 © Авторы статьи / Authors of the article

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2026.167.103 EDN: HZDEET

ОЦЕНКА ВОЗМОЖНОСТЕЙ ПЕРЕХВАТА ИНФОРМАЦИИ ЧЕРЕЗ ПОБОЧНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ И НАВОДКИ ПРИ ФУНКЦИОНИРОВАНИИ КВАНТОВЫХ ПРОЦЕССОРОВ

Научная статья

Еремина А.П.[1, *], Москвитин Г.И.[2]
[1] ORCID : 0009-0004-4036-6944;
[1, 2] МИРЭА – Российский технологический университет, Москва, Российская Федерация

* Корреспондирующий автор (vgera[at]list.ru)

Предложена: 17.02.2026; Принята: 06.05.2026; Опубликована: 18.05.2026

Аннотация

В работе проводится комплексный анализ уязвимостей аппаратной части сверхпроводниковых квантовых вычислительных систем к утечкам информации по техническим каналам побочных электромагнитных излучений и наводок (ПЭМИН). Подробно рассматриваются физические принципы функционирования кубитов на базе джозефсоновских переходов как источников осциллирующих электромагнитных и магнитных полей. Произведена теоретическая оценка напряженности поля, генерируемого цепями управления, и дальности его распространения за пределы криостата. Обоснована возможность негласного перехвата информативных сигналов с использованием современной измерительной базы, включая высокотемпературные СКВИД-магнитометры, в сочетании с методами цифровой обработки (когерентного накопления и оптимальной фильтрации). На основе полученных данных разработаны практические рекомендации по построению систем активной и пассивной защиты, включающие методы многослойного экранирования и криогенной фильтрации в условиях эксплуатации в центрах обработки данных.

Ключевые слова: квантовый процессор, ПЭМИН, информационная безопасность, сверхпроводящие кубиты, СКВИД, побочные каналы, утечка информации.

ASSESSMENT OF THE POTENTIAL FOR INFORMATION INTERCEPTION VIA SIDE ELECTROMAGNETIC RADIATION AND INDUCING DURING THE OPERATION OF QUANTUM PROCESSORS

Research article

Eremina A.P.[1, *], Moskvitin G.I.[2]
[1] ORCID : 0009-0004-4036-6944;
[1, 2] MIREA – Russian Technological University, Moscow, Russian Federation

* Corresponding author (vgera[at]list.ru)

Suggested: 17.02.2026; Accepted: 06.05.2026; Published: 18.05.2026

Abstract

The work presents a complex analysis of the vulnerabilities of the hardware components of superconducting quantum computing systems to information leakage via technical channels of Transient ElectroMagnetic Pulse Emanation Standard (TEMPEST). The physical principles of the operation of qubits based on Josephson junctions as sources of oscillating electromagnetic and magnetic fields are examined in detail. A theoretical assessment is made of the field strength generated by control circuits and the range of its propagation beyond the cryostat. The possibility of covert interception of informative signals using modern measurement equipment, including high-temperature SQUID magnetometers, in combination with digital processing methods (coherent accumulation and optimal filtering), is substantiated. Based on the obtained data, practical recommendations have been developed for the construction of active and passive protection systems, including methods of multilayer shielding and cryogenic filtering under operating conditions in data centres.

Keywords: quantum processor, TEMPEST, information security, superconducting qubits, SQUID, side channels, information leakage.

Введение

В настоящее время мир находится на пороге «второй квантовой революции», характеризующейся переходом с фундаментальных открытий к созданию практических квантовых технологий, таких как квантовые компьютеры, квантовая связь и высокоточные сенсоры, которые используют манипуляцию с квантовым состоянием, кубитами. Согласно дорожной карте развития высокотехнологичной области «Квантовые вычисления» в Российской Федерации, к 2030 году планируется создание универсальных квантовых компьютеров, способных решать прикладные задачи в интересах атомной, химической и финансовой отраслей [1]. Подобные системы перестают быть исключительно лабораторными установками, они интегрируются в облачные платформы и центры обработки данных, что ставит новые вопросы для информационной безопасности.

Традиционный подход к безопасности квантовых технологий в основной массе сфокусирован на постквантовой криптографии и защите алгоритмом. Однако надо не забывать, как и в классической вычислительной технике, физическая реализация вычислителя неизбежно вызывает побочные эффекты. Любая обработка информации, на

 © Авторы статьи / Authors of the article

аппаратном уровне сопровождается изменением токов, напряжением и магнитных потоков, что приводит к генерации побочных электромагнитных излучений и наводок (ПЭМИН). Для оборонной и аэрокосмической отраслей понимание этих физических уязвимостей становится критически важным фактором обеспечения технологического суверенитета [2].

Реализация систем квантовой обработки информации существенно отличается от идеализированных математических моделей. Без учета неидеальностей реальных систем, таких как флуктуации параметров, тепловые шумы и паразитные связи, невозможно гарантировать криптографическую и эксплуатационную стойкость оборудования [3]. Квантовые процессоры на сверхпроводниковых кубитах, являющиеся одной из лидирующих платформ (Google, IBM, «Росатом»), работают в микроволновом диапазоне (4–8 ГГц) и управляются быстрыми импульсами магнитного потока.

Проблема исследования заключается в том, что физические процессы, управления кубитами, создают физическое поле, которые могут выходить за пределы криостата, или наводится на вспомогательные цепи. Злоумышленник, оснащённый современной измерительной аппаратурой, теоретически может зарегистрировать эти поля и восстановить информацию о квантовом регистре, при этом не нарушая целость состояния, а лишь пассивно наблюдать за вычислениями

Целью данной работы является оценка возможности перехвата информации, циркулирующей в квантовом процессоре, через электромагнитные и магнитные каналы, а также анализ методов противодействия данным угрозам.

Научная новизна работы заключается в следующем:

1) предложена комплексная модель угроз утечки информации по каналам ПЭМИН для сверхпроводниковых квантовых процессоров, учитывающая как СВЧ-сигналы управления (4–8 ГГц), так и низкочастотные магнитные поля;

2) выполнена количественная оценка возможности перехвата информативных сигналов на различных расстояниях (от 5 см до 1 м) с учетом чувствительности современных ВТСП-СКВИД сенсоров;

3) обоснована применимость алгоритмических методов маскировки вычислений (введение «шумовых» квантовых операций) как специфического средства защиты квантовых систем.

Физическая природа излучений квантового процессора и оценка дальности распространения

В основе функционирования наиболее распространённых на сегодняшний день квантовых процессоров лежат сверхпроводящие цепи. Базовым элементом джозефсоновский переход – это структура из двух сверхпроводников, разделенный тонким слоем диэлектрика.

2.1. Генерация электромагнитных полей

С точки зрения электродинамики, кубит (например, трансмон) представляет собой нелинейный колебательный контур. Управление его состоянием осуществляется посредством подачи микроволновых импульсов в диапазоне 4–8 ГГц.

Амплитуда управляющих микроволновых импульсов, подаваемых на входные линии криостата, составляет порядка 10–100 мВ, однако после прохождения через каскад аттенюаторов (для снижения теплового шума) до самого чипа доходит сигнал мощностью порядка -100 дБм (10^-13 Вт) [6]. Тем не менее, даже столь малая мощность в замкнутом объеме криостата способна создавать паразитные переотражения.

Динамика кубита описывается нестационарным эффектом Джозефсона. Напряжение на переходе связано с изменением фазы волновой функции соотношением, приведенным в работах Kraft [4] и Krantz [6]:

$$\frac{\mathrm{d}\phi}{\mathrm{dt}} = \frac{2\mathrm{eV}}{\mathrm{h}}$$

где V — напряжение, e — заряд электрона, а $\hbar$ — приведенная постоянная Планка. Данное соотношение показывает, что изменение квантового состояния сопровождается протеканием осциллирующих токов I(t) в контуре кубита и подводящих линиях.

Это теория гласит, что любое изменение квантового состояния, вызванное управляющим напряжением, создают осциллирующие токи высокой частоты. Эти токи протекают не только в самом кубите, а также в линиях управления и считывания, которые также могут стать передающие антенны. В случае недостаточного экранирования или наличия паразитных связей, часть энергии этих СВЧ-сигналов излучается в окружающее пространство в виде побочных электромагнитных излучений (ПЭМИ).

2.2. Магнитные поля и оценка уровня сигнала

Для настройки частоты кубитов и организации взаимодействия между ними используются сверхпроводящие квантовые интерферометры “SQUID”, интегрированные непосредственно в архитектуру процессора. Управление такими элементами происходит за счет изменения магнитного потока Ф, пронизывающего контур [5].

Ток управления, протекающий по шинам смещения, создает магнитное поле. Поскольку операции квантовой логики требуют быстрых изменений состояния, из-за этого изменение магнитного поля носит импульсный характер. Типичные токи управления составляют порядка I ≈ 1–10 мкА. Согласно законам электродинамики, переменное магнитное поле порождает вихревое электрическое поле, что создает условия для возникновения наводок на соседние проводники и элементы конструкции криостата [3].

Для оценки возможности перехвата воспользуемся законом Био-Савара-Лапласа. Индукция магнитного поля B на расстоянии r от проводника с током I оценивается как:

$$\boldsymbol{B} = \frac{\mu_0 I}{2\pi r}$$

 © Авторы статьи / Authors of the article

Для количественного обоснования возможности перехвата нами была выполнена оценка отношения сигнал/шум (SNR) для канала утечки. Отношение сигнал/шум определяется как:

$$SNR = \frac{B_{\text{signal}}}{\delta B \cdot \sqrt{\Delta f}}$$

где $B \quad signal$ — индукция магнитного поля, δB — чувствительность датчика, Δf — полоса пропускания.

Принимая длительность управляющего импульса $\tau \approx 20$ нс ($\Delta f \approx 50$ МГц) и чувствительность ВТСП-СКВИД $\delta B \approx 44$ фТл/ $\sqrt{\text{Гц}}$, получаем:

· на расстоянии 5 см ($B \approx 40$ пТл): $SNR \approx 0,13$;

· на расстоянии 1 м ($B \approx 2$ пТл): $SNR \approx 0,006$.

Это означает, что одиночный импульс не выделяется на фоне шума. Однако при когерентном накоплении по N циклам отношение сигнал/шум растет как √N. Для достижения уровня достоверного обнаружения (SNR>5) требуется накопление по $N \approx 1,5 \cdot 10^3$ циклам (для 5 см) и до $N \approx 7 \cdot 10^5$ (для 1 м).

При типичной тактовой частоте управляющей электроники квантового процессора (1–10 МГц), время восстановления сигнала составляет от 0,001 до 0,7 секунд. Это доказывает, что перехват информации возможен в режиме реального времени даже при значительном удалении датчика от криостата.

Как раз эти наводки и могут быть зарегистрированы внешними высокочувствительными датчиками, что позволяет злоумышленнику восстановить последовательность управляющих импульсов, а следовательно, и логику исполняемого квантового алгоритма.

При токе управления I =10 мкА на расстоянии r = 5 см (типичное расстояние до внешнего кожуха криостата) магнитное поле составит порядка 40 пТл. На расстоянии r = 1 метр (при размещении датчика вне стойки) уровень поля падает до 2 пТл.

Чувствительность современных СКВИД-сенсоров составляет 40–50 фТл/√Гц, что значительно ниже расчетного уровня сигнала. Это позволяет злоумышленнику восстановить последовательность управляющих импульсов, а следовательно, и логику исполняемого квантового алгоритма.

Технические средства перехвата и методы анализа сигналов

В рамках исследования проведено сопоставление технических средств перехвата по критерию эффективности регистрации сигналов квантового процессора. Результаты анализа сведены в таблицу 1.

Таблица 1 - Сравнительный анализ технических средств перехвата ПЭМИН

DOI: https://doi.org/10.60797/IRJ.2026.167.103.1

Средство перехвата	Эффективность	Дистанция	Особенности и ограничения
СВЧ-антенны	Низкая	< 0,1 м	Сильное затухание сигнала (4–8 ГГц) в защитном кожухе криостата.
Низкотемпературные СКВИД (LTS)	Высокая	до 0,5 м	Требуют охлаждения жидким гелием (4 К), громоздкость, сложность скрытой атаки.
ВТСП-СКВИД (HTS)	Оптимальная	до 1,5 м	Работа при 77 К (жидкий азот), компактность, мобильность, высокая чувствительность.
Лазерные виброметры	Средняя	Прямая видимость	Позволяют косвенно восстановить циклы вычислений через микровибрации корпуса.

Успешность атаки по побочным каналам на квантовый процессор, определяется чувствительностью приемной аппаратуры и эффективностью алгоритмов выделения полезного сигнала из шума. Учитывая крайне малые величины магнитных полей, генерируемых кубитами, использовать стандартные антенны анализаторы спектра будет неэффективно. Поэтому основным инструментом для перехвата становятся сверхпроводящие квантовые интерферометры (СКВИДы).

3.1. Использование СКВИД-магнитометров как средства негласного съема

Как следует из принципа работы квантового процессора, магнитный поток является управляющей величиной. Для его регистрации злоумышленник может использовать внешний СКВИД-датчик.

 © Авторы статьи / Authors of the article

Особую опасность представляют высокотемпературные (ВТСП) СКВИД-магнитометры. В отличие от низкотемпературных аналогов, требующих жидкого гелия, они работают при температуре жидкого азота (77 K), что позволяет разместить компактный датчик в непосредственной близости к криостату или на линиях системы охлаждения без сложной криогенной инфраструктуры.

В частности, в диссертационном исследовании S. Ruffieux [5], посвященном разработке сенсоров для on-scalp магнитоэнцефалографии, экспериментально доказано, что современные ВТСП-СКВИДы на базе бикристаллических джозефсоновских переходов при температуре 77 K достигают уровня спектральной плотности шума 44 фТл/√Гц. Это значение подтверждено на практике при измерении сверхслабых магнитных полей головного мозга. Для сравнения: сигналы управления кубитами создают поля, которые на порядки превышают порог чувствительности таких сенсоров. Это позволяет рассматривать ВТСП-СКВИД как эффективное средство бесконтактного съема информации о токах, циркулирующих в процессоре.

В Российской Федерации разработка высокочувствительных сенсоров такого класса ведется в ведущих научных центрах (например, ИЗМИРАН, Российский квантовый центр), что подтверждает наличие отечественной технологической базы как для защиты, так и для потенциального анализа защищенности подобных систем.

3.2. Средства регистрации акустических и вибрационных сигналов

Помимо магнитных полей, для съема информации могут применяться средства виброакустического контроля. Поскольку работа криогенных систем (в частности, компрессоров Pulse Tube) создает механические вибрации, которые могут коррелировать с циклами вычислений, злоумышленник может использовать лазерные виброметры или высокочувствительные пьезоэлектрические акселерометры, установленные на корпусе оборудования. Регистрация микрофонного эффекта в проводниках позволяет косвенно восстановить параметры управляющих сигналов.

Особую угрозу представляют квантовые акселерометры и гравиметры. Согласно исследованиям Объединенного центра компетенций воздушных сил (JAPCC), подобные устройства уже рассматриваются для применения в оборонной сфере стран НАТО для задач разведки (ISR — Intelligence, Surveillance, Reconnaissance) и навигации в условиях отсутствия GPS [2]. Высокая чувствительность этих сенсоров, позволяющая обнаруживать подземные сооружения и подводные объекты, делает их идеальным инструментом для регистрации микровибраций криостата, вызванных изменением тепловой нагрузки при вычислениях.

В Российской Федерации развитие квантовой сенсорики также является одним из приоритетных направлений. Согласно аналитическому отчету АНО «Цифровая экономика» [1], отечественные разработки (в том числе на базе ГК «Росатом» и ОАО «РЖД») направлены на создание высокоточных квантовых сенсоров для навигации и геологоразведки. Наличие собственной технологической базы позволяет как разрабатывать методы защиты, так и моделировать потенциальные векторы атак с использованием отечественного оборудования.

3.3. Методы цифровой обработки перехваченных сигналов

Сырой сигнал, полученный с датчиков, представляет собой смесь полезной информации и шумов: тепловых, вибрационных, электромагнитных наводок. Для восстановления информации применяются методы статистической радиофизики [6].

1. Оптимальная фильтрация. Применяется для максимизации отношения сигнал/шум, если известна форма управляющего импульса. Этот метод используется в штатных системах считывания кубитов, но также применим и для анализа перехваченных данных [6].

2. Усреднения. Поскольку квантовые алгоритмы часто являются циклическими, злоумышленник может синхронизироваться с циклом работы процессора, к примеру по характерным импульсам сброса, и производить когерентное накопление сигнала. Это позволяет подавить некоррелированные шумы и выделить слабые периодические сигналы утечки.

3. Анализ «обратного излучения». При считывании состояния кубита через резонатор часть зондирующего сигнала отражается обратно в линию. В работе [3] отмечается, что пассивное детектирование такого излучения, а также «активное зондирование» позволяют получить информацию о внутренней конфигурации системы.

3.4. Локализация источников излучения

Современные методы, используемые в магнитоэнцефалографии (MEG), позволяют не только регистрировать поле, но и решать обратную задачу, то есть локализовать источник излучения с точностью до миллиметров [5]. Применительно к квантовому процессору это означает, что, используя массив датчиков, расположенных вокруг криостата, можно определить, какой именно физический кубит или группа кубитов активны в данный момент времени. Это открывает возможность для частичного восстановления топологии исполняемого алгоритма.

Таким образом, сочетание высокочувствительных сенсоров и алгоритмов цифровой обработки сигналов создает реальную угрозу конфиденциальности вычислений, производимых на квантовом процессоре, даже без физического доступа к кристаллу.

Методы защиты и противодействия утечкам информации

Обеспечение информационной безопасности квантовых процессоров требует комплексного подхода, сочетающего методы физической изоляции (экранирование) и схемотехнические решения по фильтрации сигналов. Анализ физической природы побочных излучений позволяет сформулировать основные методы защиты.

4.1. Многоуровневое электромагнитное и магнитное экранирование

Для защиты от перехвата магнитных полей необходимо использование многослойных экранов. Внешний контур криостата должен быть выполнен из материалов с высокой магнитной проницаемостью для ослабления низкочастотных полей. Внутренние экраны, изготовленные из сверхпроводников, обеспечивают эффект Мейснера, полностью вытесняя внешние поля и «запирая» внутренние поля внутри объема процессора [4].

 © Авторы статьи / Authors of the article

Согласно экспериментальным данным [5], наиболее эффективной конструкцией является «магнитно-экранированная комната» (Magnetically Shielded Room — MSR), состоящая из нескольких слоев мю-металла и дополнительного слоя алюминия с медным покрытием (copper-coated aluminum). Такая многослойная структура позволяет добиться коэффициента ослабления внешних и внутренних полей более 100 дБ.

Критически важным является экранирование кабельных вводов. Все линии управления и считывания должны проходить через фильтры нижних частот и аттенюаторы, установленные на различных температурных ступенях криостата. Это не только снижает тепловой шум, но и предотвращает выход высокочастотных информативных сигналов наружу.

В работе Krantz [6] для этих целей предлагается использование специализированных порошковых фильтров (metal powder filters) и Eccosorb-фильтров. Эти устройства, представляющие собой коаксиальные линии, заполненные поглощающим материалом (смесь эпоксидной смолы и металлического порошка), эффективно подавляют высокочастотные гармоники сигнала, не позволяя им покинуть защищенный объем криостата.

4.2. Использование оптических развязок и циркуляторов

Для предотвращения утечки через канал «обратного излучения» (back-action) в цепях считывания необходимо использовать невзаимные элементы — ферритовые циркуляторы и изоляторы. Они пропускают сигнал только в одном направлении (от процессора к усилителю), блокируя обратный поток излучения, который может быть использован для активного зондирования системы [1]. Использование каскада из двух изоляторов на выходе из смесительной камеры рефрижератора позволяет снизить мощность обратного сигнала более чем на 40 дБ, делая его неразличимым для внешнего наблюдателя.

4.3. Активное зашумление и маскировка

По аналогии с системами защиты речевой информации, возможно применение методов активного зашумления. Генераторы белого шума могут быть подключены к неиспользуемым линиям управления или специальным антенам внутри корпуса для создания маскирующего фона, скрывающего тонкую структуру полезных сигналов. Кроме того, возможна реализация алгоритмической защиты: добавление в квантовую программу ложных операций, которые не влияют на итоговый результат, но создают сложную шум. Подобный подход коррелирует с развитием отечественных систем квантового распределения ключей (КРК), разрабатываемых компаниями

«ИнфоТеКС», QRate и «СМАРТС-Квантителеком» [1]. Интеграция аппаратных модулей КРК в контур управления квантовым процессором позволит защитить канал передачи данных от перехвата даже при наличии физического доступа к линиям связи.

В дополнение к рассмотренным методам предлагается алгоритмический подход к маскировке канала утечки. Суть метода заключается во введении в квантовую программу дополнительных «пустых» операций (identity gates), не влияющих на результат вычислений, но создающих дополнительный электромагнитный фон.

Это приводит к ухудшению условий выделения полезного сигнала и увеличивает необходимое время когерентного накопления для злоумышленника на несколько порядков. В отличие от аппаратных методов, данный подход не требует изменения конструкции криостата и может быть реализован на программном уровне управления процессором.

Заключение

В работе выполнена количественная оценка реализуемости атак по побочным каналам на квантовые процессоры с использованием параметров современных высокочувствительных СКВИД-сенсоров.

На основании проведенных расчетов показано, что при использовании методов цифровой обработки и когерентного накопления сигнала, восстановление параметров управляющих импульсов возможно за время менее одной секунды. Это подтверждает практическую реализуемость угроз перехвата информации даже без физического доступа к криостату.

Предложенный в работе комплекс защитных мер, включающий многослойное экранирование и авторский метод алгоритмической маскировки вычислений (внедрение «шумовых» операций), позволяет существенно снизить вероятность успешной атаки. Результаты исследования могут быть использованы при проектировании защищенных квантовых вычислительных центров и разработке стандартов информационной безопасности для обеспечения технологического суверенитета РФ в области квантовых технологий до 2030 года.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Перспективные сценарии применения квантовых и смежных технологий в отраслях : аналитический отчет. — Москва : АНО «Цифровая экономика», 2025. — URL: https://files.data-economy.ru/Docs/AI-Q_web.pdf (дата обращения: 17.02.2026).

 © Авторы статьи / Authors of the article

2. Krelina M. Quantum Technologies for Defence: What to Expect in the Air and Space Domains / M. Krelina, D. Dubravčík // Joint Air Power Competence Centre (JAPCC) Journal. — 2023. — № 35. — P. 39–46.

3. Молотков С.Н. Побочные каналы утечки информации в квантовой криптографии: нестрого однофотонные состояния, разные квантовые эффективности детекторов, конечные передаваемые последовательности / С.Н. Молотков // Журнал экспериментальной и теоретической физики. — 2021. — 3. — С. 327–365.

4. Kraft A. Superconducting Quantum Interference Device (SQUID) / A. Kraft, C. Rupprecht, Y.C. Yam // UBC Physics 502 Project; — Vancouver: University of British Columbia, 2017. — 6 p.

5. Ruffieux S. High-temperature superconducting magnetometers for on-scalp MEG dis.....PhD: --- : defense of the thesis 2026-05-13 : approved 2026-05-13 / S. Ruffieux. — Gothenburg: 2026. — 150 p.

6. Krantz M. Development of a metallic magnetic calorimeter with integrated SQUID readout dis.....PhD: 00.00.00 : defense of the thesis 2026-05-13 : approved 2026-05-13 / M. Krantz. — Heidelberg: 2026. — 180 p.

7. Clarke J. The SQUID Handbook Vol. 1: Fundamentals and Technology of SQUIDs and SQUID Systems: in 2 vol.; / J. Clarke, A.I. Braginski. — Weinheim: Wiley-VCH, 2004. — Vol. 1. — 406 p.

8. Kjaergaard M. Superconducting Qubits: Current State of Play / M. Kjaergaard // Annual Review of Condensed Matter Physics. — 2020. — 11. — P. 369–395.

9. Arute F. Quantum supremacy using a programmable superconducting processor / F. Arute // Nature. — 2019. — 574. — P. 505–510.

10. Еремина А.П. Технические средства негласного съема информации с квантовых вычислительных систем: магнитный и виброакустический каналы / А.П. Еремина, Г.И. Москвитин. // Актуальные вопросы науки и практики и перспективы их решений : сборник материалов XV Международной научно-практической конференции (АВН-15); — Аннапа: НИЦ ЭСП в ЮФО, 2026. — С. 16–19.

Список литературы на английском языке / References in English

1. Perspektivnye scenarii primeneniya kvantovyh i smezhnyh tekhnologij v otraslyah [Promising scenarios for the use of quantum and related technologies in industries] : analytical report. — Moscow : ANO "Digital Economy", 2025. — URL: https://files.data-economy.ru/Docs/AI-Q_web.pdf (accessed: 17.02.2026).

2. Krelina M. Quantum Technologies for Defence: What to Expect in the Air and Space Domains / M. Krelina, D. Dubravčík // Joint Air Power Competence Centre (JAPCC) Journal. — 2023. — № 35. — P. 39–46.

3. Molotkov S.N. Pobochny'e kanaly' utechki informacii v kvantovoj kriptografii: nestrogo odnofotonny'e sostoyaniya, razny'e kvantovy'e e'ffektivnosti detektorov, konechny'e peredavaemy'e posledovatel'nosti [Side Channels of Information Leakage in Quantum Cryptography: Nonstrictly Single-Photon States, Different Quantum Efficiencies of Detectors, and Finite Transmitted Sequences] / S.N. Molotkov // «Journal of Experimental and Theoretical Physics» (JETP). — 2021. — 3. — P. 327–365. [in Russian]

4. Kraft A. Superconducting Quantum Interference Device (SQUID) / A. Kraft, C. Rupprecht, Y.C. Yam // UBC Physics 502 Project; — Vancouver: University of British Columbia, 2017. — 6 p.

5. Ruffieux S. High-temperature superconducting magnetometers for on-scalp MEG dis.....of PhD in : --- : defense of the thesis 2026-05-13 : approved 2026-05-13 / S. Ruffieux. — Gothenburg: 2026. — 150 p.

6. Krantz M. Development of a metallic magnetic calorimeter with integrated SQUID readout dis.....of PhD in : 00.00.00 : defense of the thesis 2026-05-13 : approved 2026-05-13 / M. Krantz. — Heidelberg: 2026. — 180 p.

7. Clarke J. The SQUID Handbook Vol. 1: Fundamentals and Technology of SQUIDs and SQUID Systems: in 2 vol.; / J. Clarke, A.I. Braginski. — Weinheim: Wiley-VCH, 2004. — Vol. 1. — 406 p.

8. Kjaergaard M. Superconducting Qubits: Current State of Play / M. Kjaergaard // Annual Review of Condensed Matter Physics. — 2020. — 11. — P. 369–395.

9. Arute F. Quantum supremacy using a programmable superconducting processor / F. Arute // Nature. — 2019. — 574. — P. 505–510.

10. Eremina A.P. Texnicheskie sredstva neglasnogo s"ema informacii s kvantovy'x vy'chislitel'ny'x sistem: magnitny'j i vibroakusticheskij kanaly' [Technical means of covert information interception from quantum computing systems: magnetic and vibroacoustic channels] / A.P. Eremina, G.I. Moskvitin. // Current issues of science and practice and prospects for their solutions : proceedings of the XV International Scientific and Practical Conference (AVN-15); — Annapa: NICz E'SP v YuFO, 2026. — P. 16–19. [in Russian]