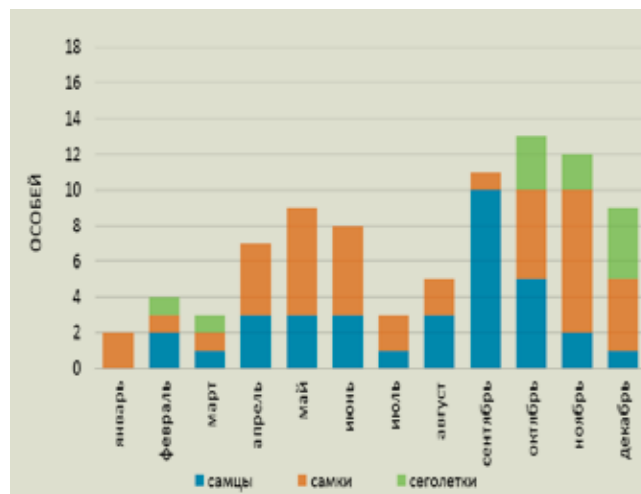


Рис. 8. Количество оленей благородных, погибших в ДТП в 2022 г.

копытными – лосем, оленем благородным, кабаном, оленем пятнистым, ланью и косулей. Анализ показал, что интенсивность совершения данных ДТП и половозрастная структура погибших в них животных зависит от сезона года (рис. 3–8). Наибольшее количество ДТП с участием диких животных фиксируется в мае – июне, что, на наш взгляд, обусловлено как повышением активности копытных (связана со сменой стадий обитания, поиском новых индивидуальных участков для жизни, проявлением самостоятельности у молодняка прошлого года), так и увеличением интенсивности дорожного движения.

В 2021, как и в 2022 г., в мае и июне наблюдается существенное увеличение фактов гибели лосей в ДТП. В этот же период года еще более ярко выражен рост столкновений транспортных средств с косулей. Следует также отметить, что в мае среди погибших и травмированных косуль преобладают самцы. Так, в 2021 г. их доля от общего количества в этом месяце составила 67%, а в 2022 г. – 70%. Такая закономерность обусловлена биологическими особенностями вида,

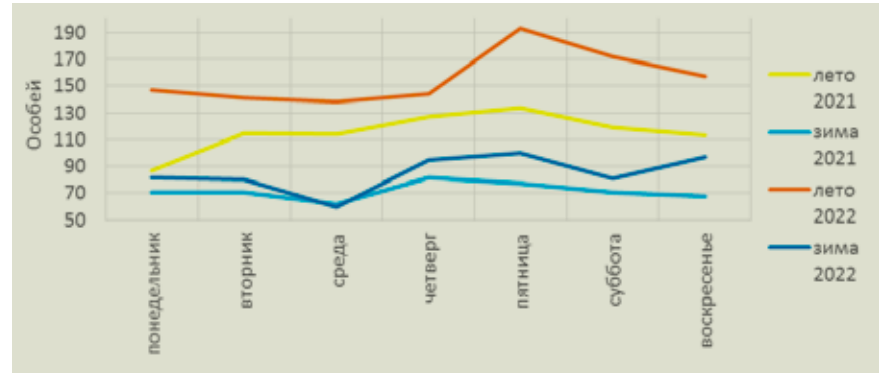


Рис. 9. Распределение животных, погибших в ДТП, по дням недели

связанными с тем, что в мае и июне молодые самцы косули ведут активный поиск новых индивидуальных участков.

Установлено, что самцы лося, косули и оленя благородного преобладают среди погибших и травмированных особей в период гона. Так, доля самцов от общего количества погибших лосей в сентябре 2021 и 2022 гг. составила 68%. Доля погибших самцов оленя благородного в сентябре 2021 г. – 66%, в 2022 г. – 90%. Доля погибших самцов косули в период занятия ими индивидуальных участков и в период гона в июне 2021 г. – 65%, в июле – 78%, в августе – 73% от общего числа погибших косуль. В 2022 г. доля

погибших самцов в июне – 59%, в июле – 78%, в августе – 62%.

Анализ в разрезе дней недели показал, что в пятницу и выходные дни регистрируется наибольшее количество травмированных или погибших в результате ДТП диких копытных, а в будние дни аварийность снижается (рис. 9). Также установлено, что гибель животных по данной причине увеличивается в летние месяцы.

Предварительный статистический анализ фактов ДТП в разрезе административных районов показал, что количество случаев гибели диких копытных в результате столкновения с автотранспортом достоверно зависит от протяженности



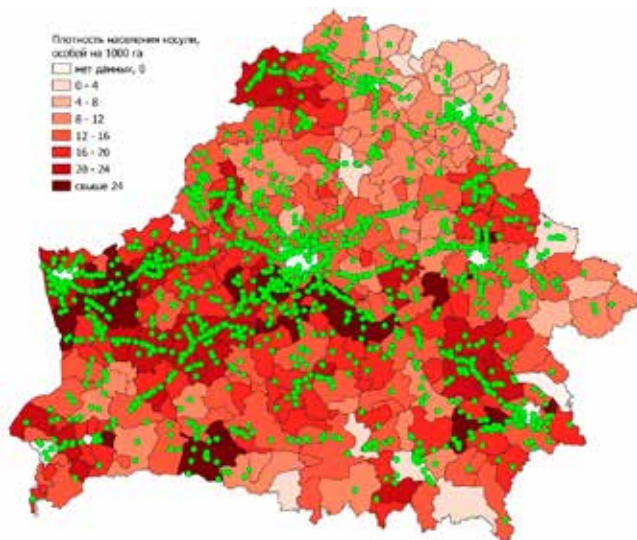


Рис. 10. Плотность населения косули и места ее гибели в ДТП в 2021 г.

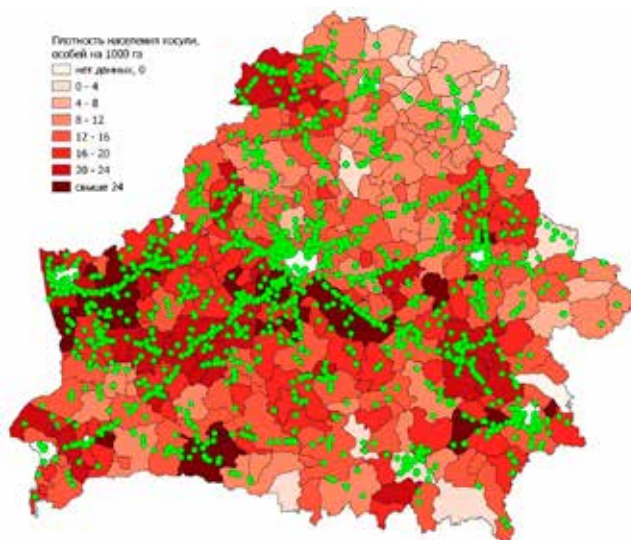


Рис. 11. Плотность населения косули и места ее гибели в ДТП в 2022 г.

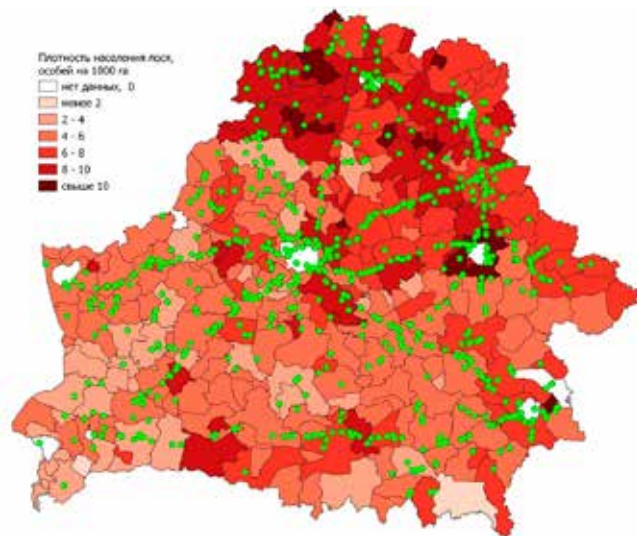


Рис. 12. Плотность населения лося и места его гибели в ДТП в 2021 г.

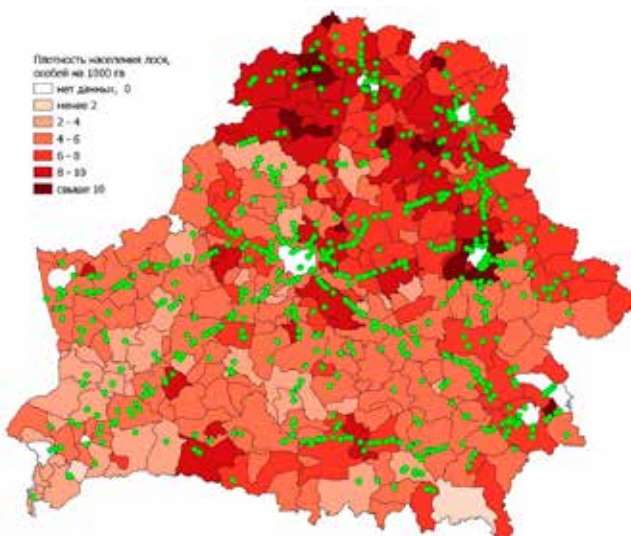


Рис. 13. Плотность населения лося и места его гибели в ДТП в 2022 г.

дорог с интенсивным движением (2021 г. –  $R^2=0,5239$ ; 2022 г. –  $R^2=0,5472$ ) и численности населения района (2021 г. –  $R^2=0,4765$ ; 2022 г. –  $R^2=0,4276$ ). Данные показатели определяют интенсивность транспортного потока на территории административных районов, поэтому можно утверждать, что именно этот фактор оказывает основное влияние на рост случаев ДТП с участием диких животных в конкретных регио-

нах. Это также подтверждается увеличением данных происшествий в пятницу и в выходные дни, когда интенсивность транспортного потока возрастает.

Анализ в разрезе границ охотничьих хозяйств не выявил четкой зависимости между аварийностью с участием диких животных и плотностью населения диких копытных: для лося она составила  $R^2=0,0181$ ; для оленя  $R^2=0,0813$ ; для косули  $R^2=0,0407$ ; для кабана  $R^2=0,066$ .

Также статистический анализ не выявил четкой зависимости между количеством погибших животных и размером их изъятия с 1000 га угодий, пригодных для их обитания (показателя, характеризующего плотность населения диких копытных). Для лося она составила  $R^2=0,0032$ ; для оленя  $R^2=0,1366$ ; для косули  $R^2=0,0161$ ; для кабана  $R^2=0,0009$ . В качестве примера необходимо привести Минский район, в котором при относи-

тельно низкой плотности населения копытных фиксируется наибольшая интенсивность ДТП с участием диких животных в Беларуси. При этом в ряде охотничьих хозяйств, где присутствует высокая плотность населения копытных, ежегодно отмечается относительно небольшое количество случаев указанных ДТП.

Для визуального отображения на карты, характеризующие состояние численности популяций, были нанесены места регистраций фактов гибели диких копытных в результате ДТП (рис. 10–13). Как в 2021, так и 2022 г. местами концентрации ДТП с участием диких животных, как правило, являлись участки автомобильных дорог, прилегающие к г. Минску, областным центрам и иным крупным населенным пунктам, а также автомобильные дороги, характеризующиеся высокой интенсивностью транспортного потока, вне зависимости от численности и плотности населения диких копытных.

Анализ зарубежного опыта показал, что в целях снижения аварийности с участием диких копытных применяется множество различных методов. Большинство из них можно свести к следующим основным направлениям:

- *предотвращение выхода диких животных на дорогу (установка заградительных сооружений вдоль автомобильных дорог, установка акустических и световых отпугивающих устройств, нанесение химических отпугивающих репеллентов);*
- *устройство переходов для диких животных и экодуков;*
- *повышение осведомленности водителей (установка табло,*

*срабатывающих при приближении животных, а также предупреждающих знаков, билбордов; информирование общественности через средства массовой информации; установка автомобильных систем, предупреждающих водителя о диком животном; вырубка придорожной растительности);*

- *сокращение численности копытных;*
- *ограничение скорости транспортных средств в наиболее аварийно опасных местах.*

Мировой опыт также показывает, что лишь немногие перечисленные меры могут быть относительно эффективными по отдельности. Многими экспертами признано, что снижения аварийности с участием диких копытных можно добиться только путем взаимного дополнения и использования сразу нескольких методов. Также следует отметить, что, несмотря на высокий уровень аварийности с участием диких животных и большое внимание к этой проблеме на протяжении последних десятилетий, в странах Европы так и не удалось найти эффективные методы, способные существенно снизить количество данных ДТП.

Таким образом, дорожно-транспортные происшествия с участием диких животных – проблема сложная и многогранная, требующая одновременного применения целого комплекса взаимодополняющих мероприятий. При этом ряд методов, таких как установка заградительных сооружений вдоль автомобильных дорог и устройство переходов для диких животных, являются достаточно дорогостоящими мероприятиями. Поэ-

тому крайне важно продолжать осуществлять постоянный мониторинг ДТП с участием диких животных и их изучение. Это позволит за счет всестороннего понимания процессов и закономерностей их возникновения не только повысить эффективность мер, принимаемых с целью снижения аварийности, но и снизить затраты на их реализацию. ■

■ **Summary.** Quantitative characteristics and a comparative analysis of traffic accidents involving wild animals in Belarus and other countries are given. The patterns of distribution of the ungulates number killed in road accidents are presented by seasons, days of the week, sex and age structure. It has been established that the places of accidents concentration are road sections adjacent to large settlements, as well as highways with high traffic.

■ **Keywords:** traffic accidents with wild animals, accident reduction methods, population adaptive regulation.

■ <https://doi.org/10.29235/1818-9857-2023-08-70-75>

#### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Langbein J., Putman R., Pokorny B. Traffic collisions involving deer and other ungulates in Europe and available measures for mitigation // In: Ungulate Management in Europe; Problems and Practises.– Cambridge, 2011.
2. Apollonio M., Reidar A., Putman R. European Ungulates and Their Management in the 21st Century.– Cambridge, 2010.
3. Pokorny B. Roe deer-vehicle collisions in Slovenia: situation, mitigation strategy and countermeasures // Veterinarski Arhiv. 2006. №76. P. 177–187.
4. Wypadki drogowe w Polsce w 2022 roku // Komenda główna policji. Biuro ruchu drogowego.– Warszawa, 2023.

Статья поступила  
в редакцию 06.07.2021 г.



# КЛИНИКО-ГЕНЕАЛОГИЧЕСКИЕ КРИТЕРИИ ОПУХОЛЕЙ КИШЕЧНИКА



**Олег Кузнецов,**  
директор Института биохимии биологически  
активных соединений НАН Беларуси, доцент  
кафедры микробиологии, вирусологии  
и иммунологии имени С.И. Гельберга  
Гродненского государственного медицинского  
университета, кандидат биологических наук;  
[olegkuznetsov@inbox.ru](mailto:olegkuznetsov@inbox.ru)

УДК 616.34-006-071-056.7

Трудности диагностики, распространенность онкологических процессов, их медицинская, социальная и экономическая значимость, а также высокий уровень летальности определяют актуальность борьбы с ними и делают проблему изучения механизмов их ранней диагностики и профилактики одной из ключевых [2, 5].



**Аннотация.** Трудности своевременной диагностики, дороговизна и сложность лечения, а также высокий уровень летальности от злокачественных новообразований определяет актуальность борьбы с ними. Наибольшая заболеваемость раком кишечника наблюдается в промышленных населенных пунктах. С высокой частотой встречаются первично-множественные опухоли, а также рак груди у мужчин. Роль Амстердамских критериев в диагностике наследственного неполипозного рака толстого кишечника в Гродненском регионе ограничена. Автором предложены критерии формирования групп риска развития опухолей толстого кишечника, удобные для онкогенетического консультирования.

**Ключевые слова:** группа риска, рак толстого кишечника, наследственные факторы, скрининг.

**Для цитирования:** Кузнецов О. Клинико-генеалогические критерии опухолей кишечника // Наука и инновации. 2023. №8. С. 76–83. <https://doi.org/10.29235/1818-9857-2023-08-76-83>

**В** 2020 г. в мире зафиксировано 19,3 млн новых случаев онкозаболеваний и почти 10 млн случаев смерти по их причине, при этом рак молочной железы (11,7%) превзошел по частоте выявления рак легких (11,4%), затем по распространенности следуют колоректальный (10%), простаты (7,3%), желудка (5,6%) и печени (4,7%) [11].

Ежегодно выявляется около 1,1 млн новообразований, 50% из них заканчиваются летальным исходом. В экономически развитых странах заболеваемость раком толстого кишечника/колоректальным раком (РТК/КРР) составляет: рак ободоч-

ной кишки – 58,7 на 100 тыс. населения, прямой – 28,8 на 100 тыс., пятилетняя выживаемость – 60%. Для сравнения: в Африке (Дакар, Сенегал) этот показатель в первом случае равен 1,3, во втором – 2,5, пятилетняя выживаемость – менее 40%. Экономические потери, например США, от данной патологии – около 6,5 млрд долл. в год, статистика по странам СНГ практически не доступна [1].

В Беларуси ежегодно впервые устанавливаются онкодиагнозы около 50 тыс. пациентам. Мы входим в группу государств (как и страны Балтии, Россия и Украина) с относительно невысоким уровнем заболеваемости РТК, однако за последнее десятилетие он увеличился в 3 раза [3, 7]. КРР в структуре новообразований зарегистрирован на уровне 29,6 у мужчин и 20,6 у женщин на 100 тыс. населения, при смертности 19,7 и 11,8 соответственно. Ежегодно выявляется около 2,5 тыс. новых случаев опухолей толстой кишки и 1,9 тыс. – прямой кишки, 35% из них диагностируется на III и IV стадиях. Пятилетняя выживаемость пациентов, в зависимости от стадии заболевания, варьирует от 14,5% до 60,6% [8].

Значимый фактор риска развития РТК – возраст: вероятность возникновения опухоли увеличивается после 55 лет и достигает максимума после 70. У более молодых пациентов данный вид рака развивается на фоне хронических заболеваний кишечника и полипоза [10].

Около 10% РТК относят к наследственным (Lynch H. T. et al, 1999). Вероятность его развития у носителей мутаций на протяжении жизни составляет 80–85%. При этом семейный анамнез, который является значимым диагностическим признаком, зачастую не анализируется [4]. Большинство критериев предрасположенности к заболеванию установлены эмпирически и не учитывают популяционных особенностей. Отечественные данные по этому вопросу на сегодняшний день неполные. В связи с этим перспективно установить группы риска для выявления новообразований на ранних стадиях. И хотя единого подхода в их формировании пока нет [8], достижения молекулярной биологии могут предоставить новые пути для этого.

Влияние на характеристики опухоли оказывают этнические и географические особенности населения, чем и определяется необходимость проведения их анализа в Беларуси. Его результаты позволят разработать рекомендации и принять решения для эффективной работы в группах риска [9].

Цель представленного исследования – анализ и уточнение клинико-генеалогических критериев диагностики и развития опухолей кишечника.

## Материалы и методы

Проведена оценка популяционного, госпитального скрининга и скрининг онкологического регистра пациентов Гродненского региона (данные за 1960–2014 гг.), полнота охвата – 13 182 человека: 612 пациентов онкодиспансера, из них 196 госпитализированных в стационар, 12 570 практически здоровых лиц. Семейный анамнез изучен у 10 706 респондентов, в том числе при госпитальном скрининге – 401. Клинические и генеалогические особенности РТК оценены в анамнезе 865 (47,19%) из 1833 пациентов, состоящих на учете в онкологическом регистре.

Все участники были проинформированы о целях исследования, методологии, а также об анонимном и конфиденциальном характере анкетирования. Анкета отражала сведения о частоте и характере онкопатологии.

В процессе работы была проанализирована частота встречаемости опухолей в регионе. С целью нивелирования влияния естественных годовых трендов исследовались грубые интенсивные показатели заболеваемости (отражают частоту выявления новых случаев опухолей за период времени в пересчете на 100 тыс. жителей). Расчет производили по формуле:

$$C = 100000 * \frac{R}{\sum_{o}^n N_i},$$

где R – общее число новых случаев заболеваний, выявленных за период n лет, N<sub>i</sub> – численность населения в i году (в интервале от 0 до n).

Разработка клинико-генеалогических критериев опухоли и формирование групп риска проведено на основании приказа «Об онкогенетическом консультировании» и Амстердамских диагностических критериев [4].

Результаты, полученные в ходе обследования, заносились в оригинальную базу данных [6]. Статистический анализ проводился с использованием пакета программ SPSS13 и методов непараметрической статистики. Для оценки достоверности различий применялся U-критерий Манна-Уитни, определялась медиана, минимальное и максимальное значение, интерквартильный

размах (IQR), среднее арифметическое со средним квадратичным отклонением ( $M \pm \sigma$ ). Критическое значение уровня значимости при проверке статистических гипотез принималось при  $p < 0,05$ .

## Результаты и обсуждение

Анализ частоты выявления онкозаболеваний в регионе показал, что рак молочной железы (РМЖ) чаще встречался в г. Гродно, Лидском и Слонимском р-нах (тут и далее достоверность  $p < 0,0001$ ), причем у мужчин – в Берестовицком, Зельвенском, Сморгонском и Мостовском р-нах; ни одного случая за 45 лет не отмечено в Вороновском и Свислочском р-нах. Рак яичников (РЯ) чаще обнаруживался в Лидском и Слонимском р-нах, предстательной железы – в Мостовском, Гродненском, Берестовицком и Свислочском р-нах, прямой и/или поперечно-ободочной кишки – в Берестовицком, Зельвенском и Слонимском р-нах. Рак щитовидной железы выявляли в 3–5 раз чаще в Сморгонском, Слонимском р-нах и г. Гродно. Высокая накопленная онкологическая заболеваемость

по всем локализациям отмечена в Берестовицком, Слонимском, Лидском, Мостовском р-нах и г. Гродно, низкая – Вороновском, Островецком, Кореличском и Щучинском (табл. 1).

Количество молодых лиц, заболевших онкологическими заболеваниями в районах области, представлено в табл. 2.

Анализ зависимости от возраста на момент постановки диагноза показал, что чаще опухоли у лиц моложе 30 лет отмечались в Слонимском, Лидском р-нах и г. Гродно,  $p < 0,0001$ . Наибольшее число случаев заболеваний в возрасте 18–30 лет – в Волковысском, Лидском р-нах и г. Гродно. Первично-множественные опухоли диагностировались в 2 раза чаще в Берестовицком, Мостовском р-нах и г. Гродно. Сочетания диагнозов (РМЖ, РЯ, РТК, щитовидная железа, простата) определялись в Берестовицком, Мостовском, Зельвенском р-нах и г. Гродно, ни разу – в Ивьевском и Свислочском.

Возрастная структура заболеваемости проанализирована по относительным показателям – доля случаев в интересующем возрастном периоде от общего числа онкозаболеваний (табл. 3).

№	Район	Молочная/грудная железа		Яичники	Простата	Толстый кишечник	Щитовидная железа
		все случаи	мужчины				
1.	Берестовицкий	51,88	1,35	16,24	23,01	44,66	4,96
2.	Волковысский	60,05	0,14	19,12	22,08	37,16	9,29
3.	Вороновский	41,40	0,00	20,21	18,02	28,00	4,63
4.	Гродненский	53,13	0,14	15,76	24,19	32,61	5,44
5.	Дятловский	41,97	0,66	17,45	20,99	31,15	5,08
6.	Зельвенский	43,00	1,01	21,84	18,81	38,97	9,07
7.	Ивьевский	46,50	0,45	19,67	20,34	24,81	3,13
8.	Кореличский	46,03	0,27	14,35	16,79	31,95	9,21
9.	Лидский	66,38	0,41	22,94	22,70	38,07	9,36
10.	Мостовский	53,92	0,92	21,66	25,58	36,87	8,99
11.	Новогрудский	58,19	0,31	19,50	19,81	36,66	7,49
12.	Островецкий	47,35	0,32	15,57	19,14	26,27	7,46
13.	Ошмянский	49,92	0,26	16,55	21,14	27,50	6,37
14.	Свислочский	52,88	0,00	16,95	26,78	34,24	5,42
15.	Слонимский	72,26	0,32	25,75	25,75	47,00	14,32
16.	Сморгонский	54,35	0,89	19,67	18,42	23,96	14,48
17.	Щучинский	53,83	0,28	16,74	21,59	26,43	2,63
18.	г. Гродно	87,01	0,50	22,71	21,45	40,24	12,23
19.	Всего	60,91	0,42	19,86	21,49	34,68	8,62

Таблица 1. Количество заболевших некоторыми онкологическими заболеваниями в районах области в пересчете на 10 тыс. населения

№	Район	Возраст на момент постановки диагноза		Локализация	
		18–30 лет	0–30 лет	парная*	множественная**
1.	Берестовицкий	16,30	21,70	1,89	47,64
2.	Волковысский	17,24	24,06	1,61	37,77
3.	Вороновский	10,66	13,74	0,96	23,37
4.	Гродненский	12,62	18,56	1,36	36,04
5.	Дятловский	12,01	19,11	0,89	26,22
6.	Зельвенский	11,32	17,06	2,01	35,45
7.	Ивьевский	9,77	13,63	0,00	32,33
8.	Кореличский	9,07	13,02	0,83	31,30
9.	Лидский	19,51	26,53	1,80	38,73
10.	Мостовский	15,22	20,93	2,09	42,33
11.	Новогрудский	8,82	14,77	0,62	39,35
12.	Островецкий	14,50	18,27	1,00	19,93
13.	Ошмянский	11,15	18,86	0,99	31,51
14.	Свислочский	13,78	19,74	0,00	35,53
15.	Слонимский	18,33	24,51	0,84	36,63
16.	Сморгонский	18,42	23,85	1,29	31,24
17.	Щучинский	11,84	15,32	0,82	31,60
18.	г. Гродно	26,64	29,98	2,47	52,27
19.	Всего	16,63	22,10	1,45	38,37

Таблица 2. Количество лиц молодого возраста, заболевших онкологическими заболеваниями в районах области в пересчете на 10 тыс. жителей (на 31.12.1983 г.). Примечание: опухоли 2 локализаций (\*) и первично-множественные опухоли (\*\*) из числа анализируемых (в пересчете на население региона)

№	Район	1–7 лет	8–12 лет	13–17 лет	18–30 лет	0–30 лет	Множественная локализация
1.	Берестовицкий	0,80	0,00	0,25	1,78	2,83	6,21
2.	Волковысский	0,69	0,28	0,48	2,10	3,55	5,57
3.	Вороновский	0,36	0,22	0,27	1,70	2,55	4,33
4.	Гродненский	0,35	0,33	0,49	1,64	2,81	5,45
5.	Дятловский	0,68	0,38	0,38	1,81	3,24	4,45
6.	Зельвенский	0,40	0,25	0,40	1,50	2,54	5,29
7.	Ивьевский	0,34	0,34	0,19	1,42	2,29	5,35
8.	Кореличский	0,37	0,25	0,16	1,19	1,97	4,64
9.	Лидский	0,63	0,29	0,48	2,27	3,67	5,37
10.	Мостовский	0,55	0,20	0,36	1,82	2,92	5,91
11.	Новогрудский	0,43	0,19	0,48	1,19	2,28	6,02
12.	Островецкий	0,52	0,17	0,35	2,15	3,20	3,49
13.	Ошмянский	0,66	0,31	0,71	1,68	3,36	5,62
14.	Свислочский	0,55	0,25	0,35	1,86	3,02	5,43
15.	Слонимский	0,43	0,20	0,63	2,17	3,43	5,15
16.	Сморгонский	0,52	0,28	0,61	2,55	3,96	5,19
17.	Щучинский	0,25	0,36	0,17	1,58	2,35	4,85
18.	г. Гродно	0,63	0,24	0,61	3,04	4,52	7,84
19.	Всего	0,53	0,26	0,46	2,11	3,36	5,82

Таблица 3. Случаи онкозаболеваний в возрастном периоде (%)

Пол	Возраст (лет)						итого	% к общему количеству пациентов
	30–39	40–49	50–59	60–69	70–79	80–89		
Мужчины	16	60	92	115	130	109	522	61,9%
% к числу мужчин	3,1%	11,5%	17,6%	22,0%	24,9%	20,9%		
Женщины	10	40	60	70	92	71	343	38,1%
% к числу женщин	2,9%	11,7%	17,5%	20,4%	26,8%	20,7%		
Всего	26	100	152	185	222	180	865	100%
	3,0%	11,5%	17,6%	21,4%	25,7%	20,8%		

Таблица 4. Распределение пациентов с КРР (разделение по полу и возрасту)

Наибольшая накопленная заболеваемость в возрасте до 7 лет зарегистрирована в Берестовицком, Дятловском и Волковысском р-нах, 8–12 лет – в Дятлово, Ивье и Щучине, 13–17 лет – в Ошмянском, Слонимском, Сморгонском р-нах и г. Гродно, 18–30 лет – в Лидском, Сморгонском р-нах, г. Гродно.

Так как наиболее часто опухоли диагностировались в Берестовицком, Слонимском, Лидском, Мостовском р-нах и г. Гродно, можно предположить, что в промышленных регионах заболеваемость связана с окружающей средой (повышение частоты мутаций): косвенно это подтверждается самой высокой частотой опухолей среди лиц молодого возраста. В Берестовицком и Мостовском р-нах встречаются первично-множественные опухоли, а также рак груди у мужчин: вероятно, фактор, способствующий повышенной онкологической заболеваемости – наследственная предрасположенность.

Распределение пациентов по полу и возрасту, состоящих на учете, представлено в табл. 4.

Мужчины составляли 61,9% всех респондентов: их количество объективно возрастало по мере увеличения возраста возникновения онкозаболевания при постановке на учет ( $p < 0,01$ ).

В ряде исследований показано, что 15–20% пациентов с РТК имеют родственников первой степени родства с такой же патологией. По современным представлениям, наследственные факторы, предрасполагающие к развитию опухоли, включают в себя две категории заболеваний, проявляющиеся в виде полипоза и/или рака: первая – семейный аденоматозный полипоз, синдром Гарднера, синдром Пейтца-Егерса, семейный ювенильный полипоз; вторая – наследственный неполипозный колоректальный рак (HNPCC-синдром), наиболее выраженная форма наследственного КРР, составляет 4–5% случаев [12].

Семейный анамнез проанализирован в регионе в соответствии с Амстердамскими критериями («Амстердам I/II») [13].

1. Точный HNPCC (HNPCC) («Амстердам I», 1991 г., определение наследственного неполипозного рака толстой кишки): наличие 3 или более родственников с диагнозом РТК; не меньше чем один из заболевших должен быть родственником I степени родства к остальным двум; РТК встречается более чем в одном поколении; один из родственников моложе 50 лет; семейный аденоматозный полипоз исключен.

2. Точный HNPCC (HNPCC) («Амстердам II», 1997 г., уточнены и расширены критерии Бетезды): рак, отвечающий Амстердамским критериям; 2 наследственно обусловленных рака, включая синхронные или метахронные колоректальные карциномы, либо ассоциированные неоплазии; КРР у пациента и кого-либо из родственников I линии, либо ассоциированные неоплазии; аденоматозные полипы (карцинома выявлена до 45 лет, а аденоматозный полип до 40 лет); РТК либо рак эндометрия и/или рак яичников, выявленный до 45 лет; колоректальный аденоматозный полип, выявленный до 40 лет; семейный аденоматозный полипоз исключен; опухоли подтверждены гистологически.

3. Последний исходный HNPCC/(HNPCC LO): «Амстердам II» критерии без ограничения возраста.

4. Подозрительный (Suspected) HNPCC – HNPCC SUSP: у 2 родственников I степени родства с HNPCC имело место сочетание с КРР, раком эндометрия, тонкой кишки, мочеточников, почечной лоханки; один рак диагностирован в возрасте до 50 лет.

5. Расширенный (Extended) HNPCC (HNPCC EXT): у 2 родственников I степени родства с HNPCC имело место сочетание с КРР, раком яичников, желудка, гепатобилиарным, поджелудочной железы, моче-

вого пузыря, мозга, раком гениталий; один рак диагностирован в возрасте до 50 лет.

6. Семейный колоректальный рак (Familial colorectal cancer (FCC): KPP у 2 родственников I или II степени родства; у одного из них диагностирован в возрасте до 60 лет; HNPCC и FAP должны быть исключены.

7. Точный или подозреваемый наследственный рак молочной железы: 2 случая РМЖ или 1 случай РМЖ и 1 – рака яичников среди родственников I степени родства или II степени родства по отцовской линии; 1 РМЖ в семье, диагностированный в возрасте до 40 лет.

8. Рак «семейное скопление»: у 3 родственников I степени родства диагностировались злокачественные новообразования любой локализации.

При отсутствии случаев онкозаболеваний среди родственников пробанда – семья классифицировалась как «негативная». Если имелось указание на один случай, но семейство не соответствовало диагностическим критериям колоректального ракового синдрома, семья расценивалась как «другие». В случаях, когда родословная соответствовала критериям наследственного ракового синдрома, пробанду рекомендовалось молекулярно-биологическое обследование.

По результатам анкетирования родственников 865 пациентов с диагностированным РТК/КРР в 91,9% случаев (9838) от общего количества, доброкачественных и/или злокачественных образований обнаружено не было. В 7,0% случаев (753) у родственников констатируется не менее одного злокачественного новообразования ( $p < 0,01$ ).

Анализ частоты встречаемости колоректальных раковых синдромов в регионе представлен в табл. 5.

Имели место наследственные колоректальные раковые синдромы в соответствии с Амстердамскими критериями, частота которых от 0,1% (подозрительный, наследственный неполипозный РТК) до 39,8% («семейное скопление», 3 опухоли у родственников). Одна родословная (0,11%) соответствовала критериям «Амстердам I»: наличие 3 родственников с РТК (КРР, рак ректосигмоидного соединения), 2 заболевших родственника I степени родства, РТК в двух поколениях, возраст заболевшего родственника 35 лет. Всего обнаружено 452 случая КРР. Возраст на момент постановки диагноза:  $57 \pm 2,3$  лет. В 65,9% случаев (298 пациентов) опухоли локализованы в нисходящей части толстой кишки. Выявлено 3 семьи (0,35%), соответствующие критериям «Амстердам II». В одном случае (0,11%) – признаки, характерные для подозрительного наследственного неполипозного (НН) рака толстой кишки: КРР у родственника I степени родства, РТК выявлен в 38 лет. Критериям «Расширенного» подозрительного НН РТК соответствовали 2 родословные (0,23%). В обоих случаях имелось сочетание с раком яичников. Возраст при постановке диагноза:  $63 \pm 2,8$  года. К «Последнему исходному» наследственному неполипозному РТК, или соответствовавшему критериям «Амстердам II» без ограничения возраста, отнесено 83 случая (9,6%).

В 11 случаях отмечено сочетание КРР у пациента и одного из родственников I линии. Возраст для данных случаев: 48,8 года. В 6 родословных выявлено сочетание у родственников двух случаев КРР с неоплазиями у родственников I степени, средний возраст: 45,2 года. В 61 родословной РТК/КРР сочетался с неоплазией у родственника I линии, возраст:  $52,4 \pm 3,1$  года.

Диагноз	Случаи	Встречаемость, %
Точный, наследственный неполипозный рак толстого кишечника (HNPCC)	4	0,5
Подозрительный, наследственный неполипозный рак толстого кишечника (HNPCC SUSP)	1	0,1
Последний исходный, наследственный неполипозный рак толстого кишечника (HNPCC LO)	83	9,6
Расширенный, наследственный неполипозный рак толстого кишечника (HNPCC EXT)	2	0,2
Семейный колоректальный рак (FCC)	2	0,2
Рак «семейное скопление» (CFA) или 3 рака у близких родственников (ЗСА)	344	39,8
Точный или подозреваемый наследственный рак молочной железы (HBC)	16	1,8
Другие злокачественные опухоли	154	17,8
Отрицательные	259	29,9
Итого	865	100

Таблица 5. Встречаемость наследственных колоректальных раковых синдромов (критерии «Амстердам»)

Схожесть диагностических критериев «Рак «семейное скопление» и «Три рака у близких родственников» позволила объединить их в одну группу (344 случая, 39,8%). Возраст при постановке диагноза:  $63,5 \pm 2,6$  года. Количество процессов толстого кишечника с локализацией в нисходящей части толстой кишки – 67,8%.

Семейный КРР выявлен в 2 (0,23%) случаях. В 16 – среди родственников пробандов установлены критерии наследственного РМЖ, у 15 – сочетание 2 случаев РМЖ, в одном – сочетание РМЖ и РЯ. Диагнозы выставлены в возрасте до 40 лет.

Опухолевая патология, обнаруженная у родственников пациентов, представлена ( $n=753$ ) следующей патологией: колоректальный рак – 19,9%; меланома кожи – 1,9%; опухоли головного мозга – 7%, опухоли матки – 7,6%; почка – 1,7%; рак горлани – 3,6%; рак желудка – 14,2%, рак кожи – 1,5%; рак легких – 5,7%; рак молочной железы – 24,4%, рак мочевого пузыря – 1,3%; рак печени – 2,8%, рак пищевода – 1,6%, рак позвоночника – 1,5%, рак яичника – 4,2%, хронический лимфолейкоз – 1,3%.

На основании анализа (КРР, «Амстердам I/II») [8], принимая во внимание, что одним из основных критериев отбора лиц с РТК для дальнейшего молекулярно-генетического исследования (поиск мутаций в генах MSH2,

MSH6, MLH1, BRCA1, BRCA2) является возраст на момент постановки диагноза (<50 лет), а также учитывая, что такие пациенты составили 43,7% от числа состоящих на учете, предложены диагностические критерии оценки степени риска развития РТК/КРР:

- подозрение на наличие наследственного КРР: наличие синхронного или метахронного КРР и ассоциированных с ним опухолей в любом возрасте; наличие у пациента признаков высокой микросателлитной нестабильности (инфильтрации лимфоцитами, молекулярный характер роста), установленных в возрасте до 60 лет; КРР и ассоциированные с ним опухоли (рак: эндометрия, желудка, яичников, поджелудочной железы, уретры, почечных лоханок, желчных протоков, мозга, сальных желез, аденомы и кератоакантомы, карциномы), диагностированные у одного родственника I степени родства в возрасте до 50 лет; КРР или ассоциированные с ним опухоли, диагностированные в любом возрасте у 2 родственников I или II степени родства;
- высокий клинический риск возникновения наследственного КРР: КРР или ассоциированные с ним опухоли, диагностированные у 3 и более родственников I степени родства и у одного в возрасте до 50 лет.

Группа риска	n	%
<b>Скрининг онкологического регистра</b>		
Высокий риск наследственного КРР/РТК	7	1,68
Подозрение на наличие наследственного КРР/РТК	95	22,84
Отсутствует риск развития наследственного КРР/РТК	314	75,48
<b>Всего</b>	<b>416</b>	
<b>Госпитальный скрининг</b>		
Высокий риск наследственного КРР/РТК	13	6,63
Подозрение на наличие наследственного КРР/РТК	53	27,04
Отсутствует риск развития наследственного КРР/РТК	130	66,32
<b>Всего</b>	<b>196</b>	
<b>Популяционный скрининг</b>		
Высокий риск наследственного КРР/РТК	10	0,08
Подозрение на наличие наследственного КРР/РТК	52	0,41
Отсутствует риск развития наследственного КРР/РТК	12 508	99,51
<b>Всего</b>	<b>12 570</b>	

Таблица 6. Распределение пациентов по группам риска развития КРР/РТК

Результаты анкетирования позволили распределить пациентов в группы по риску развития КРР/РТК (табл. 6).

При скрининге регистра среди лиц с установленным диагнозом РТК/КРР высокий риск развития процесса составил 1,68%,  $p < 0,05$ . При госпитальном скрининге – 6,63% пациентов с высоким риском и 27,04% – с подозрением на наличие процесса. Популяционный анализ выявил суммарный высокий риск и подозрение на наличие процесса в 0,49% случаях.

## Заключение

Проведен анализ и оценка критериев развития опухоли в зависимости от клинических и генетических особенностей РТК/КРР, предложены критерии дифференциальной диагностики данной патологии у практически здоровых лиц.

Наибольшая заболеваемость РТК (накопленная, за 50 лет) наблюдается в Берестовицком, Слонимском, Лидском, Мостовском р-нах и г. Гродно, что позволяет предположить связь высокой онкозаболеваемости в промышленных населенных пунктах (в том числе среди лиц молодого возраста) с загрязнением окружающей среды, способствующим повышению частоты мутаций. В Берестовицком и Мостовском р-нах с высокой частотой встречаются первично-множественные опухоли, а также рак груди у мужчин. Вероятно, фактор, способствующий повышенной заболеваемости, – наследственная предрасположенность.

Высокий риск развития РТК/КРР наследственного генеза имеется у 0,49% населения региона. Частота выявления таких лиц выше при госпитальном скрининге, чем при использовании онкологического регистра,  $p < 0,002$ . Удельный вес родственников в этой группе составил 8,39%. Они нуждаются в дальнейшем динамическом наблюдении.

Роль Амстердамских критериев в диагностике наследственного неполипозного РТК/КРР в регионе ограничена. Диагностические критерии «Последнего исходного» НН РТК – эффективный инструмент выбора для формирования групп риска и идентификации в последующем патологии с помощью молекулярно-генетического метода. Предложенные критерии формирования групп риска развития РТК/КРР адекватны и удобны для онкогенетического консультирования (скрининга). ■

■ **Summary.** Difficulties in timely diagnosis, the high cost and complexity of treatment, as well as the high mortality rate of malignant neoplasms determine the relevance of combating them. The highest cumulative incidence of colon cancer is observed in the industrial centers of the region. Primary multiple tumors and breast cancer in men are found with a high frequency. The role of the Amsterdam Criteria in the diagnosis of hereditary non-polyposis colon cancer in the region is limited. The risk of developing colon cancer of hereditary genesis is present in 0,49% of the region's population. The proposed criteria for the formation of risk groups are adequate and convenient for oncogenetic counseling.

■ **Keywords:** risk group, colon cancer, hereditary factors, screening.

■ <https://doi.org/10.29235/1818-9857-2023-08-76-83>

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. F. Bray [et al.]. Global cancer statistics 2018: GLOBOCAN estimates of incidence and mortality worldwide for 36 cancers in 185 countries // *CA: A Cancer Journal for Clinicians*. 2018. Vol. 68. №6. P. 394–424.
2. О.Е. Кузнецов, В.М. Цыркунов. Вирус-ассоциированный гепатоцеллюлярный рак печени // *Гепатология и гастроэнтерология*. 2021. Т. 5. №1. С. 17–24.
3. F. Bray. Global Cancer Statistics: GLOBOCAN estimates of incidence and mortality worldwide for 36 cancers in 185 countries // *CA: A Cancer Journal for Clinicians*, in press. The online GLOBOCAN 2018 database is accessible at <http://gco.iarc.fr/>, as part of IARC's Global Cancer Observatory.
4. Приказ Мин-ва здравоохранения Респ. Беларусь №1018 27.12.2007 №1018 «Об онкогенетическом консультировании». – Минск, 2009.
5. Статистика злокачественных новообразований в России и странах СНГ в 2004 г. / под ред. М.И. Давыдова, Е.А. Аксель // *Вестник РОНЦ им. Н.Н. Блохина РАМН*. 2006. Т. 17. №3 (прил. 1).
6. Информационная система учета и мониторинга онкологических заболеваний: пат. №675 Респ. Беларусь / О.Е. Кузнецов; заявитель Кузнецов О.Е. – С20140041; опубл. 20.06.2014 // *Афиційны бюл. / Нац. цэнтр інтэлектуал. уласнасці*.
7. Океанов А.Е. [и др.]. Статистика онкологических заболеваний в Республике Беларусь (2008–2017) / А.Е. Океанов, П.И. Моисеев, Л.Ф. Левин, под ред. О.Г. Сукоко // Министерство здравоохранения Республики Беларусь, ГУ «Республиканский научно-практический центр онкологии и медицинской радиологии им. Н.Н. Александрова». – Минск, 2018.
8. A. Meindl [et al.]. Hereditary breast and ovarian cancer: new genes, new treatments, new concepts // *Deutsches Ärzteblatt International*. 2011. Vol. 108(19). P. 323–330.
9. H.T. Lynch, J.F. Lynch, T.G. Shaw [et al.]. HNPCC (Lynch Syndrome): Differential Diagnosis, Molecular Genetics and Management // *Review. Hereditary Cancer in Clinical Practice*. 2003. Vol. 1. P. 7. <https://doi.org/10.1186/1897-4287-1-1-7>.
10. L. Rabeneck [et al.]. Ontario's Colon Cancer Check: results from Canada's first province-wide colorectal cancer screening program // *Oncology. Ontario*. 2014. №23(3). P. 508–515.
11. Hyuna Sung [et al.]. Global Cancer Statistics 2020: GLOBOCAN Estimates of Incidence and Mortality Worldwide for 36 Cancers in 185 Countries // *American Cancer Society. CA: A Cancer Journal for Clinicians*. 2021. №71. P. 209–249.
12. M. Gerstung, C. Jolly, I. Leshchiner [et al.]. The evolutionary history of 2,658 cancers // *Nature*. 2020. №578. P. 122–128. <https://doi.org/10.1038/s41586-019-1907-7>.
13. A. Umar, C. Boland, J. Terdiman [et al.]. Revised Bethesda Guidelines for hereditary nonpolyposis colorectal cancer (Lynch syndrome) and microsatellite instability // *Journal of the National Cancer Institute*. 2004. Vol. 96. P. 261–268.

Статья поступила в редакцию 04.05.2022 г.

*Alexander Mikhalychev*

**Quantum mechanics and its basic principles** ..... 4

The article discusses the fundamentals of quantum mechanics, the features of micro objects measurements and states, as well as the differences between quantum and classical descriptions of physical systems.

*Sergey Kilin*

**The universal quantum computer is ahead of time and technology** ..... 10

The author gives a review of achievements in the field of quantum computers, analyzes the potential of these devices, as well as the first products of quantum technologies.

*Gleb Salakhov, Anton Bozhedarov, Alexey Fedorov*

**Quantum technologies: New opportunities, successes and challenges** ..... 18

The article provides an overview of the current quantum technologies on their way to practical application.

*Ilya Rodionov, Olga Efremova*

**Quantum computing: In search of coherence** ..... 24

The author considers the superconducting quantum circuits, which take one of the leading positions among the platforms for the next-generation computing.

*Sergey Kulik*

**Quantum sensors** ..... 31

Quantum sensorics was considered as one of the promising scientific and technological areas, due to which modern devices are created, as well as advanced scientific developments in the field of quantum mechanics are stimulated.

*Dmitry Mogilevtsev*

**Quantum radars** ..... 37

The article considers the new methods for diagnosing remote objects with the help of quantum radars, which enable to improve the detecting and recognizing abilities of moving or stationary targets.

*Alexey Akimov*

**Quantum sensors based on color centers in diamond** ..... 41

There is considered the quantum sensors and metrology as one of the important directions in the future quantum technologies development.

*Alexander Nizovtsev, Alexander Pushkarchuk,*

*Dmitry Filimonenko, Sergey Kilin*

**Quantum technologies based on nitrogen-vacancy color centers in diamond** ..... 46

There is given a brief review of the results of the NV centers in diamond and their complexes with <sup>13</sup>C nuclear spins characteristics computer simulation. The data obtained are used to implement various quantum technologies based on them.

*Gennady Matveev*

**Mathematical aspects of post-quantum cryptography** ..... 52

The author gives the reasons to the need for bringing the system of cryptographic information protection in the republic in line with new post-quantum requirements.

*Zhanna Komarova*

**Trust in technology** ..... 57

Scientists discuss the prospects of quantum cryptography, its advantages and disadvantages.

*Tatsiana Zhdanovich*

**The power of the roots, the abyss of the heavens. How a young Belarusian researcher deciphered our cultural code via the rustling of leaves** ..... 62

It is an essay about the young historian and ethnologist Yana Shevchenko, her path to science and research work. It also discloses why the basis of our life, physical and spiritual, is hidden under the shade of forests.

*Pavel Heshtaut, Stepan Huznei*

**Road accidents involving wild animals: Patterns and comparative analysis** ..... 70

Various statistical data have been analyzed, as well as the reasons for the increase in road accidents, including those with tragic consequences for both animals and people, in the Republic of Belarus and other countries. Based on the study of world experience, a list of measures aimed to reduce the number of such accidents in our country is given.

*Oleg Kuznetsov*

**Clinical and genealogical criteria for intestinal tumors** ..... 76

The author proposed the criteria for the formation of tumors of the large intestine risk groups, convenient for oncogenetic counseling.



**Упаковка пищевых продуктов: материалы, технологии, экология** / И. Ю. Ушакова [и др.]; под ред. В. А. Гольдаде. – Минск : Белорусская наука, 2023. – 286 с.  
ISBN 978-985-08-3013-5.

В монографии представлен широкий обзор литературных данных (в том числе результаты собственных исследований авторов) и нормативных документов по классификации современных упаковочных материалов, их свойствам, методам контроля и областям применения, отмечены роль и основные функции упаковки. Книга содержит описание материалов, используемых в производстве тары и упаковки, основных методов изготовления, схем и оборудования для изготовления тары и упаковки, отмечены их преимущества и недостатки. Подробно рассмотрены конкретные виды упаковки для различных пищевых продуктов, а также основные виды и функции потребительской маркировки товаров и упаковки, виды кодирования информации о товаре; анализируется использование маркировочных знаков для потребительской и транспортной тары. Проанализированы основные способы обращения с отходами упаковочных материалов. Уделено внимание утилизации упаковочных материалов и их экологической безопасности.

Книга адресована специалистам в области упаковочного материаловедения, инженерам-экологам, а также может быть полезна преподавателям, магистрантам и аспирантам, специализирующимся в области упаковки продовольственных товаров.



**Теоретико-методологические основы совершенствования правового обеспечения экономической безопасности** / Н. С. Минько [и др.]; под общ. ред. Н. С. Минько; Национальная академия наук Беларуси, Институт экономики. – Минск : Белорусская наука, 2023. – 261 с.  
ISBN 978-985-08-3023-4.

В монографии раскрываются теоретико-методологические основы совершенствования правового обеспечения экономической безопасности в Республике Беларусь с учетом зарубежного опыта. Определены концептуальные направления развития регулятивных и охранительных правовых механизмов в данной сфере.

Рассчитана на научных и практических работников, преподавателей, аспирантов и иных обучающихся в учреждениях высшего образования юридического и экономического профилей.



**Корпоративное управление организаций с государственным участием: оценка качества и направления совершенствования**; Д. Л. Коновалов, Е. В. Преснякова; под науч. ред. Е. В. Пресняковой. – Минск : Белорусская наука, 2023. – 185 с. – (Белорусская экономическая школа).  
ISBN 978-985-08-3011-1.

В монографии раскрыты теоретико-методологические основы корпоративного управления организаций с государственным участием. Представлен алгоритм построения механизма внутренней оценки качества корпоративного управления. Предложена к использованию методика оценки качества корпоративного управления организаций с долей государственной собственности. Сформированы организационно-управленческие мероприятия по совершенствованию системы корпоративного управления организаций с долей государственной собственности.

Рассчитана на представителей органов государственного управления, специалистов реального сектора экономики, научных работников, аспирантов, магистрантов.

## РУП «ИЗДАТЕЛЬСКИЙ ДОМ «БЕЛОРУССКАЯ НАУКА»

*предлагает литературу*

- по медицине
- искусствоведению
- литературоведению
- языкознанию
- этнографии
- фольклору
- естественным наукам

*принимает заказы на печать*

- бланки формата А<sub>5</sub>, А<sub>4</sub>, А<sub>3</sub>
  - грамоты ● дипломы
  - канцелярские книги
  - блокноты ● блоки для записей
  - календари ● буклеты
  - проспекты (с разработкой дизайна)
- тираж от 1 экземпляра*

*Получить информацию об изданиях и оформить заказ можно по телефону:*

*+375 (17) 396-83-27,  
370-64-17, 267-03-74.  
Адрес: ул. Ф. Скорины, 40,  
220084, г. Минск,  
Республика Беларусь;  
e-mail: belnauka@mail.ru;  
сайт: www.belnauka.by*

# II ФОРУМ IT-АКАДЕМГРАДА

## ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В БЕЛАРУСИ

12–13  
ОКТАБРЯ  
2023 Г.

### ОРГАНИЗАТОРЫ:

- Национальная академия наук Беларуси
- Объединенный институт проблем информатики НАН Беларуси




### В рамках II Форума состоится:

- выставка разработок в области искусственного интеллекта с презентацией белорусской цифровой платформы искусственного интеллекта
- заседание тематических секций и круглого стола с рассмотрением проблемных вопросов разработки и внедрения искусственного интеллекта
- открытый конкурс «Лидеры искусственного интеллекта в Беларуси – 2023»
- заседание Экспертного совета Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств и Регионального содружества в области связи

### Место проведения:

Республика Беларусь, г. Минск,  
пр-т Независимости, 66.

 <http://uiip.bas-net.by/2-forum-it-a/index.php>

 [ewlad@newman.bas-net.by](mailto:ewlad@newman.bas-net.by)

ИНФОРМАЦИОННЫЙ ПАРТНЕР  
Научно-практический журнал  
**Наука  
и инновации**

