**КОМПЬЮТЕРНЫЕ ИССЛЕДОВАНИЯ**
**И МОДЕЛИРОВАНИЕ 2026 Т. 18 № 5 С. 1129–1159**
DOI: 10.20537/2076-7633-2026-18-5-1129-1159

Ки&М

**МОДЕЛИ В ФИЗИКЕ И ТЕХНОЛОГИИ**

УДК: 681.5.015

# Анализ применимости QUBO-алгоритмов в области информационной безопасности. Достоинства и недостатки

**К. Ю. Хубиев[1,a], Я. А. Холодов[1,b], А. С. Петренко[2,c]**

[1]Научно-технологический университет «Сириус»,
Россия, 354340, Краснодарский край, Федеральная территория «Сириус», пгт Сириус,
проспект Олимпийский, д. 1
[2]Санкт-Петербургский федеральный исследовательский центр Российской академии наук,
Россия, 199178, г. Санкт-Петербург, 14-я линия В.О., д. 39

E-mail: [a] kasymkhankhubievnis@gmail.com, [b] holodov.ya@talantiuspeh.ru, [c] a.petrenko1999@rambler.ru

*Получено 02.04.2026, после доработки — 21.07.2026.*
*Принято к публикации 02.10.2026.*

Квадратичная неограниченная бинарная оптимизация (*QUBO*) зарекомендовала себя в качестве эффективного инструмента для решения NP-трудных задач в области информационной безопасности. В QUBO-формулировке задача описывается в виде квадратичной функции бинарных переменных, минимум которой соответствует оптимальному решению. Такая запись учитывает линейные (индивидуальное влияние) и квадратичные (парные взаимодействия) зависимости. Особенно примечательно, что QUBO-алгоритмы можно имплементировать в квантовые вычислительные устройства на основе отжига, например *D-Wave*, которые позволяют найти собственное состояние гамильтониана соответствующей модели Изинга посредством квантовых или гибридных алгоритмов. При этом решение QUBO-задачи можно получить и на полностью классической архитектуре. Такие алгоритмы называют квантово вдохновленными, потому что они имитируют физические явления. Примером таких квантово вдохновленных алгоритмов являются симулированный отжиг (Simulated Annealing, SA) и симулированные бифуркации (Simulated Bifurcation, SB). За последние 5–7 лет большое количество работ было посвящено применению QUBO-формулировки для разнообразных задач информационной безопасности, начиная от взлома ключей безопасности до детекции атак, с целью доказать эффективность новых вычислительных парадигм. В данном исследовании мы анализируем эти работы, сгруппировав их по области применения и выделяя архитектурные подходы (квантовая, гибридная, классическая) в каждом сценарии. Мы уделяем внимание тому, как задача была переформулирована в QUBO-постановку или модель Изинга, анализируем ключевые стратегии решения и полученные результаты на оптимальность, масштабируемость, сложность. Мы выделяем основные преимущества и недостатки каждой QUBO-постановки в контексте информационной безопасности и в заключение обсуждаем актуальные задачи и перспективные направления для исследований.

Ключевые слова: информационная безопасность, квантовый отжиг, квантовые вычисления, QUBO

Работа выполнена при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение № 23-03 от 27.09.2024 г.).

© 2026 Касымхан Юсуфович Хубиев, Ярослав Александрович Холодов, Алексей Сергеевич Петренко
Статья доступна по лицензии Creative Commons Attribution-NoDerivs 3.0 Unported License.
Чтобы получить текст лицензии, посетите веб-сайт http://creativecommons.org/licenses/by-nd/3.0/
или отправьте письмо в Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

**COMPUTER RESEARCH AND MODELING**
**2026 VOL. 18 NO. 5 P. 1129–1159**
DOI: 10.20537/2076-7633-2026-18-5-1129-1159

Ки&М

**MODELS IN PHYSICS AND TECHNOLOGY**

UDC: 681.5.015

# A comprehensive review of common QUBO solvers in the cybersecurity domain. Advantages and disadvantages

**K. Yu. Khubiev[1,a], Ya. A. Kholodov[1,b], A. S. Petrenko[2,c]**

[1]Sirius University of Science and Technology,
1 Olimpiyskiy ave., Sirius, Sirius Federal Territory, Krasnodar region, 354340, Russia
[2]St. Petersburg Federal Research Center of the Russian Academy of Science,
39 14th Line V.O., St. Petersburg, 199178, Russia

E-mail: [a] kasymkhankhubievnis@gmail.com, [b] holodov.ya@talantiuspeh.ru, [c] a.petrenko1999@rambler.ru

*Received 02.04.2026, after completion — 21.07.2026.*
*Accepted for publication 02.10.2026.*

Quadratic Unconstrained Binary Optimization (QUBO) provides a common modeling framework for combinatorial optimization problems arising in cybersecurity. This review analyzes how cryptanalytic constraints, anomaly-detection objectives, network-defense tasks and cyber-risk models can be encoded as QUBO or equivalent Ising formulations. We compare three classes of solvers used in the literature: physical quantum annealers, hybrid quantum-classical workflows and quantum-inspired classical heuristics such as simulated annealing and simulated bifurcation. Particular attention is paid to the gap between formal QUBO expressiveness and practical solvability on current hardware, including embedding overhead, limited connectivity, noise and scaling constraints. The reviewed studies are grouped by application domain and assessed in terms of model size, solution quality, runtime indicators and reproducibility of computational settings. We show that QUBO is already useful as a unifying language for cybersecurity optimization, while near-term practical advantages are most plausible in hybrid and quantum-inspired settings rather than in fully quantum implementations. The review concludes by outlining open problems in QUBO construction, decomposition, sparsification and benchmarking for cybersecurity applications.

Keywords: cybersecurity, quantum annealing, quantum computation, QUBO

Citation: *Computer Research and Modeling*, 2026, vol. 18, no. 5, pp. 1129–1159 (Russian).

This work was obtained with the financial support of the project “Technologies for countering previously unknown quantum cyber threats”, implemented within the framework of the state program of the “Sirius” Federal Territory “Scientific and technological development of the ‘Sirius’ Federal Territory” (Agreement No. 23-03 dated September 27, 2024).

© 2026 Kasymkhan Yu. Khubiev, Yaroslav A. Kholodov, Alexey S. Petrenko
This work is licensed under the Creative Commons Attribution-NoDerivs 3.0 Unported License.
To view a copy of this license, visit http://creativecommons.org/licenses/by-nd/3.0/
or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

## Введение

В условиях роста загруженности вычислительных ресурсов и физических ограничений развития существующих технологий, включая пределы классического масштабирования интегральных схем [Moore, 1965; Dennard et al., 1974], квантовые вычисления рассматриваются как потенциальный источник технологического роста. Квантовые устройства не являются панацеей и универсальным решением, однако квантовые эффекты суперпозиции, интерференции и запутанности позволяют достичь ускорения и увеличения производительности вычислений для определенного класса задач. Вычислительные возможности и высокая степень параллелизма обеспечивают большой потенциал квантовых вычислений, но в то же время представляют собой определенную угрозу.

В мире, где многие процессы переходят в цифровую среду, начиная от повседневных покупок, общения и заканчивая государственными услугами, финансовыми транзакциями и управлением имуществом, кибербезопасность выходит на первый план. Для криптографии значимость квантовых вычислений носит особый характер, поскольку многие криптографические алгоритмы опираются на предположения о вычислительной сложности. Алгоритм Шора [Shor, 1994] демонстрирует эффективность квантовой архитектуры в задачах факторизации целых чисел и вычисления дискретного логарифма, лежащих в основе RSA, классических схем Диффи – Хеллмана и криптосистем на эллиптических кривых. Квантовые алгоритмы позволяют решать задачи дешифрования за полиномиальное время на достаточно мощном и устойчивом квантовом компьютере. Под мощным компьютером здесь подразумевается возможность масштабирования числа кубитов пропорционально увеличению длины шифра. Даже в случаях, когда алгоритм Шора неприменим для атак, алгоритм Гровера [Grover, 1997] обеспечивает квадратичное ускорение неструктурированного поиска, влияя на перебор ключей и параметры симметричной криптографии. Проведенные исследования и экспериментальные результаты привели к масштабным инициативам по переходу к постквантовой криптографии, включая многораундовый процесс стандартизации NIST и разработку рекомендаций по миграции.

При этом квантовые вычисления в криптографии не ограничиваются задачами «взлома» шифров. Проектирование, анализ и реализация криптографических систем тесно связаны с задачами оптимизации, включая восстановление ключей как задачу удовлетворения ограничений, поиск дифференциальных и линейных характеристик, подбор параметров при компромиссе между безопасностью и производительностью, настройку контрмер против атак по побочным каналам, а также распределение ресурсов в криптографических сетях. В подобных задачах квантовая оптимизация становится значимой не столько как универсальный ускоритель, сколько как альтернативная вычислительная парадигма для семейства задач бинарной оптимизации, которые могут быть сформулированы в виде задачи минимизации энергии системы.

Ключевым связующим звеном между дискретной оптимизацией и квантовыми вычислительными архитектурами является модель Изинга [Ising, 1925]. Изначально она была предложена в рамках статистической физики для описания взаимодействий между спинами. Базовая задача оптимизации в данной модели формулируется как поиск основного состояния системы — конфигурации гамильтониана, при которой достигается минимум энергии. Модель задается набором спинов с дискретными состояниями, локальными полями и парными взаимодействиями. Такая формализация естественным образом встраивается в парадигмы адиабатических квантовых вычислений (Adiabatic Quantum Computing, AQC) и квантового отжига (Quantum Annealing, QA) [Farhi et al., 2000; Farhi et al., 2001; Albash, Lidar, 2018]. Препринт [Farhi et al., 2000] используется как исторически значимый источник исходной формулировки AQC, а опубликованная работа [Farhi et al., 2001] дополняет его экспериментальным исследованием адиабатического алгоритма на разных примерах NP-полных задач. Эти подходы основываются на адиабатическом квантовом процессе, при котором при достаточно медленном изменении гамильтониана

система остается в основном состоянии. В рамках данной постановки система инициализируется в известной конфигурации и затем эволюционирует к гамильтониану целевой задачи, а найденное основное состояние соответствует решению оптимизационной задачи. Квантовый отжиг, в частности, представляет собой квантовую реализацию классического алгоритма имитации отжига, в которой переходы между состояниями обеспечиваются квантовыми флуктуациями. Основы данного подхода были заложены в исследованиях модели Изинга с поперечными полями [Kadowaki, Nishimori, 1998]. Экспериментальная реализация программируемых систем искусственных спинов [Johnson et al., 2011] заложила фундамент для практического применения квантового отжига как метода поиска глобального минимума энергетического ландшафта модели Изинга.

На практике стандартной формой постановки подобных задач оптимизации является модель квадратичной неограниченной бинарной оптимизации (Quadratic Unconstrained Binary Optimization, QUBO):

$$\min_{\mathbf{x}\in\{0,1\}^n} \mathbf{x}^T\mathbf{Q}\mathbf{x}, \tag{1}$$

которая является алгебраическим эквивалентом широкого класса задач, формулируемых в рамках модели Изинга.

Формулировка QUBO привлекательна тем, что предлагает универсальную целевую функцию: ограничения включаются в нее в виде штрафных слагаемых, а полиномы Жегалкина высоких порядков могут быть сведены к квадратичной форме путем введения вспомогательных переменных. Эти свойства позволяют применять QUBO к широкому классу NP-трудных задач и задач псевдобулевой оптимизации [Boros, Gruber, 2012]. Кроме того, многие NP-трудные задачи допускают явное отображение в модель Изинга или QUBO [Lucas, 2014], что позволяет проводить как качественную, так и количественную оценку эффектов перехода к квантовым вычислительным архитектурам.

Однако существуют фундаментальные физические ограничения: поиск основного состояния гамильтониана модели Изинга в общем случае является NP-трудной задачей [Barahona, 1982]. Таким образом, квантовый отжиг не устраняет NP-трудность, а предоставляет новые эвристические — и в ряде случаев алгоритмические — подходы к исследованию энергетического ландшафта системы состояний. Разрыв между теоретической эффективностью и реальной мощностью формализмов QUBO и Изинга, с одной стороны, и физическими ограничениями реальных квантовых устройств, связанными с шумами, стабильностью квантовых систем, точностью управления и сложностью встраивания задач, с другой стороны, определяет актуальную научную повестку в области квантовой оптимизации.

В криптографии текущая исследовательская повестка носит достаточно прикладной характер: значительное число работ сфокусировано на криптоаналитических задачах, включающих факторизацию, решение систем булевых уравнений и формализацию ограничений блочных и потоковых шифров в QUBO-постановке, пригодной для решателей на основе квантового отжига [Zhang, Feng, 2022]. Работа [Zhang, Feng, 2022] включена в обзор, поскольку содержит специализированное изложение конкретных преобразований криптографических задач к постановкам QUBO и квантового отжига, не сведенное к общим положениям о квантовой оптимизации. Результаты подобных исследований потенциально способствуют развитию альтернативных подходов к криптоанализу. В отличие от вентильных квантовых алгоритмов, требующих построения длинных когерентных цепочек операций, как в алгоритме Шора, криптографическая структура в рамках QUBO может быть представлена в виде энергетической функции, которая с использованием квантового, классического или гибридного отжига приводится к конфигурации с минимальной энергией, соответствующей ключу шифрования или допустимому решению.

Параллельно с быстрым развитием квантовых технологий QUBO-формализм превратился в практичный инструмент и универсальный интерфейс для оптимизации, предоставляющий

различные вычислительные парадигмы для алгоритмических решателей. Решатели, основанные на физических аналогиях, часто относят к классу квантово вдохновленных алгоритмов. Существуют реализации таких подходов на классических, гибридных и квантовых вычислительных архитектурах. В классическом случае метаэвристика симулированного отжига представляет собой устойчивый метод поиска состояний с минимальной энергией за счет медленного понижения температуры системы и имитации адиабатической эволюции. Данный метод является одним из стандартных инструментов для решения задач QUBO. Помимо него, существуют и другие квантово вдохновленные алгоритмы, позволяющие моделировать физические процессы без использования реальной квантовой когерентности. Характерным примером является алгоритм симулированной бифуркации, основанный на нелинейной динамике системы и явлении бифуркации для эффективного исследования энергетического ландшафта модели Изинга. Аналогичные принципы реализуются и на квантовой архитектуре: в рамках адиабатических квантовых вычислений и квантового отжига параметры задачи кодируются во времязависимом гамильтониане системы, который эволюционирует таким образом, чтобы в финальный момент система находилась в основном состоянии, соответствующем глобальному минимуму энергии.

В данной работе рассматриваются QUBO-решатели и основные вариации алгоритмов квантового отжига. Вначале анализируются физические основы квантового отжига, затем их применение в задачах QUBO-оптимизации. И наконец проводится сравнительный анализ эффективности различных моделей в криптографическом контексте с выявлением их сильных и слабых сторон. В заключение формулируются предположения о возможных направлениях совершенствования адиабатических квантовых вычислений и их применимости в задачах квантовой безопасности.

### *Методика отбора литературы*

Отбор источников проводился в несколько этапов. Сначала выполнялся широкий поиск публикаций по основным базам научной литературы, затем найденные работы проверялись на соответствие тематике обзора и наличие воспроизводимой оптимизационной постановки. Первичный поиск выполнялся в базах IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Google Scholar и arXiv. Использовались комбинации запросов QUBO cybersecurity, quantum annealing cryptanalysis, Ising formulation cryptography, QUBO anomaly detection, quantum annealing network security, quantum-inspired optimization cybersecurity и D-Wave QUBO security. Поисковые запросы использовались только как начальный механизм обнаружения релевантных источников; само включение публикации в обзор определялось не наличием отдельного термина в названии или аннотации, а соответствием содержательным критериям.

После первичного поиска публикации проходили содержательный просмотр по аннотации, постановке задачи и экспериментальному разделу. В обзор включались работы, удовлетворяющие следующим условиям: рассматриваемая задача относится к одному из прикладных направлений статьи (криптоанализ, обнаружение аномалий, сетевая безопасность, размещение защитных ресурсов или оценка киберрисков); в работе явно задана QUBO-постановка, постановка в модели Изинга или близкая псевдобулевая формализация; описано соответствие между предметными переменными задачи и бинарными переменными оптимизационной модели; приведены сведения о размерности модели, об используемом решателе, экспериментальных результатах, о вычислительных ограничениях или процедуре преобразования исходной задачи к QUBO-постановке или модели Изинга. После содержательного просмотра работы группировались в узкие тематические кластеры: криптоаналитические QUBO-постановки, детекция аномалий, сетевые графовые задачи, размещение защитных ресурсов, оптимизация политик защиты и оценка киберрисков. Затем близкие по математической структуре постановки объединялись в более крупные группы, что позволило сопоставлять не только публикации из кибербезопасности, но и реле-

вантные задачи из смежных областей. Например, задачи размещения honeypot-систем, сенсоров или защитных узлов рассматривались вместе с задачами покрытия, размещения объектов и логистической оптимизации, а задачи сегментации или прореживания сети сопоставлялись с графовым разбиением, минимальным разрезом, размещением ресурсов и другими QUBO-совместимыми постановками на графах. Для прикладных работ приоритет отдавался публикациям последних 5–7 лет, поскольку именно в этот период сформировался корпус исследований по применению QUBO-формализма в задачах информационной безопасности. Фундаментальные работы по модели Изинга, адиабатическим квантовым вычислениям, квантовому и симулированному отжигу включались независимо от года публикации как методологическая основа обзора.

Исключались публикации, в которых квантовые вычисления обсуждались без связи с QUBO-постановкой, моделью Изинга или другой воспроизводимой оптимизационной формализацией, а также работы по кибербезопасности, не содержащие математической формализации или данных, позволяющих оценить масштаб и вычислительную реализуемость предложенного подхода. Не включались популярные и технически нерецензируемые материалы, обзорные упоминания без самостоятельной модели, а также дублирующие препринты при наличии последующей журнальной или конференционной версии. Препринты arXiv учитывались только в тех случаях, когда они содержали конкретную QUBO-постановку, постановку в модели Изинга, экспериментальные параметры или результаты, отсутствующие в рецензируемых источниках; для более ранних препринтов дополнительно проверялось наличие опубликованной версии.

## Физические основы квантовых алгоритмов оптимизации

### *Модель Изинга*

Задачи комбинаторной оптимизации в рамках квантовой оптимизации часто формулируются с использованием модели Изинга. Основной целью является нахождение конфигурации спинов, минимизирующей энергию системы:

$$E_{\text{Ising}} = -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} J_{i,j}s_i s_j - \sum_{i=1}^{N} h_i s_i. \tag{2}$$

В выражении (2) спиновые переменные $s_i \in \{-1, 1\}$ принимают бинарные значения, $N$ обозначает число спинов в системе, а коэффициенты попарного взаимодействия удовлетворяют условиям

$$J_{i,i} = 0, \quad J_{i,j} = J_{j,i} \quad \forall i \neq j. \tag{3}$$

В общем случае параметры $h_i$ в выражении энергии модели Изинга (2) соответствуют локальным полям, действующим на $i$-й спин. Поскольку введение дополнительных спиновых переменных позволяет свести задачу к случаю с нулевым локальным полем, далее будем рассматривать модель Изинга при $h_i = 0$.

Важно отметить, что конфигурации $\{s_i\}$ и $\{-s_i\}$ приводят к одинаковому значению энергии системы, вследствие чего задача всегда имеет по меньшей мере два симметричных решения. Минимизация энергии модели Изинга в общем случае является NP-трудной задачей. В дальнейшем будут рассмотрены различные алгоритмические подходы, основанные на физических процессах, которые позволяют эффективно исследовать пространство состояний и решать задачи комбинаторной оптимизации в рамках данной модели.

### *Квантовая адиабатическая теорема*

Согласно квантовой адиабатической теореме квантовая система, инициализированная в невырожденном основном состоянии гамильтониана, зависящего от времени, будет оставаться в основном состоянии при сколь угодно длительной эволюции, если гамильтониан изменяется достаточно медленно.

Если гамильтониан квантовой системы не зависит от времени, динамика системы описывается уравнением Шрёдингера. Для гамильтониана $H$, не зависящего от времени, решение уравнения Шрёдингера имеет вид

$$i\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle \tag{4}$$

с начальным состоянием

$$|\psi(t)\rangle = \exp(-iHt)|\psi(0)\rangle. \tag{5}$$

Таким образом, любое собственное состояние $|E\rangle$ гамильтониана $H$, для которого выполняется соотношение $H|E\rangle = E|E\rangle$, эволюционирует во времени лишь за счет фазового множителя $\exp(-iEt)$. В этом случае переходы между собственными состояниями отсутствуют.

Если гамильтониан системы зависит от времени, эволюция квантового состояния, вызванная этими изменениями, в общем случае может быть существенно более сложной, а аналитическое описание динамики становится затруднительным. Однако при достаточно медленном изменении гамильтониана система остается близкой к своему мгновенному собственному состоянию. Квантовая адиабатическая теорема формализует данное поведение.

Для наглядности рассмотрим простой пример спина в магнитном поле, которое плавно вращается от одного направления к другому за конечное время $T$:

$$H(t) = -\cos\left(\frac{\pi t}{2T}\right)\sigma_x - \sin\left(\frac{\pi t}{2T}\right)\sigma_z. \tag{6}$$

Предположим, что в начальный момент времени спин ориентирован вдоль оси $x$, то есть система находится в основном состоянии гамильтониана при $t = 0$. По мере медленного вращения магнитного поля в направлении оси $z$ состояние спина начинает прецессировать вокруг мгновенного направления поля. При увеличении времени эволюции $T$ угловая скорость изменения гамильтониана уменьшается по сравнению со скоростью прецессии, вследствие чего амплитуда отклонений от мгновенного основного состояния сокращается. В пределе бесконечно медленного вращения магнитного поля квантовое состояние системы остается в основном собственном состоянии гамильтониана на каждом моменте времени.

В более общем случае рассмотрим эрмитов оператор $H(s)$, где параметр $s \in [0, 1]$, являющийся непрерывной функцией по $s$. Введем замену переменной $s = \frac{t}{T}$, где $T$ — общее время эволюции системы. При достаточно большом $T$ гамильтониан $H(t)$ изменяется сколь угодно медленно как функция времени $t$. Начальное квантовое состояние $|\psi(0)\rangle$ эволюционирует согласно уравнению Шрёдингера:

$$i\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle, \tag{7}$$

или с учетом замены $s = \frac{t}{T}$

$$i\frac{d}{ds}|\psi(s)\rangle = TH(s)|\psi(s)\rangle. \tag{8}$$

Предположим, что начальное состояние $|\psi(0)\rangle$ является собственным состоянием гамильтониана $H(0)$ и для простоты соответствует его невырожденному основному состоянию. Дополнительно будем считать, что основное состояние гамильтониана $H(s)$ остается невырожденным для всех $s \in [0, 1]$. Тогда, согласно квантовой адиабатической теореме, в пределе $T \to \infty$ конечное состояние системы $|\psi(T)\rangle$ совпадает с основным состоянием гамильтониана $H(1)$.

Разумеется, на практике требуется получить конкретные оценки необходимого времени эволюции $T$, обеспечивающего выполнение адиабатического приближения. Подробное доказательство адиабатической теоремы выходит за рамки данной работы. Говоря простыми словами, если создать систему, динамика изменения которой удовлетворяет условиям квантовой адиабатической теоремы, в любой момент времени $\tau \in [0, T]$ система будет находиться в основном состоянии.

### *Квантовые вычисления на основе бифуркации*

Динамика нелинейной системы качественно зависит от значений ее параметров. Точки, в которых происходит резкое изменение поведения системы, называются точками бифуркации. Квантово-механический осциллятор может достигать состояния суперпозиции в результате адиабатической эволюции через точку бифуркации. Квантовый алгоритм бифуркации, предложенный Хаято Гото [Goto, 2016; Goto, 2019], вводит новую вычислительную парадигму, в которой вместо системы квантовых битов используется ансамбль нелинейных квантовых осцилляторов, а оптимизационная задача решается посредством квантовой адиабатической эволюции.

Существующие квантовые вычислительные архитектуры уже используют нелинейные осцилляторы в качестве физических реализаций кубитов, в том числе с задействованием эффектов суперпозиции [Mirrahimi et al., 2014], при этом вычисления осуществляются с помощью квантовых вентильных операций. Однако подобный подход не в полной мере использует непрерывные степени свободы нелинейных осцилляторных систем. Ансамбль из $N$ нелинейных квантовых осцилляторов способен, в результате суперпозиции, охватывать пространство из $2^N$ эффективных состояний. В ходе поиска оптимального решения посредством адиабатической эволюции через точки бифуркации управляющие параметры системы постепенно увеличиваются.

В алгоритме Гото [Goto, 2016] используется параметрический осциллятор с эффектом Керра (Kerr parametric oscillator, KPO). В системе отсчета, вращающейся с угловой скоростью, равной половине частоты параметрического возбуждения $\frac{\omega_p}{2}$, и в приближении вращающейся волны гамильтониан системы имеет вид

$$H = \hbar\Delta a^\dagger a + \hbar\frac{K}{2}a^{\dagger 2}a^2 - \hbar\frac{p}{2}\left(a^2 + a^{\dagger 2}\right), \tag{9}$$

где $a$ и $a^\dagger$ обозначают операторы уничтожения и рождения, $\Delta$ — расстройка, определяемая как отклонение собственной частоты осциллятора от половины частоты параметрического возбуждения, $K$ — коэффициент Керра, а $p$ — неотрицательный управляющий параметр, соответствующий амплитуде параметрического возбуждения. Предполагается, что параметры $K$ и $\Delta$ принимают положительные значения, причем $\Delta = \omega_{\text{KPO}} - \frac{\omega_p}{2}$, где $\omega_{\text{KPO}}$ обозначает резонансную частоту осциллятора.

Переход в состояния суперпозиции происходит следующим образом. Система инициализируется в вакуумном состоянии, то есть в основном состоянии $|0\rangle$ с нулевой амплитудой поля. При этом $|0\rangle$ является основным состоянием гамильтониана (9) при $p = 0$. В процессе адиабатической эволюции величина управляющего параметра $p$ медленно увеличивается, что приводит к плавному изменению гамильтониана системы.

В пределе $p \gg \Delta$ конечное состояние системы приближенно соответствует основному состоянию гамильтониана при $\Delta = 0$, которое представляет собой суперпозицию двух когерентных состояний $\left|\pm\sqrt{\frac{p}{K}}\right\rangle$. Поскольку гамильтониан инвариантен относительно преобразования паритета $a \to -a$, конечное состояние сохраняет тот же паритет, что и начальное вакуумное состояние $|0\rangle$. В результате система переходит в состояние суперпозиции вида

$$\frac{\left|\sqrt{\frac{p}{K}}\right\rangle + \left|-\sqrt{\frac{p}{K}}\right\rangle}{\sqrt{2}}, \quad \left\langle\sqrt{\frac{p}{K}}\,\middle|\,-\sqrt{\frac{p}{K}}\right\rangle = e^{-2p/K} \xrightarrow{p\gg 1} 0. \tag{10}$$

Поскольку решаемая задача бинарной оптимизации формулируется в рамках модели Изинга (2), необходимо задать гамильтониан системы нелинейных осцилляторов в соответствующей форме. Попарное линейное недиссипативное взаимодействие между осцилляторами описывается выражением

$$H_{\text{coupling}} = -\frac{\hbar\xi_0}{2}\sum_{i<j}^{N} J_{i,j}\left(a_i^\dagger a_j + a_j^\dagger a_i\right). \tag{11}$$

С учетом гамильтониана одиночного параметрического осциллятора (9) и введенного взаимодействия итоговый гамильтониан системы из $N$ осцилляторов принимает вид

$$H(t) = \hbar\sum_{i=1}^{N}\left[\Delta_i a_i^\dagger a_i + \frac{K_i}{2}a_i^{\dagger 2}a_i^2 - \frac{p_i(t)}{2}\left(a_i^{\dagger 2} + a_i^2\right) - \left(\epsilon_i a_i^\dagger + \epsilon_i^* a_i\right)\right] - \hbar\frac{\xi_0}{2}\sum_{i<j} J_{i,j}\left(a_i^\dagger a_j + a_j^\dagger a_i\right), \tag{12}$$

где $\xi_0$ — положительная константа с размерностью частоты, характеризующая силу связи между осцилляторами. Для корректной реализации адиабатической эволюции требуется выполнение условия

$$\Delta_i = \xi_0\sum_{j=1}^{N}|J_{i,j}|. \tag{13}$$

### *Квантовые вычисления на основе отжига*

Квантовый отжиг представляет собой вычислительную парадигму, основанную на принципе квантовой адиабатической эволюции. Исторически идеи отжига были впервые предложены в контексте классической оптимизации Киркпатриком и соавт. [Kirkpatrick et al., 1983] в виде алгоритма симулированного отжига (Simulated Annealing, SA), который стал универсальным методом решения широкого класса оптимизационных задач. Основная идея алгоритма заключается в использовании термических флуктуаций для выхода системы из локальных минимумов целевой функции посредством контролируемого понижения температуры.

Скорость охлаждения системы играет ключевую роль в эффективности алгоритма: при слишком быстром понижении температуры система может застревать в локальных минимумах, тогда как чрезмерно медленное охлаждение делает алгоритм практически неэффективным, несмотря на теоретическую сходимость к глобальному минимуму. Геман и Геман [Geman, Geman, 1984] получили оценку для скорости изменения температуры, при которой в общем случае обеспечивается достижение глобального минимума:

$$T \leqslant \frac{c}{\log t},$$

где $c$ — константа, определяемая размерностью задачи и параметрами целевой функции, а $t$ — время эволюции системы.

В общем виде алгоритмы поиска глобального минимума основаны на последовательном исследовании различных состояний системы и переходах между ними. Это естественным образом приводит к идее использования квантовых эффектов для улучшения сходимости оптимизационных процедур. В основе квантового отжига лежит концепция, предложенная Кадоваки и Нисимори [Kadowaki, Nishimori, 1998], согласно которой квантовое туннелирование позволяет системе эффективно преодолевать потенциальные барьеры, включая седловые точки и локальные минимумы энергетического ландшафта.

Для учета туннелирования между состояниями в модель вводится поперечное квантовое поле $\Gamma(t)$, и гамильтониан модели Изинга с учетом выражения (2) принимает вид

$$H(t) = -\sum_{i=1}^{N}\sum_{j=1}^{N} J_{i,j}\sigma_i^z\sigma_j^z - \sum_{i=1}^{N} h_i\sigma_i^z - \Gamma(t)\sum_{i=1}^{N}\Delta_i\sigma_i^x, \tag{14}$$

где $\sigma_i^x$ и $\sigma_i^z$ обозначают матрицы Паули, действующие на $i$-й спин, с собственными значениями $\pm 1$, а параметр $\Delta_i$ характеризует интенсивность квантового туннелирования между базисными состояниями $|\pm 1\rangle$.

Пусть гамильтониан модели Изинга без поперечного поля имеет вид

$$H_p = -\sum_{i=1}^{N}\sum_{j=1}^{N} J_{i,j}\sigma_i^z\sigma_j^z - \sum_{i=1}^{N} h_i\sigma_i^z, \tag{15}$$

тогда выражение для времезависимого гамильтониана (14) можно переписать в форме

$$H(t) = -\Gamma(t)\sum_{i=1}^{N}\Delta_i\sigma_i^x + H_p. \tag{16}$$

Плавно изменяя амплитуду поперечного поля $\Gamma(t)$ от большого начального значения $\Gamma(0) \gg 1$ до нуля, можно реализовать процесс адиабатической эволюции, в ходе которого система переходит в основное состояние гамильтониана $H_p$, соответствующее минимальной энергии. В работе [Johnson et al., 2011], например, предложена реализация квантового отжига на основе системы искусственных спинов с гамильтонианом вида

$$H(t) = -\Gamma(t)\sum_{i=1}^{N}\Delta_i\sigma_i^x + \Lambda(t)H_p. \tag{17}$$

В начальный момент времени система инициализируется при $\Gamma(0) = 1$ и $\Lambda(0) = 0$, так что динамика полностью определяется поперечными членами $\Delta_i\sigma_i^x$. Основное состояние такой системы представляет собой суперпозицию в базисе собственных состояний оператора $\sigma^z$. В процессе адиабатической эволюции вклад поперечного поля постепенно уменьшается, в то время как вклад гамильтониана модели Изинга возрастает, то есть функция $\Gamma(t)$ монотонно убывает от 1 до 0, а функция $\Lambda(t)$ монотонно возрастает от 0 до 1. При достаточно медленном изменении параметров, согласно квантовой адиабатической теореме, система остается в основном состоянии на протяжении всей эволюции и в конечный момент времени оказывается в основном состоянии гамильтониана $H_p$.

## Применение методов квадратичной бинарной оптимизации в области информационной безопасности

Рассмотрев физические модели и алгоритмические основы решения задач QUBO, перейдем к анализу их применения в прикладных задачах информационной безопасности. В дальнейшем изложении различаются четыре уровня реализации QUBO-подходов. К физическим квантовым реализациям относятся эксперименты, в которых задача отображается на реальное квантовое устройство, например квантовый отжигатель D-Wave или нейтрально-атомный QPU. К гибридным реализациям относятся схемы, где декомпозиция, предобработка, постобработка и часть поиска выполняются классически, а квантовое устройство используется как сопроцессор для подзадач. К симуляциям и квантово-вдохновленным алгоритмам относятся программы, выполняемые на обычной классической архитектуре: например, SA, SB, qbsolv без обращения к QPU. Такие методы могут использовать математическую аналогию с физическими процессами, но само вычисление выполняется классически и не использует квантовую когерентность. Наконец, часть работ содержит только QUBO-постановку или оценку масштаба без экспериментального запуска на решателе. Это разграничение важно для интерпретации заявлений об ускорении: результаты физических устройств отражают свойства конкретного аппаратного поколения, тогда как симуляционные результаты характеризуют прежде всего качество постановки и выбранного классического решателя. Ниже при обсуждении прикладных работ дополнительно указывается, к какому из этих уровней относится соответствующий результат.

### *Криптоанализ в форме QUBO*

Во многих случаях криптоанализ сводится к решению сложных комбинаторных задач, таких как восстановление секретных ключей или выявление уязвимых структур в криптографических алгоритмах. Подобные задачи часто формулируются в виде систем алгебраических уравнений с ограничениями, являющихся NP-трудными, и могут быть приведены к формулировке QUBO. В ряде недавних исследований рассматривается представление криптоаналитических задач в виде QUBO-задач, пригодных для решения на вычислительных устройствах, основанных на квантовом отжиге. В частности, несколько работ продемонстрировали возможность формализации атак на симметричные шифры в виде решения задачи QUBO.

В работе [Burek et al., 2022; Burek, 2025] предложен метод представления блочного шифра AES-128 в виде системы полиномиальных уравнений с последующей формулировкой оптимизационной задачи в виде QUBO; в данном случае речь идет прежде всего о теоретической QUBO-постановке и оценке требуемой размерности, а не о запуске полномасштабной атаки на реальном QPU. Авторы отмечают, что криптоанализ AES-128 с использованием квантового отжига оказывается вычислительно менее сложным с точки зрения размерности задачи по сравнению с задачей факторизации открытого ключа сопоставимого уровня стойкости. Так, представление факторизации RSA с длиной ключа 3072 бита, что соответствует уровню безопасности AES-128, в форме QUBO требует порядка 2 360 000 бинарных переменных, тогда как для формулировки атаки на AES-128 необходимо около 30 000 бинарных переменных. Данный результат подчеркивает существенный разрыв в вычислительной сложности между криптоанализом симметричных шифров и задачей факторизации RSA в парадигме QUBO.

В последующем исследовании [Burek, Wroński, 2022] авторы применили QUBO-подход для атаки на блочный шифр Speck, продемонстрировав еще более компактные представления по сравнению с AES; данная работа также относится главным образом к уровню теоретической QUBO-постановки и эвристической оценки применимости квантового отжига. Предложенная QUBO-формулировка для Speck-128/128 требует 19 311 бинарных переменных, а для Speck-128/256 — 33 721, тогда как для AES-128 и AES-256 соответствующие значения составляют 29 770 и 72 597 бинарных переменных. Эти результаты демонстрируют различия в вычислительной сложности криптоаналитических задач для различных шифров при использовании одной и той же алгебраической модели атаки. Существенное сокращение размерности достигается за счет оптимизированного разбиения систем уравнений и введения вспомогательных переменных с целью минимизации общего числа бинарных переменных, что указывает на прогресс в разработке эффективных QUBO-представлений для симметричных криптографических примитивов.

Еще одним значимым вкладом является работа [Pakhomchik et al., 2022], в которой предложены два универсальных метода преобразования булевых формул, возникающих в криптоанализе, в формы, пригодные для оптимизационных решателей: либо в виде систем линейных уравнений и неравенств для смешанного целочисленного линейного программирования (Mixed Integer Linear Programming, MILP), либо непосредственно в форму QUBO с использованием штрафных членов. Эта работа относится к теоретико-методологическому уровню: она задает процедуру преобразования булевых ограничений, но не демонстрирует преимущество конкретного физического квантового устройства. Авторы иллюстрируют данный подход на примере симметричных криптографических примитивов, включая формализацию раундовых операций AES в виде MILP с последующим преобразованием в QUBO. Ключевая идея заключается в том, что любая булева функция, например S-box или раундовая функция, может быть представлена через линейные ограничения с введением дополнительных бинарных переменных, после чего это представление переводится в квадратичную целевую функцию. Несмотря на универсальность метода, авторы отмечают, что он может приводить к существенному росту числа вспомогательных переменных.

В работе [Wroński et al., 2025] детально рассмотрен перевод криптоаналитической задачи для шифра Grain-128/128a в форму QUBO, которая требует порядка 5751 бинарной переменной и 77 496 попарных связей для описания ограничений шифра. По типу реализации это в первую очередь QUBO-постановка и оценка аппаратной реализуемости, поскольку полная задача остается слишком плотной для прямого встраивания на текущие квантовые отжигатели. На основе эвристических оценок авторы утверждают, что для задач размерности $N$ квантовый отжиг в среднем обеспечивает ускорение по сравнению с симулированным отжигом на классической архитектуре приблизительно в $\sqrt{N}$ раз. В результате оптимизационные атаки на основе квантового отжига потенциально превосходят как жадные методы поиска, так и алгоритм Гровера при достаточно больших размерах ключевого пространства.

В совокупности рассмотренные подходы основаны на общей идее: логические зависимости криптографического алгоритма кодируются в виде QUBO-формулировки, после чего специализированный решатель, например квантовый отжигатель компании D-Wave, осуществляет поиск конфигурации с минимальной энергией в модели Изинга, соответствующей секретному ключу. Представленные работы демонстрируют, что задача восстановления ключа может быть сведена к QUBO и решена с использованием квантовых оптимизационных устройств. Однако размерность получающихся задач по-прежнему остается чрезвычайно большой и существенно превышает доступное число кубитов в современных квантовых вычислительных системах. Несмотря на это, данные исследования являются важным шагом в направлении разработки специализированных квантовых вычислительных архитектур, в частности квантовых отжигателей, которые потенциально способны обеспечивать эффективный криптоанализ симметричных шифров.

В контексте криптографии с открытым ключом и, в частности, RSA QUBO-формализм применяется для решения задачи факторизации целых чисел. В работе [Dridi, Alghassi, 2017] предложен метод формализации задачи факторизации в виде QUBO. С помощью этого метода удалось факторизовать числа вплоть до 200 099 на физическом квантовом отжигателе *D-Wave 2X*. Полиномиальные члены высоких степеней были сведены к квадратичной форме посредством разложения с использованием базисов Гребнера. Аналогичным образом в работе [Jiang et al., 2018] разработана QUBO-формулировка для факторизации целых чисел до 376 289 с применением 94 логических кубитов на физическом устройстве D-Wave 2000Q. Эти исследования на примере небольших чисел демонстрируют перевод криптоанализа RSA в задачу QUBO-оптимизации. Близкая линия работ рассматривает также HUBO- и QUBO-модели факторизации [Jun, Lee, 2023]; по типу реализации это прежде всего теоретическая постановка и сравнение формализмов, а не демонстрация атаки на криптографически значимые ключи. Более поздние исследования показывают, что существенную роль начинает играть не только сама QUBO-формулировка, но и способ ее встраивания в физическую топологию отжигателя. В работе [Ding et al., 2024] предложено модульное локально структурированное встраивание схемы бинарного умножения непосредственно в топологию Pegasus устройства D-Wave Advantage: управляемый полный сумматор кодируется в виде 8-кубитного модуля, после чего из таких модулей собирается схема умножителя. Авторам удалось закодировать умножители до $21 \times 12$ бит в топологии из 5760 кубитов и экспериментально факторизовать на реальном D-Wave Advantage 4.1 число $8\,219\,999 = 32\,749 \times 251$; последующий отчет [Ding et al., 2024] подробно описывает использованные стратегии инициализации, паузы, обратного отжига и настройки смещений. Другой недавний подход основан на явном моделировании переноса разрядов при бинарном умножении [Ryou et al., 2025]: HUBO-модель остается применимой только для малых полупростых чисел, тогда как CQM-формулировка с глобальным ограничением произведения позволяет в гибридном рабочем процессе D-Wave рассматривать полупростые числа до 60 бит, включая $N = 1\,152\,921\,423\,002\,469\,787$. Следовательно, современные результаты по факторизации следует

разделять на прямые эксперименты на физическом квантовом отжигателе и гибридные/ограниченные модели, которые улучшают масштабируемость, но не являются прямым встраиванием большой QUBO-задачи на QPU. Вместе с тем при масштабировании подхода к криптосистемам практического размера, например для RSA с длиной ключа 3072 бита, QUBO-представление требует порядка одного миллиона бинарных переменных [Burek et al., 2022]; эта оценка относится к теоретическому анализу размерности, а не к эксперименту на QPU.

Таблица 1. Сравнение QUBO-подходов к криптоанализу шифров и задаче факторизации

| Работа | Задача | Размерность QUBO / сложность | Тип QPU/решателя: отжигатель, компьютер, бифуркация | Физическое устройство |
|---|---|---|---|---|
| [Burek et al., 2022] | AES и SmallCipher | SmallCipher: 64 переменные для одного раунда и 200 переменных для двух раундов; AES-128: до 237 915 бинарных переменных; оценка RSA-3072: порядка 2 360 000 переменных | D-Wave-совместимый квантовый отжиг; для малых примеров использовался симулятор | Нет для полной атаки; только симуляция/оценка |
| [Burek, 2025] | Simon | Simon-16/16: матрица $Q$ с 1684 ненулевыми элементами; Simon-128/128: 27 270 переменных; Simon-128/256: 49 408 переменных | Квантовый отжигатель D-Wave | Да для Simon-16/16; нет для полных версий |
| [Burek, Wroński, 2022] | Speck | Speck-128/128: 19 311 переменных; Speck-128/256: 33 721 переменная; эвристическая сложность отжига порядка $O\left(e^{\sqrt{N}}\right)$ | Квантовый отжигатель как целевая архитектура | Нет для реального Speck; теоретическая оценка |
| [Pakhomchik et al., 2022] | Булевы ограничения AES, MD5, SHA-256 | MD5: около 17 280 переменных; SHA-256: 47 808; AES-128: около 90 000; AES-256: около 250 000 | QUBO/MILP-преобразование; проверка встраивания в топологии D-Wave | Нет; эксперимент только по встраиванию |
| [Phab et al., 2023] | Heys toy cipher | QUBO не строится; CNF/MAX-SAT/QAOA: от 5 переменных и 19 клауз до 29 переменных и 164 клауз | Вентильные квантовые компьютеры IBM и QAOA-симуляторы | Да для малой 5-кубитной формулы; не QUBO-задача |
| [Dridi, Alghassi, 2017] | Факторизация | До 200 099 = 499 × 401; для column algorithm после предобработки базисами Гребнера около 72–75 логических переменных | Квантовый отжигатель D-Wave 2X | Да |
| [Jiang et al., 2018] | Факторизация | $N$ = 143 использует 12 логических кубитов; 376 289 описано с 94 логическими кубитами; 249 919 встраивается в 1803 физических кубита | Квантовый отжигатель D-Wave 2000Q | Да для малых экземпляров и экспериментов встраивания |
| [Jun, Lee, 2023] | Факторизация | QUBO для $N$ = 15: 15 логических кубитов; большие примеры представлены как HUBO / диапазонные модели; квадратизация требует до $\frac{7}{4}n^2(n-1)^2$ дополнительных переменных для слагаемых четвертого порядка | D-Wave Advantage для малой QUBO; Ocean / Leap и ExactPolySolver для HUBO | Да только для малого QUBO; большие результаты не являются прямым QPU-QUBO |
| [Ding et al., 2024; Ding et al., 2024] | Факторизация | Локально структурированное встраивание: 8 кубитов на модуль полного сумматора; до 21 × 12 бит в идеальной Pegasus-топологии; решено 8 219 999 | Квантовый отжигатель D-Wave Advantage 4.1 | Да |
| [Ryou et al., 2025] | Факторизация | HUBO становится непрактичной около 10 бит; CQM-тесты до 60-битных полупростых чисел; нет единого QUBO-размера, сопоставимого с прямым встраиванием | Гибридный D-Wave CQM / Ocean; ExactPolySolver для малых HUBO | Нет для прямой большой QUBO на QPU |

Сравнение рассмотренных работ по криптоанализу симметричных шифров и факторизации приведено в табл. 1. В таблице отдельно указано, была ли задача действительно запущена на физическом квантовом устройстве, поскольку в ряде работ терминология QUBO используется только для оценки размерности или для запуска на симуляторах и гибридных решателях.

Из табл. 1 видно, что среди рассмотренных криптографических задач реальные физические эксперименты почти полностью относятся к квантовым отжигателям D-Wave, тогда как вентильные квантовые компьютеры применялись только в QAOA-эксперименте для имитации шифра и не реализовывали QUBO-постановку. Бифуркационные решатели в этой группе работ не выступают основной экспериментальной платформой: они остаются релевантным классом квантово вдохновленных QUBO-методов, но в приведенных криптоаналитических и факторизационных примерах не дают отдельной подтвержденной аппаратной демонстрации.

Криптоанализ с использованием квантового отжига не гарантирует асимптотического ускорения по сравнению с алгоритмом Гровера или классическим перебором, однако в ряде специфических сценариев может превосходить традиционные методы атак. Алгоритм Гровера [Grover, 1997] на идеальном квантовом компьютере вентильной архитектуры обеспечивает квадратичное ускорение для задач неструктурированного поиска, требуя порядка $\sqrt{N}$ итераций в пространстве размера $N$. В частности, поиск ключа в пространстве из $2^n$ возможных значений требует порядка $2^{n/2}$ шагов. Тем не менее сложность остается экспоненциальной по длине ключа.

Квантовый отжиг, напротив, использует эффект квантового туннелирования при переходе между состояниями, что теоретически может обеспечивать более быструю сходимость в оптимизационных задачах [Mukherjee, Chakrabarti, 2015]. Однако вопрос о том, способен ли квантовый отжиг в общем случае превзойти перебор с ускорением Гровера, остается открытым. Так, в работе [Burek, Wroński, 2022] авторы на основе эвристических правил оценивают сложность квантового отжига порядка $O\left(e^{\sqrt{N}}\right)$. В таком случае QUBO-оптимизация с использованием квантового отжига потенциально может требовать меньше итераций по сравнению с экспоненциальным перебором, однако практическое подтверждение подобных оценок в настоящее время отсутствует.

На практике современные устройства квантового отжига подвержены шумам и существенно ограничены по масштабу. Экспериментальные исследования на упрощенных криптографических примитивах, таких как миниатюрная версия AES с шестью раундами и 64-битный шифр Хейса, показали, что ни квантовые отжигатели, ни квантовые приближенные алгоритмы пока не превосходят классические методы криптоанализа даже для малых размерностей задач [Phab et al., 2023]. В отличие от чисто теоретических QUBO-постановок эта работа важна именно как сравнительный эксперимент на малых модельных экземплярах, где проверяются реальные и симулируемые оптимизационные процедуры. В итоге в задачах перебора ключей алгоритм Гровера обеспечивает гарантированное квадратичное ускорение, тогда как квантовый отжиг теоретически может предложить дополнительное ускорение в отдельных классах QUBO-задач, но для практической реализации такого преимущества требуется дальнейшее развитие как алгоритмов, так и аппаратных платформ.

### *Детекция аномалий как задача QUBO*

Обнаружение аномалий представляет собой задачу выявления точек данных или поведенческих паттернов, существенно отклоняющихся от общих закономерностей выборки, что является критически важным для таких областей, как финансы, здравоохранение и в особенности кибербезопасность. В контексте информационной безопасности задачи обнаружения сетевых вторжений и мошеннической активности часто сводятся к выявлению редких вредоносных событий, скрытых в больших объемах данных. Традиционные статистические и эвристические методы широко применяются на практике, однако при росте размерности и объема данных возникают

существенные ограничения по точности, скорости обработки и масштабируемости. Кроме того, поведенческие паттерны со временем изменяются, что требует адаптации детекционных систем.

В последние годы с развитием методов искусственного интеллекта получили распространение подходы на основе глубокого обучения и обучения с подкреплением, позволяющие строить высокоточные модели типа «черного ящика» с использованием вычислительных ускорителей. Такие методы демонстрируют высокую эффективность, однако их дальнейшее масштабирование и ускорение часто ограничиваются доступными вычислительными ресурсами. В этом контексте квантовые вычисления рассматриваются как потенциальная альтернатива [Stein et al., 2024], предлагающая новую вычислительную парадигму для обработки сложных оптимизационных задач; в цитируемой работе используются как симуляционные процедуры для подбора параметров, так и запуски на квантовых отжигателях D-Wave. В частности, ряд исследований формулирует задачи детекции аномалий в виде QUBO-задач [Mellaerts, 2023]; при этом работа [Mellaerts, 2023] относится к программной, квантово-вдохновленной реализации, поскольку полученная QUBO-модель решается на классическом компьютере эвристическим оптимизатором, без запуска на физическом QPU.

Формализм QUBO предоставляет удобный аппарат для представления задач обнаружения аномалий в виде бинарных оптимизационных задач. В общем случае каждой точке данных или признаку сопоставляется бинарная переменная, принимающая значение 1, если элемент считается аномальным, и 0 — в противном случае. Далее определяется квадратичная целевая функция таким образом, чтобы ее минимум соответствовал наиболее вероятной конфигурации системы, содержащей аномальные элементы.

В частности, в работе [Mellaerts, 2023] предложена QUBO-формулировка, объединяющая статистические и плотностные критерии детекции аномалий. Эта работа включена в обзор, поскольку содержит явную QUBO-модель детекции аномалий и экспериментальное сравнение по метрикам качества, что важно для оценки применимости подхода в задачах кибербезопасности. Однако полученные результаты следует интерпретировать как результаты программного решения QUBO на классической архитектуре, а не как эксперимент на реальном квантовом процессоре. В рамках данного подхода линейные члены целевой функции отражают степень отклонения каждой точки данных от центроида распределения, тогда как квадратичные члены учитывают попарные расстояния между элементами выборки. Для набора данных $X = (x_0, \ldots, x_{N-1})$ из $N$ элементов функция QUBO записывается в виде

$$Q(x, \alpha) = \alpha \sum_{i=1}^{N} d_i x_i + (1 - \alpha) \sum_{i \neq j}^{N} d_{i,j} x_i x_j, \quad \sum_{i=1}^{N} x_i = k,$$

где $d_i$ обозначает расстояние точки $x_i$ до центроида распределения, $d_{i,j}$ — расстояние между точками выборки, $0 < k \leqslant N$ — предполагаемое число аномалий в наборе данных, а параметр $\alpha \in [0, 1]$ задает относительный вклад линейных и квадратичных членов. Такая формулировка позволяет одновременно учитывать локальные отклонения и глобальную структуру данных.

В качестве метрики расстояния в подобных QUBO-моделях часто используется расстояние Махаланобиса, которое учитывает коррелированность признаков и обеспечивает устойчивую многомерную оценку отклонений. Согласно экспериментальным результатам [Mellaerts, 2023] QUBO-подход продемонстрировал улучшение качества детекции на различных наборах данных по метрике *ROC AUC* по сравнению с классическими методами. При этом в отличие от многих моделей глубокого обучения QUBO-подход относится к классу методов обучения без учителя [Stein et al., 2024] и не требует предварительной разметки данных, что является важным преимуществом при построении практических систем кибербезопасности; в работе [Stein et al.,

2024] это проверяется на QBM-модели с использованием симулированного отжига и физических отжигателей D-Wave.

Ряд исследований посвящен применению квантовых вычислительных устройств для решения QUBO-задач обнаружения аномалий. В частности, в работе [Stein et al., 2024] была использована квантовая машина Больцмана (Quantum Boltzmann Machine, QBM), реализованная на квантовом отжигателе D-Wave, для задач детекции аномалий в сценариях Endpoint Detection and Response (EDR). По типу реализации это смешанный случай: подбор гиперпараметров выполнялся с использованием классического симулированного отжига, а итоговые варианты модели проверялись на физических системах D-Wave 2000Q и Advantage. По результатам экспериментов квантовая модель превзошла классическую реализацию машины Больцмана на одном и том же наборе данных, что указывает на потенциальные преимущества квантового отжига по сравнению с классическими подходами.

Несмотря на существующие физические ограничения квантовых решателей, появляются работы, демонстрирующие практическую эффективность квантовых алгоритмов для задач обнаружения аномалий на реальных квантовых устройствах. Так, в работе [Canonici, Caruso, 2024] авторы переформулировали классификатор опорных векторов (Support Vector Machine, SVM) в виде QUBO-задачи и реализовали модель на квантовом процессоре на нейтральных атомах (Quantum Processing Unit, QPU). Данная работа включена как актуальное исследование, поскольку представляет не только теоретическую QUBO-постановку, но и экспериментальную реализацию QUBO-SVM на реальном квантовом устройстве. Кроме физического запуска на нейтрально-атомном QPU, в ней также используются идеальные и шумовые симуляции, поэтому результаты следует разделять на аппаратную и симуляционную части. Были предложены несколько вариаций квантового SVM, и некоторые из них в задаче детекции мошеннических операций продемонстрировали меньшую ошибку на тестовой выборке по сравнению с рядом популярных классических моделей машинного обучения. Полученные результаты показывают, что прямое формулирование задачи обнаружения аномалий в виде оптимизационной задачи может привести к более качественным решениям и потенциально облегчать масштабирование на данные высокой размерности.

В то же время такой подход, как правило, приводит к плотной матрице $Q$ в QUBO-постановке, что требует длинных цепочек связанных кубитов при встраивании задачи на реальные квантовые устройства. В связи с этим авторы отмечают, что при текущем уровне развития квантовых процессоров решение полномасштабных задач остается недостижимым. Однако эксперименты на QPU с 24 кубитами показали, что квантовая вариация SVM обладает высокой устойчивостью к шумам, причем квантовый шум в ряде случаев даже способствует снижению переобучения. Эти результаты демонстрируют, что квантовые устройства с несколькими десятками кубитов уже способны эффективно решать маломасштабные задачи детекции аномалий и достигать конкурентной точности, подтверждая перспективность QUBO-подхода для развития квантового машинного обучения в области информационной безопасности.

Отдельный класс задач обнаружения аномалий в области информационной безопасности связан с выявлением вторжений и системами обнаружения вторжений (Intrusion Detection Systems, IDS). Такие системы предназначены для идентификации вредоносной активности в сетевых средах или на отдельных хостах и, как правило, осуществляют классификацию трафика на «нормальный» и «вредоносный». Модели IDS работают с высокоразмерными данными и направлены на выявление скрытых поведенческих паттернов. В данном контексте QUBO-формализм может применяться либо в качестве слоя предобработки для моделей машинного обучения, либо как самостоятельный классификатор.

Первый подход часто используется в стохастических нейронных сетях, в частности в ограниченных машинах Больцмана (Restricted Boltzmann Machines, RBM). Энергетическая функция

RBM имеет квадратичную форму и совместима с оптимизационными решателями для модели Изинга, включая квантовые отжигатели [Moro, Prati, 2023]; эта ссылка используется как методологическая основа для связи RBM/QBM с изинговыми моделями, а не как самостоятельный QUBO-бенчмарк в кибербезопасности. Так, в работе [Dixit et al., 2021] авторы одними из первых предложили метод обучения RBM с использованием физического квантового отжигателя D-Wave 2000Q для задач обнаружения вторжений. В данной реализации RBM выполняла одновременно роль классификатора и генератора синтетических событий. Вследствие физических ограничений квантового отжигателя размерность задачи была существенно ограничена и использовались бинарные векторы длиной 64 бита. Согласно экспериментальным результатам, RBM, обученная на квантовом отжигателе (Quantum Annealing RBM, QARBM), достигла сопоставимой точности по сравнению с моделью RBM, обученной классическими методами.

Другим направлением исследований является разработка гибридных архитектур [Li et al., 2015; Salama et al., 2011], в которых классические модели применяются для уменьшения размерности входных данных с целью последующей обработки на квантовых устройствах, либо квантовые методы используются для генерации дополнительных признаков, передаваемых далее в классические алгоритмы машинного обучения. В данном обзоре эти работы используются как классические и гибридные бейзлайны для IDS, а не как примеры запуска QUBO на физическом квантовом оборудовании.

Сравнительная характеристика рассмотренных работ по обнаружению аномалий приведена в табл. 2. В таблице отдельно выделены масштаб QUBO-модели или изинговой модели, тип вычислительной платформы и наличие реального физического квантового запуска, поскольку в этой группе работ встречаются как полноценные эксперименты на QPU, так и классические квантово вдохновленные решения или только методологически близкие RBM/DBN бейзлайны.

Из табл. 2 видно, что наиболее зрелые аппаратные эксперименты в задачах обнаружения аномалий связаны с квантовыми отжигателями D-Wave и малыми аналоговыми нейтрально-атомными QPU. При этом явная QUBO-селекция аномалий на уровне всей выборки быстро приводит к плотным матрицам и квадратичному росту числа связей, тогда как RBM/QBM-подходы переносят вычислительную нагрузку на выборку из энергетической модели. Бифуркационные решатели в рассмотренных работах по anomaly detection не выступают экспериментальной платформой, хотя остаются потенциально применимым классом квантово вдохновленных QUBO-методов.

QUBO-формулировка в задачах обнаружения аномалий обладает высокой степенью гибкости: посредством настройки весов и структуры целевой функции возможно интегрировать предметно-ориентированные знания, включая специализированные метрики расстояния. QUBO естественным образом поддерживает бинарные решения для каждой точки выборки, что удобно в сценариях, где требуется явно выделить подмножество аномальных событий для последующего анализа. Еще одним существенным преимуществом является возможность явно ограничивать количество аномалий на уровне целевой функции без привлечения дополнительных эвристик, например путем введения линейных ограничивающих членов, что не всегда реализуется напрямую в моделях машинного и глубокого обучения.

Основным ограничением данного подхода остается сложность практической реализации оптимизационных алгоритмов на квантовых вычислительных архитектурах. Использование дополнительных эвристических методов позволяет частично снизить вычислительную нагрузку, однако не гарантирует сходимости к глобальному минимуму. Еще одной проблемой является выбор корректной метрики расстояния в высокоразмерных пространствах признаков, который сам по себе является нетривиальной задачей. При использовании чрезмерно простой метрики модель может генерировать значительное число ложноположительных срабатываний, что приводит к дополнительной нагрузке на последующие аналитические модули.

Таблица 2. Сравнение QUBO-подходов к задаче обнаружения аномалий

| Работа | Задача и модель | Размерность QUBO / сложность | Тип QPU/решателя: отжигатель, компьютер, бифуркация | Физическое квантовое устройство |
|---|---|---|---|---|
| [Stein et al., 2024] | Ненадзорная детекция аномалий / фродовые EDR; QBM | 21 видимая переменная и 82 скрытые в лучшей SA-модели: 103 логические бинарные переменные и около $21 \cdot 82 + \binom{21}{2} = 1932$ квадратичных связей до встраивания; аппаратные ограничения: до 94 скрытых переменных на D-Wave 2000Q и до 632 на Advantage 4.1 | Симулированный отжиг для подбора гиперпараметров; физические квантовые отжигатели D-Wave 2000Q и Advantage 4.1; бифуркационный решатель не использовался | Да; итоговая проверка на D-Wave |
| [Mellaerts, 2023] | Ненадзорная детекция выбросов; явная QUBO-селекция аномалий | $N$ бинарных переменных, по одной на точку данных; без прореживания попарные члены имеют масштаб $O\left(N^2\right)$, при $k$ наиболее удаленных соседей — $O(Nk)$, но штраф $\left(\sum_i x_i - k\right)^2$ снова создает плотные связи; в MNIST-тестах: 50 переменных и $k = 5$ | Классический компьютер / квантово вдохновленный QUBO через `qbsolv`; предлагаются SA/SQA/QUBO-эвристики | Нет; только классическое решение QUBO |
| [Canonici, Caruso, 2024] | Детекция фродовых транзакций кредитных карт; QUBO-SVM | Матрица QUBO размером $KN \times KN$; время построения $O\left(N^2K^2N_{\text{features}}\right)$, квантовая часть $O\left(N^2K^2\right)$, число атомов $O(NK)$; при $K = 2$ симуляции используют 8–16 атомов, физические запуски — 18–24 атома | Аналоговый нейтрально-атомный квантовый компьютер Pasqal Fresnel; идеальные и шумовые симуляции Pulser; размещение атомов оптимизировалось классически | Да; реальные запуски на нейтрально-атомном QPU |
| [Moro, Prati, 2023] | Детекция аномалий IDS; QRBM/RBM | NSL-KDD: 85 видимых битов и 30 скрытых, всего 115 логических единиц; CSE-CIC-IDS2018: 156 видимых битов и 90 скрытых, всего 246 логических единиц; классический CD масштабируется как $O(kN)$, время доступа к QPU эмпирически близко к $O(Ns)$ | Физический квантовый отжигатель D-Wave Advantage 4.1; классические CPU в качестве бейзлайна | Да; эксперименты на D-Wave Advantage 4.1 |
| [Dixit et al., 2021] | IDS на ISCX IDS 2012; QARBM | 64 видимые и 64 скрытые логические единицы, всего 128 бинарных переменных и до $64 \cdot 64 = 4096$ видимо-скрытых связей до встраивания; каждый логический узел представлен цепочкой из 16 физических кубитов | Физический квантовый отжигатель D-Wave 2000Q; классическая RBM CD-1 как бейзлайн; бифуркационный решатель не использовался | Да; D-Wave 2000Q |
| [Li et al., 2015] | Malicious-code / IDS classification; AutoEncoder + + DBN | Явная QUBO не формулируется; используется классическая сжатая нейросетевая модель, например AutoEncoder $41 \to 300 \to 150 \to 75$ и DBN на выборке 2000 записей KDDCUP'99 | Классический компьютер с алгоритмом в MATLAB | Нет; классический бейзлайн |
| [Salama et al., 2011] | IDS на NSL-KDD; DBN-SVM | Явная QUBO не формулируется; DBN используется для снижения размерности, например $41 \to 13 \to$ $\to 5$ признаков, с последующей SVM-классификацией | Классический компьютер | Нет; классический бейзлайн |

Указанные ограничения могут быть частично компенсированы за счет гибридных стратегий, например путем применения классических моделей машинного обучения для предварительного отбора потенциальных аномалий или релевантных признаков с последующим использованием QUBO для финальной оптимизационной селекции.

Таким образом, формулировка задач обнаружения аномалий в виде QUBO-задач открывает возможность использования специализированных оптимизационных решателей, которые потенциально способны превзойти классические алгоритмы как по точности, так и по скорости. QUBO-формализм позволяет интегрировать несколько критериев аномальности в единую оптимизационную цель, что в ряде исследований привело к улучшению качества детекции выбросов в различных сценариях.

На уровне решателей квантовые отжигатели предлагают принципиально новый механизм поиска решений, основанный на квантовых физических эффектах. В отдельных работах демонстрируются преимущества по качеству получаемых моделей, однако на практике их применение ограничено шумами, проблемами связности и масштабируемости на реальном оборудовании. В то же время квантово вдохновленные алгоритмы сокращают разрыв между теоретическими возможностями квантовой оптимизации и практической реализацией, позволяя запускать QUBO-задачи на классических вычислительных архитектурах с высокой производительностью.

Текущая динамика исследований указывает на то, что представление задач обнаружения аномалий в виде QUBO, поддерживаемое как квантовыми, так и высокопроизводительными классическими решателями, может стать важным автономным или интегрируемым компонентом будущих систем кибербезопасности, обеспечивая более эффективное выявление угроз в условиях постоянно возрастающих объемов данных.

### *Сетевая безопасность*

Обеспечение безопасности коммуникационных сетей включает широкий спектр оптимизационных задач, таких как поиск защищенных маршрутов передачи данных, размещение защитных ресурсов (например, ловушек — honeypot — и сенсоров), а также сегментация сети для локализации угроз. Подобные задачи традиционно решаются с использованием эвристических методов или ручного проектирования. Однако с ростом масштабов и усложнением сетевых инфраструктур такие подходы становятся все менее масштабируемыми, а поиск оптимальных решений — более затруднительным.

В данном контексте QUBO-формализм и специализированные оптимизационные решатели, включая квантовые отжигатели, рассматриваются как перспективное направление для автоматизации процессов защиты сетей, предоставляя инструменты для быстрого и эффективного решения сложных оптимизационных задач. Современные исследования применения QUBO в сетевой безопасности охватывают задачи защищенной маршрутизации, восстановления цепочек атак, развертывания систем honeypot, конфигурации межсетевых экранов и оптимального размещения сенсоров. Поскольку QUBO-постановка совместима как с классическими, так и с квантовыми решателями, возможна реализация классических, квантовых и гибридных вычислительных подходов.

Маршрутизация в защищенных сетях связи требует поиска путей передачи данных с минимальным уровнем риска, избегая компрометированных узлов и перегруженных каналов, а также удовлетворяя ограничениям качества обслуживания (Quality of Service, QoS). Задача становится особенно сложной в беспроводных сенсорных сетях и ad-hoc-сетях, где необходимо одновременно учитывать требования к энергоэффективности, надежности и безопасности.

В частности, в работе [Chen et al., 2022] авторы предложили QUBO-формулировку задачи энергоэффективной маршрутизации в беспроводных сенсорных сетях (Wireless Sensor Networks, WSN) и реализовали ее с использованием физических квантовых отжигателей D-Wave 2000Q

и Advantage. Каждый возможный маршрут представлялся в виде бинарной переменной, а итоговая целевая функция QUBO учитывала суммарное энергопотребление сети и ограничения маршрутизации. Экспериментальные результаты на сетях малого масштаба показали, что квантовые процессоры D-Wave 2000Q и Advantage находили оптимальные или близкие к оптимальным маршруты быстрее по сравнению с классическими оптимизационными решателями.

Несмотря на ограниченные размеры исследуемых сетей, обусловленные аппаратными возможностями квантовых устройств, полученные результаты демонстрируют потенциал квантового отжига для ускоренного поиска оптимальных маршрутов. Важно отметить, что QUBO-подход позволяет естественным образом интегрировать не только энергетические критерии, но и показатели безопасности, например путем назначения повышенной стоимости маршрутам, проходящим через уязвимые или ненадежные узлы сети.

Еще одной важной и вычислительно сложной задачей в сетевой безопасности является восстановление путей атак. При обнаружении вторжения в сеть необходимо определить маршрут распространения вредоносного трафика от источника к целевому узлу. Классические методы анализа трафика часто сталкиваются с проблемами высокой вычислительной нагрузки и задержек обработки, особенно в распределенных сетевых средах.

В работе [Antwi et al., 2025] авторы применили QUBO-формализм для решения задачи трассировки атак в беспроводных сенсорных сетях (Wireless Sensor Networks, WSN). По типу реализации это сочетание сетевого моделирования и физического квантового отжига: сценарии формировались в среде ns-3, а оптимизационная часть решалась на D-Wave. Оптимизационная задача была сформулирована в виде следующей функции минимизации:

$$\min_x \sum_{i,j} c_{i,j} x_{i,j} + \lambda \sum_{i,j,k} (x_{i,j} + x_{j,k} - x_{i,k})^2,$$

где $c_{i,j}$ обозначает вес соединения или задержку передачи между узлами $i$ и $j$, а параметр $\lambda$ задает штраф за нарушение транзитивности маршрутов. Экспериментальные исследования проводились с использованием квантового отжигателя D-Wave в среде сетевого моделирования ns-3. Бинарные переменные $x_{i,j}$ кодировали гипотезы о передаче пакетов между узлами, а конфигурация с минимальной энергией соответствовала наиболее вероятному пути атаки.

По результатам экспериментов оптимизация на основе квантового отжига продемонстрировала существенное улучшение качества восстановления маршрутов, достигнув точности порядка 90 %, что заметно превышает показатели классических методов. Кроме того, уровень ложноположительных срабатываний снизился на 5–10 % при сохранении сопоставимых значений задержек и энергопотребления. Эти результаты подчеркивают практический потенциал квантовой оптимизации для задач анализа сетевой безопасности.

Еще одной важной задачей сетевой безопасности является оптимальное размещение honeypot-систем. Такие системы используются для привлечения и анализа атак без угрозы для реальных сервисов. Выбор их количества и расположения представляет собой сложную оптимизационную задачу, в рамках которой необходимо максимизировать вероятность перехвата атакующих воздействий на ловушки при одновременной минимизации затрат на их развертывание и предотвращении перегрузки сети избыточным числом приманок. В общем случае требуется определить подмножество узлов сети, которые будут выступать в роли ловушек, с учетом возможных пересечений путей атак.

В работе [Ngo et al., 2023] авторы показали, что задача оптимального размещения ловушек в сети является NP-трудной даже для статических графов. Эта работа используется здесь как прикладная постановка и теоретическое обоснование сложности honeypot placement; прямого запуска QUBO на QPU в ней не рассматривается. Вместе с тем было отмечено, что для

сетей небольшого размера данная задача может быть эффективно решена в виде QUBO-задачи с использованием квантовых оптимизационных решателей.

Насколько известно на сегодняшний день, полноценных исследований, напрямую применяющих QUBO-формализм к задаче оптимизации размещения honeypot-систем, пока не представлено. Тем не менее для формулирования соответствующей QUBO-задачи можно использовать следующие идеи. Рассматривая сеть в виде графа, каждому узлу сопоставляется бинарная переменная, принимающая значение 1 в случае размещения ловушки и 0 — в противном случае. Целевая функция может быть построена таким образом, чтобы ее минимум соответствовал максимальному пересечению возможных путей атак с узлами-ловушками. При этом каждая потенциальная атака вносит вклад в энергию системы в зависимости от того, проходит ли соответствующий путь через хотя бы один узел-ловушку. В целом данная постановка сводится к задачам максимального покрытия подграфа или поиска доминирующего множества, для которых известны эффективные QUBO-формулировки.

Еще одним важным аспектом является динамичность сетевых инфраструктур. Структура сети со временем изменяется, вследствие чего стратегии размещения honeypot-систем должны обладать адаптивностью. В случае ручного управления требуются постоянный мониторинг сети и повторное проектирование схем размещения ловушек при каждом изменении топологии, что является трудоемким и слабомасштабируемым процессом.

Использование квантовых или гибридных оптимизационных решателей потенциально позволяет автоматизировать процесс расстановки ловушек и выполнять переоптимизацию практически в режиме реального времени при изменении графа сети. Такой подход открывает возможность реализации слоя активной защиты, способного динамически адаптироваться к текущему состоянию инфраструктуры и эволюции угроз.

Следующий класс задач, представляющий значительный интерес в контексте сетевой безопасности, связан с сегментацией сети и оптимизацией межсетевых экранов. Корректная сегментация сети, то есть разделение инфраструктуры на изолированные зоны или сообщества с ограниченным взаимодействием, является ключевой стратегией защиты, направленной на предотвращение горизонтального перемещения атакующих. Под горизонтальным перемещением понимается распространение вредоносных агентов по внутренней сети после первоначального компрометирования системы.

Аналогичным образом оптимизация правил межсетевых экранов включает выбор, настройку и упорядочивание политик контроля доступа с целью блокирования вредоносного трафика при одновременном обеспечении прохождения легитимных потоков данных. Обе задачи могут быть сформулированы как комбинаторные задачи на графах или множествах, что делает их естественными кандидатами для моделирования в форме QUBO.

Одним из подходов к формализации сегментации является представление ее в виде задачи разбиения графа или кластеризации. Цель заключается в разделении сетевого графа на подграфы, соответствующие сегментам, таким образом, чтобы минимизировать число критических соединений между сегментами с точки зрения безопасности при одновременном выполнении заданных ограничений, например на размер сегментов или допустимые взаимодействия. Задача разбиения графа является классической NP-трудной задачей и естественным образом допускает формулировку в виде QUBO. Более того, квантовые отжигатели уже применялись для решения родственных задач, включая обнаружение сообществ в сложных сетевых структурах.

В частности, в работе [Negre et al., 2020] был продемонстрирован подход к решению задачи выявления сообществ в графе в формализме модели Изинга с использованием квантового отжигателя D-Wave. Для малых задач это физическая реализация на D-Wave 2X/2000Q, а для более крупных графов используются гибридная декомпозиция через qbsolv и инструменты D-Wave

Ocean. Под сообществами понимаются кластеры узлов с плотными внутренними связями и относительно разреженными внешними соединениями. Авторы показали, что задача обнаружения не более двух сообществ в сети «естественным образом вписывается» в архитектуру D-Wave и требует минимальной дополнительной переформулировки.

Решения, полученные с помощью квантового отжига, совпали с результатами классических алгоритмов кластеризации для графов малого масштаба. Данная работа иллюстрирует способность квантового отжига эффективно решать базовые задачи разбиения графов, что делает данный подход перспективным для задач сетевой сегментации в информационной безопасности.

Рассмотрим задачу сегментации сети в виде QUBO-постановки на примере разбиения на два кластера — $A$ и $B$. Каждый узел сети сопоставляется с бинарной переменной, указывающей его принадлежность к одному из сегментов. Квадратичные члены целевой функции накладывают штраф за каждое ребро графа, которое оказывается разрезанным между сегментами. Задача заключается в поиске такого разбиения на два подмножества, при котором число связей между сегментами минимально. Таким образом, минимизация энергии QUBO приводит к уменьшению количества межсегментных соединений, фактически реализуя задачу минимального разреза графа.

Дополнительные члены целевой функции могут вводиться для обеспечения баланса сегментов или учета ограничений по их размеру и пропускной способности, штрафуя чрезмерно неравномерные разбиения. Подобная QUBO-формулировка по своей сути совпадает с моделями, применяемыми в задачах сегментации изображений, которые уже были реализованы на квантовых отжигателях [Venkatesh et al., 2024]. Эта работа не является исследованием сетевой безопасности, но важна как пример смежной QUBO-задачи графового разбиения, решавшейся с использованием квантового отжига. Следовательно, методологическая база для квантово-ассистированной сегментации сетей уже существует.

Квантовые или гибридные оптимизационные решатели способны осуществлять поиск среди экспоненциально большого числа возможных сегментаций сети и находить разбиения, наиболее эффективно ограничивающие распространение угроз с учетом бизнес-ограничений. Например, путем изоляции узлов повышенного риска в отдельный карантинный сегмент.

Для наглядности рассмотрим аналогию с задачей сегментации изображений [Venkatesh et al., 2024]; здесь ссылка используется именно как переносимая методологическая аналогия, а не как прямой эксперимент по сегментации компьютерной сети. В данном случае каждый пиксель интерпретируется как узел графа, а ребра между узлами характеризуют степень схожести пикселей. Схожесть часто оценивается с использованием гауссовой метрики:

$$w'(p_i,\, p_j) = 1 - \exp\left(-\frac{\left(I(p_i) - I(p_j)\right)^2}{2\sigma^2}\right), \tag{18}$$

где $p_i$ и $p_j$ обозначают пиксели изображения, $I(p_i)$ и $I(p_j)$ — соответствующие значения интенсивности, а $\sigma$ является гиперпараметром, определяющим масштаб чувствительности метрики. Значения функции $w'$ лежат в интервале [0, 1]. Далее полученные значения нормализуются в интервал [−1, 1] следующим образом:

$$w(p_i,\, p_j) = -1 \cdot \left(\frac{(b-a)(w'(p_i,\, p_j) - \min(w'))}{\max(w') - \min(w')} + a\right), \tag{19}$$

где $a = -1$ и $b = 1$ задают требуемые границы нормализации, а $\max(w')$ и $\min(w')$ обозначают максимальное и минимальное значения по всем парам пикселей.

С учетом выражений (18) и (19) QUBO-задача принимает вид

$$\mathbf{x}^* = \arg\min_{\mathbf{x}} \sum_{1 \leqslant i < j \leqslant n} x_{p_i} \left(1 - x_{p_j}\right) w(p_i,\, p_j), \tag{20}$$

где $\mathbf{x} = \left(x_{p_1},\, x_{p_2},\, \ldots,\, x_{p_n}\right)$, а переменные $x_{p_i} \in \{0,\, 1\}$ определяют принадлежность соответствующего пикселя одному из сегментов.

Экспериментальные результаты показывают преимущество квантовых оптимизационных решателей по сравнению с ведущими классическими алгоритмами при сегментации изображений большого масштаба. Авторы [Venkatesh et al., 2024] также отмечают, что квантовые алгоритмы демонстрируют особенно высокую эффективность в условиях наличия шума в данных изображениях; перенос этого вывода на сетевые данные требует отдельной проверки.

Еще одной важной задачей сетевой безопасности является конфигурация правил межсетевых экранов, которую можно рассматривать с различных точек зрения. В частности, к числу ключевых подзадач относятся поиск минимального набора правил, обеспечивающего требуемый уровень защиты, а также оптимизация порядка применения правил с целью минимизации времени обработки трафика. Задача минимизации числа правил может быть сведена к задаче минимального покрытия множества, тогда как оптимизация их последовательности может рассматриваться как задача планирования или упорядочивания.

Учитывая, что оптимизация подобных задач в общем случае является NP-трудной, данные постановки естественным образом допускают формулировку в виде QUBO-задач и, следовательно, потенциально могут извлечь выгоду из использования квантовых оптимизационных решателей. Насколько нам известно, на момент проведения данного исследования специализированные работы, посвященные применению квантовых методов оптимизации к задаче конфигурации межсетевых экранов, пока отсутствуют. Тем не менее, учитывая успешные примеры применения QUBO-подходов в смежных областях оптимизации, представляется обоснованным ожидать появления будущих работ, использующих QUBO-модели для автоматизации настройки политик межсетевой безопасности, особенно в условиях возрастающей сложности корпоративных сетей и стремления к автономным системам защиты.

Таким образом, как сегментация сети, так и оптимизация конфигурации межсетевых экранов могут быть естественным образом сформулированы в виде QUBO-задач. Ранние результаты из смежных областей демонстрируют эффективность квантового оборудования для решения оптимизационных задач малого масштаба. Потенциальная выгода для обеспечения безопасности сети может быть значительной: оптимизированная сегментация способна динамически изолировать скомпрометированные участки сети с минимальным влиянием на функционирование системы, а оптимизированный набор правил межсетевого экрана может сокращать окна уязвимости и снижать задержки обработки трафика.

В защищенных сетевых средах, таких как корпоративные ИТ-инфраструктуры и объекты критической информационной инфраструктуры, развертывание датчиков, включая системы обнаружения вторжений (Intrusion Detection Systems, IDS) и мониторинговые зонды, играет ключевую роль в раннем выявлении угроз. Основная задача заключается в определении оптимального размещения ограниченного числа датчиков с целью максимального покрытия критических активов и ключевых маршрутов передачи данных. Это еще одна комбинаторная задача оптимизации, в которой из множества возможных позиций установки, например узлов или каналов сети, необходимо выбрать оптимальное подмножество из $k$ элементов.

Формально подобные задачи часто сводятся к различным вариантам задач покрытия множества или задач размещения объектов, которые являются NP-трудными, но допускают формулировку в виде QUBO и, соответственно, могут быть решены с использованием как классических, так и квантовых оптимизационных решателей, включая квантовые отжигатели.

Существуют успешные примеры применения квантового отжига и гибридных квантово-классических методов для эффективного решения задач размещения датчиков. В частности, в исследовании [Speziali et al., 2021], выполненном компанией *Idea-re S.r.l.*, рассматривалась задача оптимального размещения датчиков давления в сети водоснабжения. По типу реализации это гибридный подход: QUBO-задача сравнивалась при решении с классическим симулированным отжигом и гибридным квантово-классическим решателем D-Wave. Данная задача была сформулирована в виде QUBO и решена с использованием методов квантового отжига.

Ключевая цель заключалась в своевременном обнаружении и локализации утечек и неисправностей в инфраструктуре. Авторы описали способ построения QUBO-модели на основе графа сети и заданных негативных сценариев, в рамках которой минимум целевой функции соответствует оптимальному набору позиций размещения датчиков для мониторинга сети. В работе задача решалась как с помощью классического симулированного отжига, так и с применением гибридного квантово-классического решателя D-Wave. Сравнительный анализ показал, что гибридный квантовый подход продемонстрировал наилучшую производительность для решения практической задачи оптимизации в контексте сетей водоснабжения.

Минимум гамильтониана QUBO соответствовал конфигурациям размещения датчиков, при которых обеспечивались оптимальное обнаружение и локализация событий в сети. Представленная методология естественным образом переносится в область кибербезопасности: вместо датчиков давления и утечек в трубопроводной сети можно рассматривать IDS-датчики и кибератаки. В этом случае топология сети и возможные пути распространения атак определяют структуру QUBO-задачи. Кроме того, в формулировку QUBO могут быть включены веса, отражающие критичность узлов сети, что позволяет приоритизировать защиту наиболее ценных активов.

Обсудив отдельные конкретные механизмы защиты, перейдем к более общей задаче — распределению ресурсов и оптимизации киберзащиты в целом. Современные корпоративные системы информационной безопасности предполагают эффективное распределение ограниченных защитных ресурсов, включая honeypot-системы, сенсоры мониторинга, средства контроля доступа и оптимизированные наборы правил сетевой безопасности.

Принятие решений о том, какие уязвимости следует устранять, в каких узлах и в какой последовательности развертывать защитные механизмы, а также какие элементы инфраструктуры и в каком приоритете мониторить, представляет собой сложную задачу комбинаторной оптимизации. Современные злоумышленники часто применяют многоэтапные стратегии атак, включающие последовательное использование различных уязвимостей. Такая последовательность действий обычно описывается в рамках концепции **cyber kill chain**.

В этих условиях защитники должны выбирать такой набор мер, который разрывает все критические пути атак при минимальных затратах ресурсов. С формальной точки зрения поиск оптимальной стратегии защиты является NP-трудной задачей, близкой по структуре к задачам покрытия множества или вершинного покрытия на графе атак.

Классические подходы, такие как целочисленное линейное программирование и игровые модели, демонстрируют эффективность на сетях малого и среднего масштаба. Альтернативным направлением является использование эвристических методов. Так, в работе [Durkota et al., 2019] была предложена методика оптимального размещения защитных ловушек на графе атак с применением игр Штакельберга и динамического программирования. Это классический бейзлайн без QUBO-постановки и без квантового оборудования; он используется для сопоставления с потенциальными QUBO-подходами к защитному размещению ресурсов. Однако подобные решения оказываются существенно ограниченными по масштабируемости вследствие экспоненциального роста вычислительной сложности с увеличением размера сети.

В исследовании [Carney, 2022] авторы предложили QUBO-формулировку задачи разрыва цепочек атак на графе уязвимостей и реализовали ее с использованием квантовых отжигателей.

Здесь речь идет о прикладной QUBO-постановке с запуском на физическом D-Wave Advantage Solver 4.1 и сравнением с классическим ExactSolver на модельных графах. Несмотря на отсутствие обнаруженной журнальной версии, работа оставлена в обзоре из-за редкой прикладной постановки, связывающей модель kill chain, граф уязвимостей и оптимизационную QUBO-формализацию защитных действий. Целевая функция была построена таким образом, что минимум энергии соответствовал максимальному числу прерванных цепочек атак при ограниченном количестве ресурсов на устранение уязвимостей.

В другой работе [Marini, Arpe, 2025] была разработана строгая QUBO-модель оценки киберрисков, объединяющая локальные факторы риска узлов сети и штрафные члены, отражающие связанность рисков и распространение угроз по инфраструктуре. По типу реализации эта работа сопоставляет классические, квантовые и гибридные решатели, поэтому ее выводы относятся к полной вычислительной схеме, а не только к физической части квантового отжига. Эта работа включена из-за новизны задачи и наличия воспроизводимой модели, в которой киберриск представлен через локальные характеристики узлов, сетевые связи и ограничения распространения угроз. В данной модели гамильтониан системы представлен в виде линейной комбинации гамильтонианов отдельных подзадач:

$$H = \lambda_1 H_1 + \lambda_2 H_2 + \lambda_3 H_3 + \lambda_4 H_4 + \lambda_5 H_5, \tag{21}$$

где каждый компонент $H_k$ соответствует определенному типу риска, а коэффициенты $\lambda_k$ задают относительную важность соответствующих факторов и выступают настраиваемыми гиперпараметрами модели. В дальнейшем авторы подробно анализируют вклад каждой составляющей гамильтониана в итоговую оценку риска.

Первый гамильтониан $H_1$ направлен на сохранение итоговых уровней риска узлов вблизи их исходных значений. Он препятствует коллективному смещению рисков к усредненным уровням и делает существенное снижение риска для узлов с высоким начальным уровнем менее вероятным:

$$H_1 = \sum_i IS_i \cdot (IS_i - FS_i)^2,$$

где $IS_i$ обозначает исходный уровень риска узла $i$, а $FS_i$ — итоговый уровень риска узла $i$.

Второй гамильтониан $H_2$ штрафует конфигурации, в которых узлы с большим числом связей сохраняют высокий уровень риска, поскольку такие узлы потенциально способствуют более быстрому распространению угроз:

$$H_2 = \sum_{i<j} S_{i,j} \cdot FS_i \cdot FS_j,$$

где $S_{i,j}$ характеризует силу связи между узлами $i$ и $j$, а $FS_i$ и $FS_j$ — соответствующие итоговые уровни риска.

Третий гамильтониан $H_3$ моделирует влияние соседних узлов на уровень риска каждого элемента сети:

$$H_3 = \sum_i \left( FS_i - \frac{1}{|N(i)|} \sum_{j \in N(i)} FS_j \right)^2,$$

где $N(i)$ обозначает множество узлов, смежных с узлом $i$, а $|N(i)|$ — их количество.

Четвертый гамильтониан $H_4$ штрафует связанность между узлами, отмеченными признаками критической уязвимости, поскольку такие конфигурации могут ускорять системную компрометацию:

$$H_4 = -\sum_{i<j} \left( f_i^{\text{patched}} + f_i^{\text{internet}} + f_j^{\text{patched}} + f_j^{\text{internet}} \right) (FS_i + FS_j),$$

где бинарная переменная $f_i^{\text{patched}} = 0$ означает, что узел $i$ обновлен и, следовательно, менее уязвим, а переменная $f_i^{\text{internet}} = 1$ указывает на наличие у узла $i$ выхода в интернет.

Пятый и заключительный гамильтониан $H_5$ изолирует и существенно штрафует уменьшение уровня риска для критически опасных узлов ($IS_i \geqslant 7$), поскольку такие элементы инфраструктуры, как правило, сохраняют высокую уязвимость даже при окружении узлами с низким уровнем риска:

$$H_5 = -\sum_{i:\, IS_i \geqslant 7} FS_i.$$

Для решения данной задачи авторы использовали классические методы оптимизации (в частности, поиск с запретами), квантовый отжиг и гибридные квантово-классические подходы. В работе подчеркивается высокая гибкость предложенной модели, являющаяся одним из ее ключевых преимуществ, поскольку все компоненты целевой функции легко модифицируемы. Это позволяет адаптировать алгоритм к различным конфигурациям сетей и сценариям киберрисков.

Авторы [Marini, Arpe, 2025] также отмечают, что классические алгоритмы демонстрируют высокую эффективность при решении задач малого масштаба. Однако с увеличением размера сети время, необходимое для поиска решения, возрастает экспоненциально, что существенно ограничивает практическую применимость данных методов. Квантовые алгоритмы, напротив, теоретически предлагают более масштабируемый подход к решению подобных оптимизационных задач. Вместе с тем текущие аппаратные возможности квантовых решателей остаются ограниченными: значительная часть вычислительных ресурсов расходуется на предобработку QUBO-формулировок для встраивания на квантовую архитектуру, особенно в случаях плотных матриц взаимодействий.

Гибридные квантово-классические алгоритмы позволяют обойти ограничения, связанные с размещением полной QUBO-матрицы на квантовом устройстве, за счет распределения вычислительной нагрузки между классическими и квантовыми компонентами. Такой подход обеспечивает более стабильную масштабируемость и высокое качество получаемых решений в практических сценариях.

Сравнение рассмотренных работ по сетевой безопасности и методологически близких графовых задач приведено в табл. 3. В таблице отдельно указаны размерность и структурная сложность QUBO, тип использованного решателя и наличие запуска на физическом квантовом устройстве. Такое разделение существенно, поскольку часть публикаций представляет прямые эксперименты на квантовых отжигателях, часть использует гибридные или классические вычисления, а работы по размещению honeypot-систем и играм на графах атак включены только как классические сравнительные модели.

Из табл. 3 видно, что подтвержденные физические эксперименты в этой группе выполнены главным образом на квантовых отжигателях D-Wave; вентильные квантовые компьютеры и бифуркационные решатели в рассмотренных работах не применялись. Прямой запуск ограничивается малыми либо разреженными QUBO, тогда как увеличение числа переменных и плотности связей приводит к декомпозиции, классическому решению или использованию управляемых гибридных сервисов. Кроме того, результаты по выявлению сообществ, сегментации изображений и размещению сенсоров следует трактовать как переносимые графовые аналоги, а не как прямые эксперименты по защите компьютерных сетей.

## Заключение

Проведенный обзор демонстрирует, что квантовая оптимизация и, в частности, формализм квадратичной неограниченной бинарной оптимизации (QUBO) формируют универсальную

Таблица 3. Сравнение QUBO-подходов и смежных моделей в задачах сетевой безопасности

| Работа | Задача и модель | Размерность QUBO / сложность | Тип QPU/решателя: отжигатель, компьютер, бифуркация | Физическое квантовое устройство |
|---|---|---|---|---|
| [Chen et al., 2022] | Энергоэффективная маршрутизация WSN; выбор одного пути для каждого потока | Число переменных определяется наборами допустимых путей и slack-переменными; графы содержат 4–12 узлов и до 11 источников. Большинство успешных прямых запусков имело менее 20 переменных; после редукции размер плотных экземпляров достигал первых сотен переменных | Физические квантовые отжигатели D-Wave 2000Q и Advantage System 1.1; CPLEX и Gurobi на классическом компьютере | Да; D-Wave 2000Q и Advantage |
| [Antwi et al., 2025] | IP-трассировка в WSN; бинарная переменная для каждого кандидатного ориентированного ребра | $\|E\|$ логических переменных, в плотном ориентированном графе до $O\left(\|V\|^2\right)$; моделировалась сеть из 100 узлов. Точное число логических и физических кубитов не приведено | Квантовый отжигатель D-Wave Advantage для малых экземпляров; D-Wave hybrid и классический `qbsolv` для крупных | Да для малых экземпляров; крупные решались гибридно и классически |
| [Ngo et al., 2023] | Размещение honeypot в динамических графах Active Directory; MIP, не QUBO | QUBO отсутствует; статическая задача NP-трудна. Для $m$ снимков графа с $n$ узлами MIP содержит $O(mn)$ переменных; рассматриваются тысячи узлов, сотни тысяч ребер и миллионы путей | Классический компьютер: MIP, динамическое программирование и жадный поиск | Нет; классический бейзлайн |
| [Negre et al., 2020] | Выявление сообществ как максимизация модулярности; аналог сегментации сети | Для двух сообществ — $n$ переменных; для $k$ сообществ — $nk$ one-hot-переменных с плотными связями внутри $k$ блоков. Тесты: 34–453 узла, до 2265 переменных; прямое полное встраивание ограничено 46/64 переменными | Физические квантовые отжигатели D-Wave 2X и 2000Q; гибридный `qbsolv` и SA | Да для подзадач и малых экземпляров; крупные декомпозировались |
| [Venkatesh et al., 2024] | Минимальный разрез графа для сегментации изображений; переносимый аналог сегментации сети | $n$ переменных и $O(n)$ связей для сетки степени не более четырех; пространство решений $2^n$, общий минимальный разрез со знаковыми весами NP-труден. Эксперименты: 4–1936 переменных, реальные изображения — патчи по 1024 переменные | Физический квантовый отжигатель D-Wave Advantage (5670 кубитов); Gurobi на классическом компьютере | Да; реальный D-Wave, но задача не относится напрямую к кибербезопасности |
| [Speziali et al., 2021] | Размещение сенсоров как взвешенное вершинное покрытие с ограничением мощности | 1368 переменных при $s = 48$ или до 1416 с one-hot-переменными; штраф $\left(\sum_i x_i - s\right)^2$ делает QUBO плотной. Прямое встраивание в Chimera/Pegasus оказалось невозможным | D-Wave Leap Hybrid Solver и SA на классическом компьютере | Нет; только управляемый гибридный решатель |
| [Durkota et al., 2019] | Защита сети в игре на графе атак; классическая сравнительная модель, не QUBO | QUBO-размерность отсутствует; оптимизация на графе атак выполняется методами игр Штакельберга и динамического программирования | Классический компьютер | Нет; классический бейзлайн |
| [Carney, 2022] | Разрыв цепочки атаки на графе уязвимостей; QUBO защитных действий | Размерность QUBO не приведена | Физический квантовый отжигатель D-Wave Advantage Solver 4.1; классический ExactSolver | Да; D-Wave Advantage 4.1 |
| [Marini, Arpe, 2025] | Оценка киберриска по локальным факторам и связям между узлами | Точная размерность QUBO не установлена | В тексте заявлено сравнение классического табу поиска, квантового отжига и гибридного решателя; бифуркация не использовалась | Не подтверждено по предоставленному источнику |

вычислительную основу для решения широкого класса задач информационной безопасности. Представляя криптоанализ, обнаружение аномалий, сетевую сегментацию, размещение защитных ресурсов и управление киберрисками в виде единых оптимизационных моделей, QUBO позволяет использовать как квантовые вычислительные устройства, так и высокопроизводительные классические и гибридные решатели в рамках общей методологической парадигмы.

Анализ существующих исследований показывает, что квантовые алгоритмы, в особенности квантовый отжиг и алгоритмы на основе адиабатической эволюции, способны обеспечивать улучшение качества решений и ускорение поиска оптимальных конфигураций в задачах малого и среднего масштаба. Однако текущее развитие квантового аппаратного обеспечения накладывает существенные ограничения на практическое применение квантовых вычислений для полномасштабных задач кибербезопасности. Основными барьерами остаются ограниченное число кубитов, шумы, сложности встраивания плотных QUBO-матриц и значительные накладные расходы на предобработку задач.

В этих условиях наибольший практический потенциал демонстрируют гибридные квантово-классические подходы, позволяющие сочетать вычислительную мощность классических архитектур с эвристическими преимуществами квантовых оптимизаторов. Такие методы уже сегодня обеспечивают масштабируемость и устойчивость решений, формируя реалистичный путь внедрения квантовой оптимизации в прикладные системы информационной безопасности. Квантово вдохновленные алгоритмы дополнительно сокращают разрыв между теорией и практикой, предоставляя эффективные инструменты для решения QUBO-задач без необходимости использования реального квантового оборудования.

Особое значение имеет гибкость QUBO-формулировки, позволяющая интегрировать предметно-ориентированные знания, ограничения и приоритеты непосредственно в целевую функцию. Это делает возможным динамическую адаптацию моделей безопасности к изменяющейся инфраструктуре, угрозам и требованиям бизнеса, включая потенциальную работу в режиме, близком к реальному времени. Таким образом, QUBO выступает не только как средство квантовой оптимизации, но и как универсальный язык формализации сложных систем киберзащиты.

Несмотря на значительный интерес к применению квантовых алгоритмов в криптоанализе, проведенный обзор показывает, что не менее перспективными являются задачи оптимизации сетевых конфигураций, распределения защитных ресурсов, управления киберрисками и детекции аномалий. Эти направления пока остаются менее исследованными, однако обладают высоким потенциалом практической значимости. Более того, многие из них имеют прямые аналоги в смежных областях, таких как логистика, управление инфраструктурами и анализ сложных сетей, что открывает возможности для переноса уже существующих QUBO-моделей и оптимизационных стратегий.

В перспективе ключевыми направлениями развития являются создание универсальных QUBO-фреймворков для классов задач безопасности, совершенствование методов декомпозиции и прореживания QUBO-матриц, а также разработка алгоритмических подходов для эффективного встраивания задач на квантовые архитектуры. Прогресс в этих областях позволит существенно снизить вычислительные издержки и расширить применимость квантовой оптимизации в реальных системах.

В целом квантовая оптимизация в формализме QUBO уже сегодня формирует фундамент для нового поколения интеллектуальных систем кибербезопасности. Несмотря на существующие аппаратные ограничения, сочетание квантовых, квантово вдохновленных и гибридных методов демонстрирует устойчивый прогресс и практическую ценность. По мере развития квантовых технологий можно ожидать, что QUBO-подход станет одним из ключевых инструментов для автоматизированного, масштабируемого и адаптивного управления безопасностью в условиях растущей сложности цифровых экосистем.

## Список литературы (References)

*Albash T., Lidar D. A.* Adiabatic Quantum Computation // Reviews of Modern Physics. — 2018. — Vol. 90, No. 1. — P. 015002. — DOI: 10.1103/RevModPhys.90.015002

*Antwi M., Osei-Wusu F., Asiedu W., Barfi M., Atuahene W. A., Muntaka S. A.* A quantum annealing-based approach for IP traceback in WSNs // Journal of Electrical Systems and Information Technology. — 2025. — Vol. 12. — Art. 85. — DOI: 10.1186/s43067-025-00279-w

*Barahona F.* On the computational complexity of Ising spin glass models // Journal of Physics A: Mathematical and General. — 1982. — Vol. 15, No. 10. — P. 3241–3253.

*Boros E., Gruber A.* On quadratization of pseudo-Boolean functions // International Symposium on Artificial Intelligence and Mathematics (ISAIM). — 2012.

*Burek E.* Converting of Simon cipher multivariate polynomial equations to QUBO problem // Tatra Mountains Mathematical Publications. — 2025. — Vol. 91, No. 3. — P. 23–50. — DOI: 10.2478/tmmp-2025-0006

*Burek E., Wroński M.* Quantum annealing and algebraic attack on speck cipher // Proceedings of ICCS 2022. — Lecture Notes in Computer Science (LNCS). — Springer, 2022. — Vol. 13353. — P. 130–143. — DOI: 10.1007/978-3-031-08760-8_12

*Burek E., Wroński M. J., Mańk K., Misztal M.* Algebraic attacks on block ciphers using quantum annealing // IEEE Transactions on Emerging Topics in Computing. — 2022. — Vol. 10, No. 2. — P. 678–689. — DOI: 10.1109/TETC.2022.3143152

*Canonici E., Caruso F.* QUBO-based SVM for credit card fraud detection on a real QPU // arXiv preprint. — 2024. — arXiv:2409.11876 [quant-ph]

*Carney M.* Cutting medusa's path — tackling kill-chains with quantum computing // arXiv preprint. — 2022. — arXiv:2211.13740 [quant-ph]

*Chen J., Date P., Chancellor N., Atiquzzaman M., Sreenan C.* Controller-based energy-aware wireless sensor network routing using quantum algorithms // IEEE Transactions on Quantum Engineering. — 2022. — Vol. 3. — Art. 3102912. — P. 1–12. — DOI: 10.1109/TQE.2022.3217297.

*Dennard R. H., Gaensslen F. H., Yu H.-N., Rideout V. L., Bassous E., LeBlanc A. R.* Design of ion-implanted MOSFET's with very small physical dimensions // IEEE Journal of Solid-State Circuits. — 1974. — Vol. 9, No. 5. — P. 256–268. — DOI: 10.1109/JSSC.1974.1050511

*Ding J., Spallitta G., Sebastiani R.* Effective prime factorization via quantum annealing by modular locally-structured embedding // Scientific Reports. — 2024. — Vol. 14. — P. 3518. — DOI: 10.1038/s41598-024-53708-7

*Ding J., Spallitta G., Sebastiani R.* Experimenting with D-Wave quantum annealers on prime factorization problems // Frontiers in Computer Science. — 2024. — Vol. 6. — P. 1335369. — DOI: 10.3389/fcomp.2024.1335369

*Dixit V., Selvarajan R., Aldwairi T., Koshka Y., Novotny M. A., Humble T. S., Alam M. A., Kais S.* Training a quantum annealing based restricted Boltzmann machine on cybersecurity data // IEEE Transactions on Emerging Topics in Computational Intelligence. — 2021. — Vol. 6. — P. 417–428.

*Dridi R., Alghassi H.* Prime factorization using quantum annealing and computational algebraic geometry // Scientific Reports. — 2017. — Vol. 7. — P. 43048. — DOI: 10.1038/srep43048

*Durkota K., Lisý V., Bosanský B., Kiekintveld C., Pechouček M.* Hardening networks against strategic attackers using attack graph games // Computers & Security. — 2019. — Vol. 87. — P. 101578. — DOI: 10.1016/j.cose.2019.101578

*Farhi E., Goldstone J., Gutmann S., Lapan J., Lundgren A., Preda D.* A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem // Science. — 2001. — Vol. 292, No. 5516. — P. 472–475. — DOI: 10.1126/science.1057726

*Farhi E., Goldstone J., Gutmann S., Sipser M.* Quantum computation by adiabatic evolution // arXiv preprint. — 2000. — arXiv:quant-ph/0001106

*Geman S., Geman D.* Stochastic relaxation, Gibbs distributions, and the Bayesian restoration of images // IEEE Transactions on Pattern Analysis and Machine Intelligence. — 1984. — Vol. 6, No. 6. — P. 721–741. — DOI: 10.1109/TPAMI.1984.4767596

*Goto H.* Bifurcation-based adiabatic quantum computation with a nonlinear oscillator network // Scientific Reports. — 2016. — Vol. 6. — P. 21686. — DOI: 10.1038/srep21686

*Goto H.* Quantum computation based on quantum adiabatic bifurcations of Kerr-nonlinear parametric oscillators // Journal of the Physical Society of Japan. — 2019. — Vol. 88. — P. 061015. — DOI: 10.7566/JPSJ.88.061015

*Grover L. K.* Quantum mechanics helps in searching for a needle in a haystack // Physical Review Letters. — 1997. — Vol. 79, No. 2. — P. 325–328. — DOI: 10.1103/PhysRevLett.79.325

*Ising E.* Beitrag zur theorie des ferromagnetismus // Zeitschrift für Physik. — 1925. — Vol. 31. — P. 253–258.

*Jiang S., Britt K. A., McCaskey A. J., Humble T. S., Kais S.* Quantum annealing for prime factorization // Scientific Reports. — 2018. — Vol. 8. — P. 17667. — DOI: 10.1038/s41598-018-36058-z

*Johnson M. W., Amin M. H. S., Gildert S., Lanting T., Hamze F., Dickson N., Harris R., Berkley A. J., Bunyk P., Chapple E. M., Enderud C., Hilton J. P., Karimi K., Ladizinsky E., Ladizinsky N., Oh T., Perminov I., Rich C., Thom M. C., Tolkacheva E., Uchaikin S., Wang J., Wilson B., Rose G.* Quantum annealing with manufactured spins // Nature. — 2011. — Vol. 473. — P. 194–198. — DOI: 10.1038/nature10012

*Jun K., Lee H.* HUBO and QUBO models for prime factorization // Scientific Reports. — 2023. — Vol. 13. — P. 10080. — DOI: 10.1038/s41598-023-36813-x

*Kadowaki T., Nishimori H.* Quantum annealing in the transverse Ising model // Physical Review E. — 1998. — Vol. 58, No. 5. — P. 5355–5363. — DOI: 10.1103/PhysRevE.58.5355

*Kirkpatrick S., Gelatt C. D., Vecchi M. P.* Optimization by simulated annealing // Science. — 1983. — Vol. 220, No. 4598. — P. 671–680.

*Li Y., Ma R., Jiao R.* A hybrid malicious code detection method based on deep learning // International Journal of Security and Its Applications. — 2015. — Vol. 9, No. 5. — P. 205–216. — DOI: 10.14257/ijsia.2015.9.5.21

*Lucas A.* Ising formulations of many NP problems // Frontiers in Physics. — 2014. — Vol. 2. — P. 5. — DOI: 10.3389/fphy.2014.00005

*Marini R., Arpe R.* Cyber risk scoring with QUBO: A quantum and hybrid benchmark study // arXiv preprint. — 2025. — arXiv:2512.18305 [quant-ph]

*Mellaerts J.* Quantum-inspired anomaly detection, a QUBO formulation // arXiv preprint. — 2023. — arXiv:2311.03227 [quant-ph]

*Mirrahimi M., Leghtas Z., Albert V. V., Touzard S., Schoelkopf R. J., Jiang L., Devoret M. H.* Dynamically protected cat-qubits: A new paradigm for universal quantum computation // New Journal of Physics. — 2014. — Vol. 16. — P. 045014. — DOI: 10.1088/1367-2630/16/4/045014

*Moore G. E.* Cramming more components onto integrated circuits // Electronics. — 1965. — Vol. 38, No. 8. — P. 114–117.

*Moro L., Prati E.* Anomaly detection speed-up by quantum restricted Boltzmann machines // Communications Physics. — 2023. — Vol. 6, No. 1. — P. 269. — DOI: 10.1038/s42005-023-01390-y

*Mukherjee S., Chakrabarti B. K.* Multivariable optimization: quantum annealing and computation // The European Physical Journal Special Topics. — 2015. — Vol. 224, No. 1. — P. 17–24. — DOI: 10.1140/epjst/e2015-02346-8

*Negre C. F. A., Ushijima-Mwesigwa H., Mniszewski S. M.* Detecting multiple communities using quantum annealing on the D-Wave system // PLOS ONE. — 2020. — Vol. 15, No. 2. — P. e0227538. — DOI: 10.1371/journal.pone.0227538

*Ngo Q. H., Guo M., Nguyen H.* Near optimal strategies for honeypots placement in dynamic and large active directory networks // Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2023), Poster Session / Innovative Applications Track. — 2023. — P. 2517–2519.

*Pakhomchik A. I., Voloshinov V. V., Vinokur V. M., Lesovik G. B.* Converting of Boolean expression to linear equations, inequalities and QUBO penalties for cryptanalysis // Algorithms. — 2022. — Vol. 15, No. 2. — P. 33. — DOI: 10.3390/a15020033

*Phab L., Louise S., Sirdey R.* First attempts at cryptanalyzing a (toy) block cipher by means of quantum optimization approaches // Journal of Computational Science. — 2023. — Vol. 69. — P. 102004. — DOI: 10.1016/j.jocs.2023.102004

*Ryou A., Kim K., Jun K.* Quantum prime factorization algorithms using binary carry propagation // arXiv preprint. — 2025. — arXiv:2506.16799 [quant-ph]

*Salama M. A., Eid H. F., Ramadan R. A., Darwish A., Hassanien A. E.* Hybrid intelligent intrusion detection scheme // Soft Computing in Industrial Applications / eds. A. Gaspar-Cunha, R. Takahashi, G. Schaefer, L. Costa. — Advances in Intelligent and Soft Computing. — Berlin, Heidelberg: Springer, 2011. — Vol. 96. — P. 293–303. — DOI: 10.1007/978-3-642-20505-7_26

*Shor P. W.* Algorithms for quantum computation: discrete logarithms and factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science (SFCS'94). — 1994. — P. 124–134. — DOI: 10.1109/SFCS.1994.365700

*Speziali S., Bianchi F., Marini A., Menculini L., Proietti M., Termite L. F., Garinei A., Marconi M., Delogu A.* Solving sensor placement problems in real water distribution networks using adiabatic quantum computation // Proceedings of the IEEE International Conference on Quantum Computing and Engineering (QCE 2021). — IEEE, 2021. — P. 463–464. — DOI: 10.1109/QCE52317.2021.00079

*Stein J., Schuman D., Benkard M., Holger T., Sajko W., Kölle M., Nüßlein J., Sünkel L., Salomon O., Linnhoff-Popien C.* Exploring unsupervised anomaly detection with quantum Boltzmann machines in fraud detection // Proceedings of the 16th International Conference on Agents and Artificial Intelligence (ICAART 2024). — SCITEPRESS, 2024. — Vol. 2. — P. 177–185. — DOI: 10.5220/0012326100003636

*Venkatesh S. M., Macaluso A., Nuske M., Klusch M., Dengel A.* Q-Seg: quantum annealing-based unsupervised image segmentation // IEEE Computer Graphics and Applications. — 2024. — Vol. 44. — P. 27–39. — DOI: 10.1109/MCG.2024.3455012

*Wroński M., Burek E., Leśniak M.* (In)security of stream ciphers against quantum annealing attacks on the example of the Grain 128 and Grain 128a ciphers // IEEE Transactions on Emerging Topics in Computing. — 2025. — Vol. 13, No. 3. — P. 614–627. — DOI: 10.1109/TETC.2024.3474856

*Zhang A., Feng X.* Applications of quantum annealing in cryptography // arXiv preprint. — 2022. — arXiv:2211.10076