УДК 004.387

**А.А. Крючков, Ю.И. Пастухова**

# Подходы к прогнозированию результатов выработки случайных двоичных последовательностей, генерируемых на квантовых вычислительных устройствах

Доработан функционал приложения с графическим интерфейсом по выработке бинарных последовательностей на облачных квантовых компьютерах в рамках добавления программных инструментов построения регрессионных моделей. Построены модели множественной линейной регрессии и бинарного выбора, где в качестве независимых параметров моделей использованы актуальные на момент эксперимента технические характеристики квантовых состояний. Прогнозируемые значения отражают ожидаемые результаты проверки последовательностей набором статистических тестов NIST STS, а также степень равномерности распределения «0» и «1» в сгенерированных последовательностях. В рамках исследования, основываясь на информации об актуальных технических характеристиках квантового процессора, предложены подходы к прогнозированию результатов генерации случайных чисел на квантовых вычислительных устройствах, что может быть полезным при проектировании квантовой схемы до ее непосредственного запуска.

**Ключевые слова:** квантовый компьютер, генерация случайных чисел, кубит, регрессионный анализ.
**DOI:** 10.21293/1818-0442-2025-28-2-96-105

В исследовательских задачах одним из актуальных вопросов является способ выработки случайной двоичной последовательности (СП). Одновременно с предложением некоторых подходов по реализации квантовых генераторов случайных чисел (КГСЧ) в виде отдельных изделий [1–4] с момента появления возможности работы с квантовыми вычислительными устройствами (КВУ) в облачном доступе опубликовано значительное количество исследований [5–8], направленных на изучение методов использования КВУ в качестве самостоятельных генераторов случайных чисел (ГСЧ). В большинстве случаев авторы научных работ приходят к выводу, что квантовые компьютеры действительно обладают потенциалом в рассматриваемой области.

В то же время некоторые исследования не учитывают предельно допустимый уровень современного аппаратного обеспечения квантовых систем, имеющих ряд ограничений, накладываемых на вычислительные возможности NISQ-устройств (Noisy Intermediate-Scale Quantum systems) [9]. В результате несовершенства квантового оборудования, а также вследствие воздействия окружающей среды процесс выполнения квантовой схемы на современных КВУ подвержен искажениям различной природы. Такое поведение системы может существенным образом сказываться на интерпретации получаемых результатов [10, 11].

Учитывая вышесказанное, авторы выдвигают предположение о некорректности запуска схемы КГСЧ на КВУ без предварительного анализа актуальных технических характеристик устройства, что напрямую может влиять на свойства генерируемых СП. Более того, возникает вопрос – существует ли возможность предсказать результат работы КВУ в режиме ГСЧ по имеющимся в открытом доступе сведениям о состоянии квантового процессора. Наконец, действительно ли системой, к которой пользователь не имеет прямого физического доступа, является квантовый компьютер, а не его эмулятор в классическом исполнении, где для имитации преобразования Уолша–Адамара, например, используется выход регистра сдвига с линейной обратной связью.

В рамках исследования авторы поставили перед собой цель, используя методы регрессионного анализа, определить, существуют ли приемлемые способы предварительного прогнозирования возможных результатов генерации случайных последовательностей на облачных КВУ, где квантовая схема выработки СП реализована путем применения вентиля Адамара. В то же время важное следствие проводимого исследования – наглядная демонстрация возможностей прогнозирования результатов применения к произвольному кубиту вентиля Адамара, используемого в большинстве квантовых алгоритмов. Изложенный подход может оказаться полезным при проектировании квантовых схем.

Наконец, в условиях постепенного становления индустрии квантовых технологий [12], а также в рамках последовательного внедрения перспективных и практически значимых направлений отрасли в действующую информационно-вычислительную инфраструктуру коммерческого и государственного секторов [13, 14] все большее внимание обращает на себя сложившаяся за последние десятилетия парадигма обеспечения защиты информации. В настоящее время архитектура информационной безопасности подвергается пересмотру в соответствии с актуальной повесткой технологического развития, а также с учетом места, занимаемого в ней зарождающейся экосистемой квантовых технологий [15]. И если на сегодняшний день применение СП, полученных на облачных КВУ, имеет ограниченный характер, то в обозримом будущем к функциональным возможностям КВУ, вероятно, могут отнести задачи выработки СП для систем защиты информации. Тем не менее каким бы путем не пошло дальнейшее развитие квантовых вычислений, выполненное исследование может оказаться полезным для формирования более цельного представления в рассматриваемой области.

**Генерация случайных чисел**

При работе с облачным квантовым компьютером в распоряжении пользователя имеется информация о технологии исполнения квантового устройства, известны топология процессора с точным расположением кубит и вектор ошибок каждого квантового состояния. Модель кубита зачастую остается неизвестной, в результате чего КВУ воспринимается в качестве черного ящика, имеющего некоторый вход и выход в классической форме записи. В таком случае все квантовые преобразования, начиная от инициализации и вплоть до момента измерения регистра, зачастую не поддаются однозначной верификации[*].

Для проектирования квантовой схемы пользователю достаточно знать сведения о приведенных исходных данных, чтобы оптимизировать взаимосвязи между квантовыми состояниями и минимизировать уровень возникновения потенциальных ошибок в программе.

Минимальной вычислительной единицей произвольного КВУ является единичный вектор в двумерном комплексном векторном пространстве.

$$|\psi\rangle = c_1|0\rangle + c_2|1\rangle, \qquad (1)$$

где $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$ – вычислительный базис.

Сформулируем задачу генерации случайных чисел на квантовом вычислительном устройстве. В простейшем случае при работе с одиночным кубитом (1) достаточно применить к нему преобразование Уолша–Адамара, задаваемое матрицей

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \qquad (2)$$

В таком случае кубит окажется в состоянии суперпозиции, которое по результатам измерения в базисе $|0\rangle$, $|1\rangle$ случайным равновероятным образом «сгенерирует» двоичное значение «0» или «1» в классической форме записи. Для генерации СП необходимой длины достаточно запустить изложенный процесс в цикле с соответствующим количеством повторений.

Заметим, что процесс измерения квантовых состояний возможен в двух вариациях:

– измерение каждого кубита по отдельности (режим «sampler»);

– измерение квантового регистра целиком (режим «estimator»).

Несмотря на разные подходы к выбору режима работы, авторы убеждены – в контексте задачи КГСЧ на КВУ необходимо рассматривать каждый кубит независимо от других состояний процессора.

Во-первых, снимая результаты со всего регистра, можно упустить наличие скрытых зависимостей между кубитами, которые могут не проявляться в явном виде. Во-вторых, каждый кубит отличается от соседних (как минимум вектором ошибок) и выступает в качестве независимого генератора СП, что означает отсутствие теоретических обоснований его использования совокупно с другими кубитами, где весь процессор будет расцениваться в качестве единого КГСЧ.

Таким образом, при разрядности КВУ в $N$ кубит, используя весь регистр с количеством запусков квантовой схемы $n$ раз, будет получено $N$ двоичных строк $\{z_i\}_{i=1}^{n}$ длины $n \in \mathbb{N}$.

**Прогнозируемые значения**

В процессе исследований были использованы многочисленные подходы к построению моделей предсказания качества, генерируемых на квантовых компьютерах СП (до непосредственного запуска квантовых схем КГСЧ). В рамках статьи авторы предлагают ознакомиться с тремя подходами, краткое содержание которых сформулировано в табл. 1.

Таблица 1

**Прогнозирование результатов выработки СП на КВУ**

| Подход | Модель | Предсказываемое значение |
|---|---|---|
| 1 | Множественная линейная регрессия | Количество «0» |
| | | Количество «1» |
| 2 | Множественная линейная регрессия | Количество пройденных тестов NIST STS |
| 3 | Логистическая регрессия | Качество кубита – равномерность СП |

Первый подход в рамках предварительного анализа КВУ в режиме работы КГСЧ – прогнозирование числа «0» и «1» от общей длины генерируемой последовательности. Ожидается, что по параметрам квантового состояния, зная об ошибке операции применения вентиля Адамара, с некоторой погрешностью можно определить ориентировочное соотношение числа нулей и единиц в итоговой последовательности. В случае корректности работы предложенной модели пользователь сможет исключать из проектируемой квантовой схемы кубиты, не способные к выработке СП с равномерным распределением «0» и «1», что может оказаться критичным как при выработке битовой строки, так и в рамках выполнения квантовых алгоритмов.

Второй подход – прогнозирование результатов применения к генерируемым с квантового компьютера случайным последовательностям статистических тестов NIST STS [16], направленных на выявление возможных закономерностей и паттернов, наличие которых может говорить о ненадежности используемого метода генерации случайных чисел[†]. NIST STS содержит 15 наборов тестов, некоторые из них содержат более одного алгоритма исследования СП. Каждый тест NIST STS рассчитывает значение P-value, на основании которого принимается реше-

[*] В этой связи процесс генерации СП с последующим анализом результата может послужить в качестве дополнительной проверки свойств исследуемого КВУ.

[†] С поправкой на сферу применения тестов NIST STS, которые в первую очередь предназначены для исследования программных ГСЧ. Анализ физических ГСЧ, в том числе КГСЧ, должен осуществляться в рамках применения соответствующих методик. Однако при невозможности преодоления последовательностями как минимум пороговых значений тестов NIST STS дальнейшее исследование свойств СП и КГСЧ может оказаться нецелесообразным.

ние о (не)прохождении исследуемой последовательности конкретного теста по заданному правилу. Предполагается, что СП может считаться случайной (с некоторым уровнем доверия, определяемым уровнем значимости α) в том случае, если все тесты пройдены успешно.

Учитывая невозможность выполнения тестирования последовательностей до их непосредственной генерации на облачном КВУ, для выявления наличия связи между статистическими свойствами ожидаемой СП и качеством отдельно взятого кубита, выступающего в роли самостоятельного КГСЧ, авторами было решено применить следующий подход.

Каждому кубиту ставится в соответствие некоторая обобщенная характеристика того, что генерируемые с квантового состояния последовательности будут успешно проходить тесты NIST STS. Тогда квантовое состояние будет определяться величиной, которую можно интерпретировать как вероятность кубита сгенерировать качественную СП.

Всем тестам были назначены числовые характеристики $\lambda_1, \lambda_2, \ldots, \lambda_k$ (где $k$ – число проводимых тестов)*. Величины $\lambda_i \in (0,100)$ назначались методом экспертных оценок с привлечением специалистов, имеющих опыт в предметной области. Значения $\lambda_i$ сформированы с учетом сведений из официальной документации NIST, функциональных возможностей и области применения отдельного теста в контексте решаемой задачи проверки случайных последовательностей, генерируемых на КГСЧ.

По итогу для каждого $j$-го теста вычислен весовой коэффициент

$$\alpha_j = \lambda_j \left( \sum_{i=1}^{k} \lambda_i \right)^{-1}, \quad (3)$$

где $\sum_{i=1}^{k} \alpha_i = 1$, тогда $0 < \alpha_j < 1$.

В табл. 2 представлены весовые коэффициенты одиночных тестов для каждого тематического блока тестирования NIST STS.

Таблица 2

**Соответствие коэффициентов тестам NIST STS**

| Набор тестов | $\alpha_j$ | Набор тестов | $\alpha_j$ |
|---|---|---|---|
| Frequency (1 тест) | 0,011697 | Runs (1 тест) | 0,009452 |
| Block Frequency (1 тест) | 0,011224 | Longest Run (1 тест) | 0,008861 |
| Cumulative (2 теста) | 0,010043 | Rank(1 тест) | 0,009452 |
| FFT (1 тест) | 0,010633 | Approximate (1 тест) | 0,008861 |
| Non Overl. (148 тестов) | 0,005907 | Serial (2 теста) | 0,009452 |
| Overlapping (1 тест) | 0,005907 | Linear (1 тест) | 0,010633 |

В рамках исследования не представлены универсальный тест Мауэра и два теста на произвольные отклонения. В связи с ограничением на длину СП, генерируемой с одного кубита, из-за недостаточного объема выборки исходных данных упомянутые тесты преимущественно выдают отрицательный результат, вследствие чего было решено исключить данные тесты из рассмотрения.

Выполнив распределение весовых коэффициентов между различными тестами (3), сформулируем порядок вычисления числовой характеристики $p$, отражающей качество кубита с точки зрения пройденных тестов:

$$p = \sum_{i=1}^{k} \alpha_i \chi(T_i), \quad (4)$$

где $\chi(T_i)$ – индикатор теста $T_i$, т.е.

$$\chi(T_i) = \begin{cases} 1, \text{ если тест пройден,} \\ 0, \text{ в противоположном случае.} \end{cases} \quad (5)$$

В результате генерации случайных чисел на КВУ разрядностью $N$ кубит по итогам выполнения тестирования $N$ двоичных строк $\{z_i\}_{i=1}^{n}$ длины $n \in \mathbb{N}$ пользователь получит $N$ числовых характеристик $p$, демонстрирующих качество кубита с точки зрения ожидаемого числового значения, отражающего успешность прохождения случайной последовательностью 12 наборов тестов NIST STS.

В качестве третьего подхода к прогнозированию результатов работы квантовой схемы будет проведено исследование возможности предсказания способности произвольного кубита сгенерировать качественную СП. Индикаторная переменная, отражающая качество кубита с точки зрения вырабатываемой им СП, будет демонстрировать равномерность распределения двоичных чисел, где при допустимом соотношении «0» и «1» кубиту ставится в соответствие значение 1, в противном случае – 0.

**Регрессионный анализ**

В целях исследования полученных последовательностей в контексте наличия зависимости итоговых результатов по отношению к техническим характеристикам облачного КВУ предлагается провести регрессионный анализ, позволяющий оценить, насколько сильно генерируемые СП зависят от параметров квантового оборудования. Для предсказания качества работы кубита в режиме КГСЧ будут использованы два вида математического моделирования: модель множественной линейной регрессии и модель бинарного выбора.

Модель множественной линейной регрессии имеет вид

$$\bar{y} = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_k x_k, \quad (6)$$

где $\beta_i$ – коэффициенты модели, $x_i$ – набор признаков, свойственных отдельному эксперименту.

Для прогнозирования работы КГСЧ на КВУ в качестве зависимых переменных $y$, относительно которых будут выполняться предсказания, выбраны три параметра, а именно – количество наблюдаемых «0» и «1» в итоговой последовательности (первый подход) и значение числовой характеристики $p$ (второй подход) (4).

* Распределение значений между тестами является условным и призвано отобразить возможный подход к проводимым исследованиям. Цель – (до запуска квантовой схемы) по имеющимся техническим параметрам КВУ определить, какие кубиты способны сгенерировать СП, проходящие наибольшее число тестов.

В рамках исследования третьего подхода, предложенного авторами, будет реализовано построение логит-модели, которая может быть записана как

$$F(w)=\frac{1}{1+e^{-w}}, \qquad (7)$$

где $w=\beta_0+\beta_1 x_1+\beta_2 x_2+\ldots+\beta_n x_n$ по аналогии с (6).

Зависимой бинарной переменной, используемой для построения пробит-модели, выбран индикатор (8), сигнализирующий о качестве кубита $\mu_{quality}$, что определяется по результатам (не)прохождения частотного побитового теста, входящего в набор инструментов NIST STS.

$$\mu_{quality}=\begin{cases}1, P_{value}\geq\alpha,\\ 0, P_{value}<\alpha,\end{cases} \qquad (8)$$

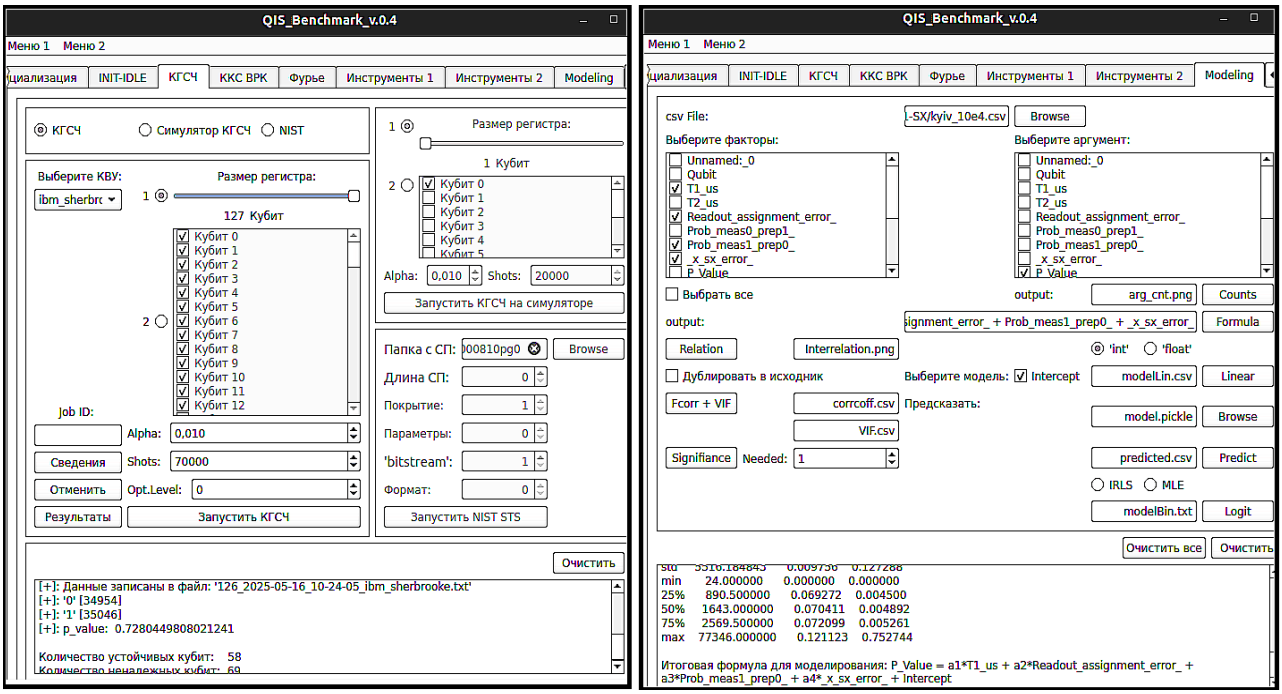
где α – уровень значимости.

Таким образом, в рамках работы ожидается получить 4 модели, исследование которых продемонстрирует возможность предварительной оценки качества работы облачного КВУ в режиме квантового генератора случайных чисел.

**Программный комплекс QISs**

В целях автоматизации выполняемых экспериментов, а также для обеспечения воспроизводимости полученных результатов заинтересованными исследователями авторами доработан функционал программного комплекса «QISs Benchmark» (Quantum Information Security) [17].

Программный код написан на языке Python, графический интерфейс разработан с помощью фреймворка QT5. Для работы с квантовыми компьютерами использована библиотека Qiskit. На рис. 1 представлены вкладки приложения, используемые при анализе свойств КВУ в режиме КГСЧ.




*а* *б*

Рис. 1. Интерфейс приложения QISs_v.0.3.10. Вкладки: генерации СП – *а*; построения регрессионных моделей – *б*

Панель программы «КГСЧ» (см. рис. 1, *а*) отвечает за построение квантовой схемы генерации СП. Пользователь выбирает КВУ, определяет кубиты, к которым будет применен вентиль Адамара (2), задает количество повторений схемы (shots), устанавливает уровень значимости α. Предусмотрена возможность запуска анализа СП набором тестов NIST STS.

Вкладка «Modeling» (см. рис. 1, *б*) разработана для облегчения процесса моделирования. Оператор выбирает .csv файл с исходными данными, определяет признаки и аргумент модели и проводит предобработку данных – графическое отображение соотношения двух факторов, построение корреляционной матрицы и коэффициента инфляции дисперсии (VIF, Variance inflation factor), отбор признаков методом RFE (Recursive feature elimination). В процессе моделирования пользователь имеет возможность редактировать формулу линейной регрессии в ходе работы программы в режиме «on-line», предусмотрены программные решения по сохранению итоговой модели и предсказанию результатов для новых файлов с произвольными структурированными данными.

**Оценка степени предсказуемости генерации случайных чисел на облачном КВУ**

Экспериментальная выборка выполнена на облачных КВУ «ibm_brisbane» и «ibm_kyvi». На каждом компьютере дважды сгенерированы пять СП с интервалом в $2\cdot10^4$ бит в диапазоне от $2\cdot10^4$ до $10^5$ бит. Для увеличения возможности выявления качественных изменений в калибровочных данных квантового компьютера временной промежуток между двумя экспериментами составил два месяца. Признаки (технические характеристики кубит), отобранные для анализа зависимых переменных, представлены в табл. 3.

Таблица 3

**Калибровочные данные КВУ как признаки модели**

| Параметр КВУ | Readout error | meas1 prep0 | meas0 prep1 | (sx) error |
|---|---|---|---|---|
| Значение | Ошибка чтения | Получение значения, ортогонального заданному | | Ошибка вентиля (sx) [native gate] |
| Признак модели | $X_1$ | $X_2$ | $X_3$ | $X_4$ |

Параметр «Readout error» отражает ошибку измерения кубита [находящегося в произвольном состоянии]; параметры «meas0/1 – prep1/0» – ошибка инициализации и измерения кубита (инициализация кубита в состояние $|0\rangle / |1\rangle$, после измерения ожидаемое значение ошибочно считывается как «1»/«0»); «SX error» – ошибка применения вентиля Адамара (перевод кубита в состояние суперпозиции).

Качество разрабатываемых моделей будет определяться статистическими мерами – коэффициентом детерминации $R^2$ и относительной погрешностью RSE (Residual standard error), которые рассчитываются следующим образом:

$$R^2 = \frac{\sum_{i=1}^{n}(\hat{y}_i - \bar{y}_i)^2}{\sum_{i=1}^{n}(y_i - \bar{y}_i)^2}, \qquad RSE = \sqrt{\frac{\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}{n-p-1}},$$

где $n$ – количество наблюдаемых, $p$ – количество признаков.

**Предсказание чисел «0» и «1»**

В рамках прогнозирования числа нулей и единиц от общей длины генерируемой последовательности в каждой из двух моделей в качестве признаков будут задействованы общие параметры $X_1$ и $X_4$ за исключением признаков $X_2$ и $X_3$, интерпретация которых в контексте сформулированных моделей является противоположной по смыслу.

Модель 1: прогнозирование количества «0»:

$$\bar{Y}_{\text{zeropred}} = \beta_0 + \beta_1 X_1 + \beta_2 X_3 + \beta_3 X_4 .$$

Результаты предсказания для наименее устойчивых кубит КВУ представлены в табл. 4.

Модель 2: прогнозирование количества «1»:

$$\bar{Y}_{\text{onepred}} = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_4 .$$

Результаты предсказания для наименее устойчивых кубит КВУ представлены в табл. 5.

Представленные результаты исследования демонстрируют низкий уровень погрешности сформулированных моделей, не зависящий от длины рассматриваемых последовательностей. Также следует отметить достаточно высокий уровень предсказательной возможности моделей [$R^2$], который в некоторой степени отличается для каждого квантового компьютера, что может быть обусловлено точностью предоставляемых вендором квантового оборудования калибровочных данных.

Выбор (представленных в таблицах) демонстрационных кубит для каждого КВУ обусловлен наличием качественного изменения (на десятые и сотые доли значений) технических параметров каждого из рассматриваемых (квантовых) состояний, изменчивость которых в наибольшей степени отражает результат моделирования. Оставшиеся 124 кубита склонны к большей устойчивости и стабильности (изменения параметров на тысячные доли значений), что служит менее наглядным примером работы модели.

**Кубит как категориальная переменная**

По результатам КГСЧ сгенерированные СП разбивались на два множества – успешно прошедшие частотный побитовый тест и двоичные строки, не удовлетворяющие предъявляемым требованиям к соотношению «0» и «1». Каждой СП ставилась в соответствие характеристика «Quality», отражающая качество двоичной строки по правилу (8).

Установив уровень значимости 0,01, авторы построили модель логистической регрессии (7), таблица попаданий которой представлена в табл. 6.

Таблица 4

**Результаты эксперимента предсказания количества «0»**

| ibm_brisbane | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Длина СП: | $2\cdot10^4$ бит | | $10\cdot10^4$ бит | | | | |
| | $R^2$ | 0,83977084 | | 0,82376291 | | | | |
| | Погрешность | 2% | | 2% | | Параметры КВУ | | |
| Дата | Кубит | $Y_{\text{zeroactual}}$ | $\bar{Y}_{\text{zeropredict}}$ | $Y_{\text{zeroactual}}$ | $\bar{Y}_{\text{zeropredict}}$ | $X_1$ | $X_3$ | $X_4$ |
| 25.01.2025 | 39 | 9 794 | 10 165 | 49 338 | 51 369 | 0,0537 | 0,0766 | 0,00059 |
| 06.03.2025 | 39 | 9 232 | 9 204 | 46 293 | 45 900 | 0,0631 | 0,015 | 0,00023 |
| 25.01.2025 | 95 | 10 949 | 10 109 | 55 154 | 50 703 | 0,02 | 0,0312 | 0,00014 |
| 06.03.2025 | 95 | 2 045 | 2 057 | 10 343 | 10 441 | 0,0935 | 0,0991 | 0,14092 |
| 25.01.2025 | 114 | 9 991 | 9 688 | 50 321 | 49 357 | 0,1307 | 0,13 | 0,00021 |
| 06.03.2025 | 114 | 8 926 | 9 453 | 45 128 | 48 230 | 0,1545 | 0,1401 | 0,00011 |
| ibm_kyvi | | | | | | | | |
| | Длина СП: | $2\cdot10^4$ бит | | $10\cdot10^4$ бит | | | | |
| | $R^2$ | 0,6594627 | | 0,7111679 | | | | |
| | Погрешность | 3% | | 3% | | Параметры КВУ | | |
| Дата | Кубит | $Y_{\text{zeroactual}}$ | $\bar{Y}_{\text{zeropredict}}$ | $Y_{\text{zeroactual}}$ | $\bar{Y}_{\text{zeropredict}}$ | $X_1$ | $X_3$ | $X_4$ |
| 28.01.2025 | 8 | 10 452 | 12 563 | 52 592 | 61 794 | 0,1528 | 0,2636 | 0,0575 |
| 05.03.2025 | 8 | 10 350 | 10 331 | 51 640 | 51 753 | 0,0449 | 0,0586 | 0,0007 |
| 28.01.2025 | 44 | 10 899 | 10 742 | 54 102 | 53 898 | 0,0724 | 0,1108 | 0,00072 |
| 05.03.2025 | 44 | 9 812 | 10 273 | 50 455 | 51 471 | 0,0617 | 0,0708 | 0,00064 |
| 28.01.2025 | 109 | 10 180 | 10 128 | 50 217 | 50 706 | 0,062(9) | 0,0622 | 0,00136 |
| 05.03.2025 | 109 | 17 464 | 16 667 | 88 673 | 84 789 | 0,4284 | 0,8251 | 0,00139 |

Таблица 5

**Результаты эксперимента предсказания количества «1»**

| ibm_brisbane | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Длина СП: | $2\cdot10^4$ бит | | $10\cdot10^4$ бит | | | | |
| | $R^2$ | 0,8397708 | | 0,82376291 | | | | |
| | Погрешность | 2% | | 2% | | Параметры КВУ | | |
| Дата | Кубит | $Y_{\text{oneactual}}$ | $\bar{Y}_{\text{onepredict}}$ | $Y_{\text{oneactual}}$ | $\bar{Y}_{\text{onepredict}}$ | $X_1$ | $X_2$ | $X_4$ |
| 25.01.2025 | 39 | 10 206 | 9 834 | 50 662 | 48 630 | 0,0537 | 0,3076 | 0,00059 |
| 06.03.2025 | 39 | 10 768 | 10 795 | 53 707 | 54 099 | 0,0631 | 0,1112 | 0,00023 |
| 25.01.2025 | 95 | 9 051 | 9 890 | 44 846 | 49 296 | 0,02 | 0,0088 | 0,00014 |
| 06.03.2025 | 95 | 17 955 | 19 942 | 89 657 | 89 558 | 0,0935 | 0,0878 | 0,14092 |
| 25.01.2025 | 114 | 10 009 | 10 311 | 49 679 | 50 642 | 0,1307 | 0,1314 | 0,00021 |
| 06.03.2025 | 114 | 11 074 | 10 546 | 54 872 | 51 769 | 0,1545 | 0,1689 | 0,00011 |
| ibm_kyvi | | | | | | | | |
| | Длина СП: | $2\cdot10^4$ бит | | $10\cdot10^4$ бит | | | | |
| | $R^2$ | 0,6594627 | | 0,71116787 | | | | |
| | Погрешность: | 3% | | 3% | | Параметры КВУ | | |
| Дата | Кубит | $Y_{\text{oneactual}}$ | $\bar{Y}_{\text{onepredict}}$ | $Y_{\text{oneactual}}$ | $\bar{Y}_{\text{onepredict}}$ | $X_1$ | $X_2$ | $X_4$ |
| 28.01.2025 | 8 | 9 548 | 7 436 | 47 408 | 38 205 | 0,1528 | 0,04199 | 0,0575 |
| 05.03.2025 | 8 | 9 650 | 9 668 | 48 360 | 48 246 | 0,0449 | 0,0312 | 0,0007 |
| 28.01.2025 | 44 | 9 101 | 9 257 | 45 898 | 46 101 | 0,0724 | 0,034 | 0,00072 |
| 05.03.2025 | 44 | 10 188 | 9 726 | 49 545 | 48 528 | 0,0617 | 0,0527 | 0,00064 |
| 28.01.2025 | 109 | 9 820 | 9 871 | 49 783 | 49 293 | 0,062(9) | 0,0638 | 0,00136 |
| 05.03.2025 | 109 | 2 536 | 3 332 | 11 327 | 15 210 | 0,4284 | 0,0317 | 0,00139 |

Таблица 6

**Таблица попаданий прогнозирования качества кубита в режиме КГСЧ**

| Модель с набором признаков ($X_1$; $X_2$; $X_4$) | | | | | | Модель с набором признаков ($X_1$; $X_4$) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ibm_brisbane | | | | | | | | | | | |
| $2\cdot10^4$ | $\bar{y}_{\text{pred}}0$ | $\bar{y}_{\text{pred}}1$ | $4\cdot10^4$ | $\bar{y}_{\text{pred}}0$ | $\bar{y}_{\text{pred}}1$ | $2\cdot10^4$ | $\bar{y}_{\text{pred}}0$ | $\bar{y}_{\text{pred}}1$ | $4\cdot10^4$ | $\bar{y}_{\text{pred}}0$ | $\bar{y}_{\text{pred}}1$ |
| $y_{\text{act}}0$ | 22 | 95 | $y_{\text{act}}0$ | 115 | 23 | $y_{\text{act}}0$ | 23 | 94 | $y_{\text{act}}0$ | 123 | 15 |
| $y_{\text{act}}1$ | 15 | 122 | $y_{\text{act}}1$ | 73 | 43 | $y_{\text{act}}1$ | 13 | 124 | $y_{\text{act}}1$ | 83 | 33 |
| ibm_kyv» | | | | | | | | | | | |
| $2\cdot10^4$ | $\bar{y}_{\text{pred}}0$ | $\bar{y}_{\text{pred}}1$ | $4\cdot10^4$ | $\bar{y}_{\text{pred}}0$ | $\bar{y}_{\text{pred}}1$ | $2\cdot10^4$ | $\bar{y}_{\text{pred}}0$ | $\bar{y}_{\text{pred}}1$ | $4\cdot10^4$ | $\bar{y}_{\text{pred}}0$ | $\bar{y}_{\text{pred}}1$ |
| $y_{\text{act}}0$ | 24 | 97 | $y_{\text{act}}0$ | 156 | 0 | $y_{\text{act}}0$ | 24 | 97 | $y_{\text{act}}0$ | 156 | 0 |
| $y_{\text{act}}1$ | 12 | 121 | $y_{\text{act}}1$ | 985 | 0 | $y_{\text{act}}1$ | 16 | 117 | $y_{\text{act}}1$ | 98 | 0 |

Как можно видеть, уже на малых длинах СП наблюдается сильное смещение предсказаний в одно из граничных состояний (преобладание «1» при длине СП $2\cdot10^4$ бит), которое сменяется на противоположное положение при небольшом увеличении объема выборки (преобладание «0» при длине СП $4\cdot10^4$ бит).

На первый взгляд может показаться, что данный подход не находит своего применения в поставленной задаче. Однако авторы предполагают – при планомерном изменении уровня значимости (например, увеличивая до 0,5 с шагом $10^{-1}$ или уменьшая в обратную сторону) можно добиться качественного улучшения получаемых результатов.

**Исследование статистических свойств СП средствами NIST STS**

Завершающим этапом исследования является предсказание результатов прохождения сгенерированных на КВУ последовательностей тестов NIST STS по правилу (3)–(5).

Модель 3: предсказание вероятности успешного прохождения тестов NIST STS:

$$\bar{P}_{\text{NISTpred}} = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_4 \cdot$$

В случае успешной работы модели можно говорить о возможности прогнозирования качества получаемых последовательностей, а следовательно, и об исследуемых кубитах как о самостоятельных генераторах случайных чисел. В то же время результат моделирования может указывать на кубиты, которые наилучшим образом оперируют с вентилем Адамара, устойчивое взаимодействие которых требуется в большинстве квантовых схем. Результаты моделирования представлены в табл. 7.

В отличие от моделей, предсказывающих количество «0» и «1», модель оценки квантовых состояний с точки зрения прохождения последовательностями тестов NIST STS с увеличением длины генерируемой СП значительно теряет в качестве, с ростом последовательности увеличивая наблюдаемую погрешность в прогнозируемых данных.

Тем не менее, несмотря на незначительные расхождения в актуальных и предсказанных значениях, можно заметить – модель имеет прочные основания для ее принятия и использования в качестве одного из подходов предварительной оценки квантовых состояний. С ее помощью можно выявлять наиболее неустойчивые кубиты, последовательности с которых предположительно пройдут наименьше количество тестов NIST STS.

Таблица 7

**Результаты эксперимента предсказания прохождения тестов NIST STS**

| ibm_brisbane | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Длина СП: | $2 \cdot 10^4$ бит | | $10 \cdot 10^4$ бит | | | | |
| | $R^2$ | 0,7329445 | | 0,4409993 | | | | |
| | Погрешность: | 3% | | 9% | | Параметры КВУ | | |
| Дата | Кубит | $P_{\text{NISTactual}}$ | $P_{\text{NISTpredict}}$ | $P_{\text{NISTactual}}$ | $P_{\text{NISTpredict}}$ | $X_1$ | $X_2$ | $X_4$ |
| 25.01.2025 | 39 | 0,9564 | 0,965358 | 0,94163 | 0,88879 | 0,0537 | 0,3076 | 0,00059 |
| 06.03.2025 | 39 | 0,82939 | 0,894285 | 0,73487 | 0,79585 | 0,0631 | 0,1112 | 0,00023 |
| 25.01.2025 | 95 | 0,86483 | 0,9742 | 0,58955 | 0,94121 | 0,02 | 0,0088 | 0,00014 |
| 06.03.2025 | 95 | 0,06379 | 0,065026 | 0,01063 | 0,00661 | 0,0935 | 0,0878 | 0,14092 |
| 25.01.2025 | 114 | 0,99409 | 0,905262 | 0,99409 | 0,72201 | 0,1307 | 0,1314 | 0,00021 |
| 06.03.2025 | 114 | 0,84711 | 0,88036 | 0,57183 | 0,66326 | 0,1545 | 0,1689 | 0,00011 |
| ibm_kyvi | | | | | | | | |
| | Длина СП: | $2 \cdot 10^4$ бит | | $10 \cdot 10^4$ бит | | | | |
| | $R^2$ | 0,5965468 | | 0,4249021 | | | | |
| | Погрешность: | 4% | | 9% | | Параметры КВУ | | |
| Дата | Кубит | $P_{\text{NISTactual}}$ | $P_{\text{NISTpredict}}$ | $P_{\text{NISTactual}}$ | $P_{\text{NISTpredict}}$ | $X_1$ | $X_2$ | $X_4$ |
| 28.01.2025 | 8 | 0,92627 | 0,69045 | 0,69588 | 0,55721 | 0,1528 | 0,04199 | 0,0575 |
| 05.03.2025 | 8 | 0,94104 | 0,93066 | 0,85302 | 0,88812 | 0,0449 | 0,0312 | 0,0007 |
| 28.01.2025 | 44 | 0,85421 | 0,88371 | 0,65453 | 0,83081 | 0,0724 | 0,034 | 0,00072 |
| 05.03.2025 | 44 | 0,95049 | 0,93138 | 0,95049 | 0,89036 | 0,0617 | 0,0527 | 0,00064 |
| 28.01.2025 | 109 | 0,97282 | 0,94492 | 0,999(9) | 0,90735 | 0,062(9) | 0,0638 | 0,00136 |
| 05.03.2025 | 109 | 0,12878 | 0,21821 | 0,01063 | 0,016669 | 0,4284 | 0,0317 | 0,00139 |

**Объем и результаты исследований. Перспективные направления**

С подробными результатами исследования, а также с программным кодом приложения QISs можно ознакомиться в облачном репозитории проектов GitHub [18].

Представленные в статье статистические материалы и результаты моделирования выступают в качестве краткого и наглядного отражения более полного исследования, выполнение которого предусматривало построение различных моделей с комбинированием имеющихся в распоряжении пользователя калибровочных данных облачных КВУ.

Так, к числу прогнозируемых значений авторы дополнительно относили такие величины, как P-value отдельных тестов NIST STS (рассматривая случаи с большим разбросом значений на отрезке [0, 1]), разницу между количеством «0» и «1» в СП.

Наравне с признаками, сформулированными в табл. 3, учитывалось время релаксации и дефазировки квантового состояния ($T_1$, $T_2$), брались их экспоненты с учетом времени работы квантовой схемы. Весь набор признаков комбинировался в различных вариациях (с учетом физики процесса и интерпретации параметров) для выявления наилучших результатов прогнозирования рассматриваемых моделей.

При разработке программного комплекса «QISs Benchmark» предусмотрены возможность предварительной выгрузки калибровочных данных КВУ и предсказание результатов КГСЧ при наличии модели одного из сформулированных в рамках статьи подходов, что упрощает пользователям взаимодействие с облачными квантовыми компьютерами в контексте оценки качества имеющихся квантовых состояний (вкладка «Инициализация»).

Структура облачного проекта с результатами исследований имеет 5 директорий:

– Data: исходные данные (двоичные последовательности и калибровочные параметры);

– Models_delta_0-1: результаты предсказания количества «0» и «1» (подход 1) и разницы между двоичными данными (в рамках статьи не рассматривается);

– Models_Pi: результаты прогнозирования прохождения выработанных СП тестов NIST STS (подход 2);

– Logit: модели оценки качества кубита на предмет равномерности распределения двоичных данных в последовательностях (подход 3);

– P-value: результаты предсказания P-value некоторых тестов NIST STS (в рамках статьи не рассматривается).

В каждой папке содержится множество подпапок, наименования которых демонстрируют, какие именно параметры КВУ использовались в качестве признаков моделей.

В качестве дальнейших направлений исследований авторами предполагается увеличение статистических данных и объема выборки, доработка модели бинарного выбора для улучшения результатов таблицы промахов и попаданий, выявление зависимости и чувствительности между параметрами КВУ и тестами NIST STS, а также проверка сгенерированных последовательностей по методикам, направленным на анализ физических генераторов случайных чисел.

**Заключение**

В рамках работы были сформулированы подходы к оценке потенциальной возможности прогнозирования результатов генерации случайных чисел на КВУ с помощью построения моделей множественной линейной регрессии и бинарного выбора.

Наилучшие результаты продемонстрировал подход, в рамках которого рассматривались модели прогнозирования количества «0» и «1» от общей длины СП. Модели показали стабильные результаты, не зависящие от длины СП, с незначительными отличиями точности для рассматриваемых КВУ.

Моделирование результатов прохождения последовательностями тестов NIST STS с ростом длины генерируемой СП уменьшает точность предсказания, но сохраняет возможность выявления наиболее ненадежных кубит. Данный подход может использоваться совместно с первым, выступая в качестве вспомогательного инструмента для принятия решения о включении кубита в квантовую схему для выработки СП.

Исследования в области построения модели бинарного выбора, в рамках которой кубит рассматривается как категориальная переменная, должны быть продолжены. Предполагается, что при изменении уровня значимости и длины последовательности можно получить более точную таблицу попаданий и промахов, отражающую результат работы модели.

Стоит отметить, что некоторые кубиты могут иметь предрасположенность к существенным отклонениям экспериментального результата по отношению к прогнозируемым величинам. Различия между предсказанием и фактическим значением может быть обусловлено двумя факторами. Во-первых, ошибкой на стороне вендора квантовых технологий, предоставляющего (не)умышленно некорректную информацию по конкретному кубиту. Во-вторых, помехами, возникающими в условиях активации всего квантового регистра, в результате чего функционирование наименее устойчивого к внешнему воздействию кубита может значительно отклониться от ожидаемого поведения квантового объекта (с чем авторам регулярно приходилось сталкиваться при исследовании точности инициализации КВУ).

По итогам выполненного исследования, в рамках которого квантовое вычислительное устройство использовалось в режиме работы квантового генератора случайных чисел, можно заключить, что, *обладая информацией о технических характеристиках квантового процессора*, с некоторым уровнем точности *можно спрогнозировать качество процесса установки произвольного кубита в состояние суперпозиции* (с учетом последующей операции измерения). Опираясь на предсказанные значения, можно спроектировать необходимую квантовую схему таким образом, чтобы используемый алгоритм задействовал наиболее устойчивые квантовые состояния (совокупно с вентилем Адамара), что может значительным образом сказаться на результатах.

В то же время сфера генерации случайных чисел напрямую связана с задачами обеспечения информационной безопасности. В таком случае выполненные исследования демонстрируют:

1. *Квантовые вычислительные устройства могут использоваться для решения задач генерации случайных последовательностей*. Малая разрядность современных КВУ накладывает ряд ограничений на скорость генерации СП, однако при масштабировании квантовых процессоров и улучшении технических свойств кубит ожидается возможность использования КВУ для генерации случайных чисел если не для потокового шифрования, то как минимум для выработки сеансовых ключей. На сегодняшний день генерируемые СП могут применяться исключительно в исследовательских задачах.

2. *Несовершенство квантового оборудования напрямую влияет на качество получаемых последовательностей*. В рамках исследования продемонстрирована возможность предсказания количества «0» и «1» (в генерируемых СП), а также прогнозирование вероятности кубита сформировать такую случайную последовательность, исследование которой статистическими тестами NIST STS будет давать наилучший результат. Преимущество предложенных подходов заключается в возможности оценки квантовых состояний до их непосредственного запуска.

3. В случае использования КВУ в режиме КГСЧ, *при наличии потенциального нарушителя*, получившего доступ к информации о технических характеристиках квантового компьютера, *злоумышленник может получить данные, по которым появляется возможность определить кубиты, генерирующие наиболее слабые последовательности*. В случае если нарушитель дополнительно осведомлен о математической модели используемых для КГСЧ кубит у него появляются все необходимые инструменты для проведения прикладного анализа чувствительной информации. Учитывая, что оператор, вырабатывающий двоичные строки на КВУ, может использовать весь квантовый регистр, не беря во внимание параметры задействованных кубит и не исключая из квантовой схемы слабые состояния, действующей системе информационной безопасности может быть нанесен непоправимый ущерб.

Однако на сегодняшний день применение современных квантовых компьютеров в задачах обеспечения защиты информации не представляется возможным. В конечном итоге, имея запас времени до момента формирования технологии в практически значимые индустриальные решения, необходимо продолжать научную деятельность по выявлению возможностей применения квантовых процессоров в прикладных задачах. В качестве одного из направлений, внимание которому авторы планируют уделить в дальнейшем, – анализ генерируемых квантовым компьютером случайных последовательностей на независимость, где в качестве инструмента исследования могут выступить соответствующие методики [19], направленные на исследование свойств именно физических генераторов случайных чисел.

*Литература*

1. Балыгин К.А. Реализация квантового генератора случайных чисел: экстракция доказуемо случайных битовых последовательностей из коррелированных марковских цепочек / К.А. Балыгин, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. – 2024. – Т. 119, № 7. – С. 533–544.

2. Гайдаш А.А. Математическая модель квантового генератора случайных чисел на основе флуктуации вакуума / А.А. Гайдаш, Р.К. Гончаров, А.В. Козубов, П.В. Яковлев // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. – 2024. – Т. 20, № 2. – С. 136–153.

3. Петренко А.А. Генерация случайных чисел с использованием массива связанных лазеров на основе микростолбиков с квантовыми точками / А.А. Петренко, А.В. Ковалев, В.Е. Бугров // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т. 21, № 6. – С. 962–968.

4. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information / T. Gehring, C. Lupo, A. Kordts et al. // Nat Commun. – 2021. – Vol. 12. – P. 605.

5. Орлов М.А. Оценка статистических свойств и криптографической стойкости случайных последовательностей, полученных квантовым компьютером IBM / М.А. Орлов, К.А. Нечаев, С.А. Резниченко // Безопасность информационных технологий. – 2023. – Т. 30, № 1. – С. 14–26.

6. Quantum random number generator using a cloud superconducting quantum computer based on source-independent protocol / Y. Li, Y. Fei, W. Wang et al. // Sci. Rep. – 2021. – Vol. 11. – P. 23873.

7. Hybrid Hadamard and Controlled-Hadamard Based Quantum Random Number Generators in IBM QX / R. Salehi, M. Razaghi, B. Fotouhi. // Physica Scripta. – 2022. – Vol. 97, № 6. – P. 065101.

8. Partial loopholes free device-independent quantum random number generator using IBM's quantum computers / A. Yadav, S. Mishra, A. Pathak. // Physica Scripta. – 2024. – Vol. 99, No. 11. – P. 115103.

9. Preskill J. Quantum computing in the NISQ era and beyond // Quantum. – 2018. – Vol. 2. – P. 79.

10. Randomized Compiling for Scalable Quantum Computing on a Noisy Superconducting Quantum Processor / A. Hashim, R. Naik, A. Morvan, J. Ville et al. // Physical Review X. – 2021. – Vol. 11, No. 4. – P. 041039.

11. Крючков А.А. Неочевидные аспекты бенчмарка квантовых вычислительных устройств на примере генерации случайных чисел / А.А. Крючков, К.Е. Комогоров // Правовая информатика. – 2024. – № 4. – С. 42–52.

12. Дорожная карта развития «сквозной» технологии «Квантовые технологии» // Минцифры РФ. – 2019 [Электронный ресурс]. – URL: https://digital.gov.ru/uploaded/files/07102019kvantyi.pdf (дата обращения: 11.07.2025).

13. Овсянников А.П. О проекте межуниверситетской квантовой сети / А.П. Овсянников, Б.М. Шабанов // Программные продукты и системы. – 2023. – Т. 36, № 4. – С. 695–702.

14. Alibrahim O. Unveiling Samsung Quantum Galaxy: Securing Smartphones With Quantum and Post-Quantum Cryptography // IEEE. – 2025. – Vol. 13. – P. 73202–73218.

15. В России разработан криптографический механизм, способный выдерживать атаки квантовых компьютеров // ТК-26. – 2024 [Электронный ресурс]. – URL: https://tc26.ru/news/novosti-kriptografii/v-rossii-razrabotan-kriptograficheskiy-mekhanizm-sposobnyy-vyderzhivat-ataki-kvantovykh-kompyuterov.html (дата обращения: 11.07.2025).

16. NIST SP 800-22. Набор статистических тестов для проверки работы генераторов случайных чисел и генераторов псевдослучайных чисел для криптографических приложений // NIST. – 2011 [Электронный ресурс]. – URL: https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software (дата обращения: 07.07.2025).

17. Патент РФ № RU2025613655. QISs_v.0.3.9 // Патент России № 2025611456, 2025. заявл. 28.01.2025. опубл. 13.02.2025 / А.А. Крючков.

18. Облачный репозиторий проектов GitHub // QISs. – 2025 [Электронный ресурс]. – URL: https://github.com/cyberravenman/QISs/tree/main/Expierement/Data%2BModels (дата обращения: 11.07.2025).

19. Проект методики по криптографической защите информации // ТК-26. – 2025 [Электронный ресурс]. – URL: https://tc26.ru/forum/viewtopic.php?f=61&t=1299&p=3441&hilit=ФГСЧ#p3441 (дата обращения: 11.07.2025).

---

**Крючков Андрей Андреевич**
Аспирант, ст. преп. каф. информационной безопасности Института искусственного интеллекта ФГБОУ ВО «МИРЭА – Российский технологический университет»
Вернадского пр-т, 78, г. Москва, Россия, 119454
ORCID: 0009-0002-4750-6204
Тел.: +7 (499) 600-80-80
Эл. почта: kryuchkov_a@mirea.ru

**Пастухова Юлия Ивановна**
Канд. физ.-мат. наук, доцент, с.н.с. лаб. стохастической оптимизации и теории риска Центрального экономико-математического института (ЦЭМИ) РАН,
доцент каф. информационной безопасности Института искусственного интеллекта ФГБОУ ВО «МИРЭА
Нахимовский пр-т, д. 47, г. Москва, Россия, 117209
Тел.: +7 (499) 129-16-44
Эл. почта: pastuhova_yu@mirea.ru

Поступила в редакцию: 19.05.2025.
Принята к публикации: 18.07.2025.

Kryuchkov A.A., Pastuhova J.I.

**Approaches to predicting the results of generating random binary sequences on quantum computing devices**

The functionality of the application with a graphical interface for generating binary sequences on cloud quantum computers has been improved by adding software tools for building regression models. Multiple linear regression and binary selection models have been built, using the current technical characteristics of quantum states as independent parameters. The predicted values reflect the expected results of testing the sequences with the NIST STS statistical test set, as well as the degree of uniformity in the distribution of «0» and «1» in the generated sequences. Based on information about the current technical characteristics of the quantum processor, the study proposes approaches for predicting the results of random number generation on quantum computing devices, which can be useful in designing a quantum circuit before it is actually run.

**Keywords:** quantum computer; random number generation; qubit; regression analysis.
**DOI:** 10.21293/1818-0442-2025-28-2-96-105

*References*

1. Balygin, K.A., Kulik, S.P. Molotkov, S.N. Realizatsiya Kvantovogo Generatora Sluchajnyh Chisel: Ekstraktsiya Dokazuemo Sluchajnyh Bitovyh Posledovatel'nostej Iz Korrelirovannyh Markovskih Tsepochek [Implementation of a Quan-

tum Generator of Random Numbers: Extraction of Provably Random Bit Sequences from Correlated Markov Chains]. *Jetp Lett,* 2024, vol. 119, pp. 538–548 (in Russ.).

2. Gaidash A.A., Goncharov R.K., Kozubov A.V., Yakovlev P.V. Matematicheskaya model' kvantovogo generatora sluchajnyh chisel na osnove fluktuatsii vakuuma [Mathematical model of random number generator based on vacuum fluctuations]. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2024, vol. 20, no. 2, pp. 136–153 (in Russ.).

3. Petrenko A.A., Kovalev A.V., Bougrov V.E. Generatsiya Sluchajnyh Chisel S Ispol'zovaniem Massiva Svyazannyh Lazerov Na Osnove Mikro-Stolbikov S Kvantovymi Tochkami [Random number generation with arrays of coupled quantumdot micropillar lasers]. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 6, pp. 962–968 (in Russ.).

4. Gehring, T., Lupo, C., Kordts, A. et al. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. *Nat Commun,* 2021, vol. 12, p. 605.

5. Orlov M.A., Nechaev K.A., Reznichenko S.A. Otsenka Statisticheskih Svojstv I Kriptograficheskoj Stojkosti Sluchajnyh Posledovatel'no-Stej, Poluchennyh Kvantovym Komp'yuterom IBM [Evaluation of statistical properties and cryptographic strength of random sequences obtained by an IBM quantum computer]. *IT Security*, 2023, vol. 30, no. 1, pp. 14–26 (in Russ).

6. Li Y., Fei Y., Wang W. et al. Quantum random number generator using a cloud superconducting quantum computer based on source-independent protocol. *Sci Rep 11*, 2021, vol. 11, p. 23873.

7. Salehi, R., Razaghi M., Fotouhi B. Hybrid Hadamard and Controlled-Hadamard Based Quantum Random Number Generators in IBM QX. *Physica Scripta*, 2022, vol. 97, no. 6, p. 065101.

8. Yadav A., Mishra S., Pathak A. Partial loopholes free device-independent quantum random number generator using IBM's quantum computers. *Physica Scripta*, 2024, vol. 99, no. 11, p. 115103.

9. Preskill J. Quantum computing in the NISQ era and beyond. *Quantum*, 2018, vol. 2, pp. 79.

10. Hashim A., Naik R., Morvan A., Ville J., Mitchell B., et al. Randomized Compiling for Scalable Quantum Computing on a Noisy Superconducting Quantum Processor. *Physical Review X*, 2021, vol. 11, no. 4, p. 041039.

11. Kryuchkov A.A., Komogorov K.E. Neochevidnye Aspekty Benchmarka Kvantovyh Vychislitel'nyh Ustrojstv Na Primere Generatsii Sluchajnyh Chisel [Non-obvious aspects of the benchmark of quantum computing devices on the example of quantum random number generation]. *Legal Informatics*, 2024, no. 4. pp. 42–52 (in Russ.).

12. Road Map «Quantum Technology». The Ministry of Digital Development, Communications and Mass Media of the Russian Federation. 2019 (in Russ.). Available at: https://digital.gov.ru/uploaded/files/07102019kvantyi.pdf (Accessed: 11 July 2025).

13. Ovsyannikov A.P., Shabanov B.M. O Proekte Mezhuniversitetskoj Kvantovoj Seti [On an interuniversity quantum network project]. *Software and Systems,* 2023, vol. 36, no. 4, pp. 695–702 (in Russ.).

14. Alibrahim O. Unveiling Samsung Quantum Galaxy: Securing Smartphones with Quantum and Post-Quantum Cryptography. *IEEE*, 2025, vol. 13, pp. 73202–73218.

15. V Rossii razrabotan kriptograficheskij mekhanizm, sposobnyj vyderzhivat' ataki kvantovyh komp'yuterov [Russia has developed a cryptographic mechanism that can withstand attacks by quantum computers]. Technical Committee 26, 2024. (in Russ.). Available at: https://tc26.ru/news/novosti-kriptografii/v-rossii-razrabotan-kriptograficheskiy-mekhanizm-sposobnyy-vyderzhivat-ataki-kvantovykh-kompyuterov.html (Accessed: 11 July 2025).

16. NIST SP 800-22. Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. 2010. Available at: https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software (Accessed: 07 July 2024).

17. Kryuchkov A.A., *QISs_v.0.3.9*. Patent RF, no. RU2025613655, 2025.

18. Developer platform GitHub. «QISs». 2025. Available at: https://github.com/cyberravenman/QISs/tree/main/Expierement/Data%2BModels (Accessed: 11 July 2025).

19. Draft methodology for cryptographic information protection. Technical Committee 26. 2025. (in Russ.). Available at: https://tc26.ru/forum/viewtopic.php?f=61&t=1299&p=3441&hilit=ФГСЧ#p3441 (Accessed: 11 July 2025).

---

**Andrey A. Kryuchkov**
Graduate student, senior lecturer, Federal State Budgetary Educational Institution of Higher Education «MIREA – Russian Technological University», Institute of Artificial Intelligence, Department of Information Security
78, Vernadskogo pr., Moscow, Russia, 119454
ORCID: 0009-0002-4750-6204
Phone: +7 (499) 600-80-80
Email: kryuchkov_a@mirea.ru

**Julia I. Pastuhova**
Candidate of Physical and Mathematical Sciences, Associate Professor, Senior Researcher at the Laboratory of Stochastic Optimization and Risk Theory at the Central Economic Mathematical Institute of the Russian Academy of Sciences, Associate Professor, Federal State Budgetary Educational Institution of Higher Education «MIREA – Russian Technological University», Institute of Artificial Intelligence, Department of Information Security
47, Nakhimovsky pr., Moscow, Russia, 117209
Phone: +7 (499) 129-16-44
Email: pastuhova_yu@mirea.ru

Received: 19.05.2025.
Accepted: 18.07.2025.