УДК 004.42 *DOI 10.55421/3034-4689_2026_29_1_137*

Ю. Ю. Калинина, Ю. А. Смирнова

ПРИНЦИПЫ КВАНТОВОЙ МЕХАНИКИ В СИСТЕМАХ КОНТРОЛЯ ДОСТУПА С ВРЕМЕННЫМИ ПАРАМЕТРАМИ

Ключевые слова: системы контроля и управления доступом (СКУД); временные пропуска; квантовая механика; редукция фон Неймана; квантовая суперпозиция; декогеренция; теорема о запрете клонирования; квантовая аутентификация; кибербезопасность.

В статье исследуется инновационная методология применения принципов квантовой механики для создания систем контроля доступа нового поколения с динамическими временными параметрами. Актуальность работы обусловлена растущими угрозами безопасности в цифровой среде в условиях распространения облачных сервисов, интернета вещей и мобильных технологий, которые кардинально меняют традиционный периметр защиты. В качестве перспективного и безопасного решения предлагается квантовый подход, основанный на фундаментальных физических принципах, а не на вычислительной сложности алгоритмов. Детально рассматриваются ключевые концепции квантовой механики: суперпозиция состояний доступа, квантовая запутанность и процесс декогеренции, которые позволяют создать динамическое управление временными параметрами пропусков. Особое внимание уделяется теоретическим основам предлагаемого квантового решения. Представлена комплексная математическая модель, описывающая состояние пропуска через волновую функцию. Подробно анализируется явление коллапса волновой функции при верификации в момент аутентификации, обеспечивающее принципиальную неопределенность процедуры проверки. В работе освещены важные практические аспекты реализации системы, включая сценарии мгновенной блокировки пропусков, динамической реконфигурации прав доступа и коллективной аутентификации на основе квантовой запутанности. Особый интерес представляют рассмотренные механизмы нелокальной синхронизации состояний и создания «размытых» временных границ доступа. Проанализированы ключевые преимущества подхода, включая абсолютную защиту от копирования благодаря теореме о запрете клонирования и принципиальную невозможность несанкционированного предсказания статуса пропуска. Исследование представляет собой парадигмальный сдвиг в области безопасности и открывает новые перспективы для создания принципиально новых «невзламываемых» систем контроля доступа, защищенность которых напрямую гарантирована законами квантовой физики.

Yu. Yu. Kalinina, Yu. A. Smirnova

PRINCIPLES OF QUANTUM MECHANICS IN ACCESS CONTROL SYSTEMS WITH TIME PARAMETERS

Keywords: access control and management systems (ACS); time passes; quantum mechanics; von Neumann reduction; quantum superposition; decoherence; anti-cloning theorem; quantum authentication; cybersecurity.

The article explores an innovative methodology for applying the principles of quantum mechanics to create a new generation of access control systems with dynamic time parameters. The relevance of the work is due to the growing threats to security in the digital environment in the context of the proliferation of cloud services, the Internet of things and mobile technologies, which are radically changing the traditional perimeter of protection. A quantum approach based on fundamental physical principles rather than computational complexity of algorithms is proposed as a promising and secure solution. The key concepts of quantum mechanics are considered in detail: superposition of access states, quantum entanglement and the decoherence process, which make it possible to create dynamic control of time parameters of gaps. Special attention is paid to the theoretical foundations of the proposed quantum solution. A complex mathematical model describing the state of passing through a wave function is presented. The phenomenon of wave function collapse during verification at the time of authentication is analyzed in detail, which ensures the fundamental uncertainty of the verification procedure. The paper highlights important practical aspects of the system's implementation, including scenarios for instant pass blocking, dynamic reconfiguration of access rights, and collective authentication based on quantum entanglement. Of particular interest are the considered mechanisms of non-local synchronization of states and the creation of "blurred" time boundaries of access. The key advantages of the approach are analyzed, including absolute copy protection due to the anti-cloning theorem and the fundamental impossibility of unauthorized prediction of the pass status. The research represents a paradigm shift in the field of security and opens up new prospects for the creation of fundamentally new "non-breakable" access control systems, the security of which is directly guaranteed by the laws of quantum physics.

Введение

Пропускной режим представляет собой комплекс организационных и технических мер, регулирующих доступ персонала и посетителей на охраняемую территорию посредством системы контроля и управления доступом (СКУД). Классическая архитектура СКУД включает следующие базовые компоненты: идентификаторы (пропуска), считывающие устройства, контроллеры, осуществляющие принятие решений о предоставлении доступа, и исполнительные механизмы (турникеты, электронные замки, шлюзы) [1].

Особое значение в современных системах безопасности приобретают временные пропуска, обеспечивающие гибкое управление доступом для различных категорий пользователей: посетителей, сотрудников на удаленном режиме работы, подрядчиков и технического персонала. Однако классические временные пропуска, функционирующие по бинарному принципу, демонстрируют уязвимость к несанкционированному копированию, кражам и неавторизованному продлению срока действия [2].

Типологии временных пропусков

Временные пропуска представляют собой специализированный класс идентификационных средств, предназначенных для ограниченного по времени использования в системах контроля и управления доступом [3]. В современных системах безопасности применяются следующие основные типы временных пропусков, каждый из которых обладает характерными особенностями и ограничениями:

1. Пропуска с фиксированным временем действия характеризуются строго определенными временными границами режима «активно/неактивно». Данный тип пропусков широко распространен в системах контроля доступа благодаря простоте реализации и управления. Однако фундаментальным недостатком такой схемы является скачкообразный переход между состояниями, что создает существенные риски несанкционированного использования при компрометации в пограничные моменты времени. Дополнительной проблемой выступает необходимость точной синхронизации времени между пропуском и системой контроля, что в условиях сетевых задержек и возможных сбоев синхронизации может приводить к критическим уязвимостям в системе безопасности.
2. Динамические пропуска используют алгоритмы периодического обновления аутентификационных данных, что теоретически обеспечивает более высокий уровень защиты по сравнению с системами фиксированного действия. В основе их работы лежат механизмы одноразовых паролей или временных токенов, генерируемых по заранее определенным алгоритмам. Несмотря на усложнение структуры, данные системы сохраняют уязвимость к атакам повторного воспроизведения в узких временных окнах и требуют постоянного подключения к централизованной системе управления для верификации и синхронизации. Кроме того, возникают серьезные вызовы, связанные с обеспечением отказоустойчивости и бесперебойной работы в условиях потери сетевого соединения.
3. Вероятностные пропуска на основе классических случайных процессов обеспечивают статистическое распределение доступа через реализацию стохастических алгоритмов аутентификации. Данный подход позволяет создать дополнительный барьер для потенциальных нарушителей за счет внесения элемента неопределенности в процесс проверки подлинности. Однако эти системы не гарантируют фундаментальной безопасности из-за детерминированной природы генераторов псевдослучайных последовательностей, которые в действительности представляют собой алгоритмы с предсказуемым выходным состоянием при известных начальных условиях.

Рассмотренные решения демонстрируют принципиальную ограниченность традиционных подходов к организации временных пропусков, что обусловливает необходимость разработки принципиально новых методов, основанных на иных физических принципах.

Ограничения традиционных систем

Современные СКУД сталкиваются с необходимостью внедрения новых алгоритмических решений для управления временными параметрами [4]. Эта потребность вызвана двумя ключевыми группами факторов:

1. Усложнение киберугроз. Злоумышленники теперь применяют искусственный интеллект и машинное обучение для проведения изощренных атак, включая фишинг и целевое вредоносное программное обеспечение. Противодействие требует создания столь же продвинутых и интеллектуальных алгоритмов безопасности [5].
2. Эволюция технологической среды. Распространение облачных сервисов, интернета вещей (IoT) и мобильных устройств кардинально меняет периметр безопасности:
3. Облачные вычисления стирают традиционные границы сети, требуя новых моделей управления доступом к данным и приложениям.
4. Интернет вещей многократно расширяет поверхность для атак за счет множества подключенных устройств, каждое из которых является потенциальной точкой проникновения.
5. Мобильные устройства работают вне защищенных корпоративных сетей, повышая риски, связанные с их кражей или утерей [6].

В данных условиях разработка инновационных алгоритмических решений становится критически важной для обеспечения эффективного контроля доступа.

Принципы квантовых временных пропусков

Одним из перспективных направлений для защиты объектов критической инфраструктуры является использование принципов квантовой механики [7] для создания временных пропусков, валидность которых определяется не классическими алгоритмами, а динамикой квантовых состояний, описываемой уравнением Шредингера $i\hbar\, {}^{\delta}/_{\delta t}\,|\psi(t)\rangle = \hat{\mathrm{H}}|\psi(t)\rangle$, где $|\psi(t)\rangle$ – вектор состояния системы, $\hat{\mathrm{H}}$ – оператор Гамильтона, описывающий эволюцию квантовой системы пропуска во времени.

Ключевая идея применения квантовой механики к временным пропускам основана на фундаментальном свойстве квантовых систем – принципе неопределенности [8]. В отличие от классических пропусков с фиксированными временными параметрами, квантовый временной пропуск существует в состоянии суперпозиции «активен/неактивен» до момента проверки. Это означает, что до проведения измерения (попытки аутентификации) пропуск одновременно содержит оба состояния, а конкретный результат проверки определяется вероятностно.

В квантовой парадигме временной пропуск можно представить как систему, описывающуюся гильбертовым пространством с двумя базисными состояниями, где $|1\rangle$ – состояние «доступ разрешен», $|0\rangle$ – состояние «доступ запрещен». Состояние доступа не определено однозначно, система не находится строго в одном из классических состояний, а

представляет собой когерентную суперпозицию разрешенного и запрещенного состояний, то есть, состояния не просто смешаны случайным образом, а существуют как согласованная линейная комбинация, сохраняющая фазу и интерференционные свойства. Суперпозицию системы возможно представить как: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где α, β – комплексные амплитуды ($|\alpha|^2 + |\beta|^2 = 1$), $|\alpha|^2$ – вероятность «запрета», $|\beta|^2$ – вероятность «разрешения» [9].

Важной особенностью является то, что эта суперпозиция не является простой смесью состояний, а представляет собой принципиально новое состояние, обладающее следующими уникальными свойствами:

1. Квантовая когерентность – фаза амплитуд вероятностей состояний «разрешено» и «запрещено» сохраняются, что позволяет им интерферировать (взаимодействовать) [10]. Это означает, что система представляется как волна, воздавая интерференционные картины, которые невозможно получить при классической вероятности.

2. Нелокальность и запутанность – если пропуск взаимодействует с другими системами, например считывающими устройствами, может создавать запутанные состояния, где результат измерения одного объекта влияет на другой, даже не расстоянии.

3. Неопределенность до измерения – до момента аутентификации пропуск не имеет фиксированного статуса, а существует в виде вероятностной волновой функции, охватывающей оба варианта. Это фундаментальное свойство системы, запрещающее точное предсказание исхода до коллапса.

4. Квантовая случайность – случайный переход в одно из базовых состояний за счет коллапса волновой функции при попытке верификации. Процесс принципиально недетерминирован – даже при полном знании начальных условий, невозможно предсказать результат с абсолютной точностью, что является главным отличием от классических вероятностных систем.

Временной пропуск не просто разрешает или запрещает доступ, а существует в квантовом гибридном состоянии, которое демонстрирует свойства, отсутствующие в классических системах контроля.

Практическая реализация и механизмы работы

Процесс декогеренции (рис. 1) – потеря квантовых свойств системы при взаимодействии с окружающей средой – может служить естественным механизмом ограничения времени действия пропуска.

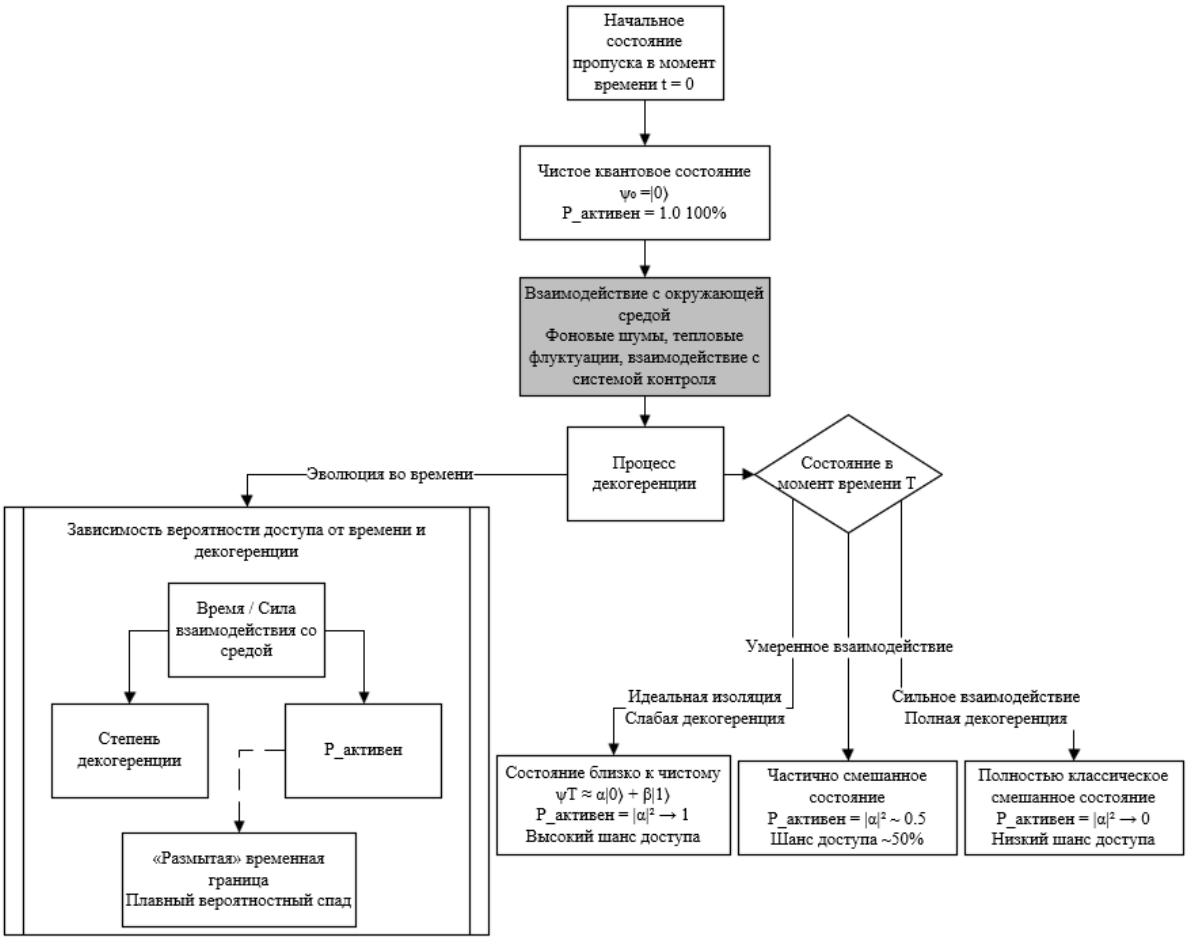

Рис. 1 – Процесс декогеренции квантового временного пропуска

Fig. 1 – The decoherence process of a quantum time skip

По мере взаимодействия квантового состояния пропуска с внешней средой (например, с системой контроля доступа) его квантовые свойства постепенно утрачиваются, что соответствует плавному уменьшению вероятности успешной аутентификации [11]. Такой подход позволяет создавать системы с «размытыми» временными границами, где переход от активного состояния к неактивному происходит не мгновенно, а в соответствии с квантовыми вероятностными законами. Использование явления квантовой запутанности открывает возможности для создания распределенных систем временных пропусков, где состояние одного пропуска может быть связано с состоянием других. Это позволяет реализовать сложные схемы коллективного доступа, когда изменение состояния одного элемента системы мгновенно (в рамках квантовой нелокальности) влияет на другие [12].

Рассмотрим практическую реализацию на примере генерации ансамбля квантово-запутанных пропусков для участников конференции. При инициализации системы создается кластер из N запутанных квантовых систем, каждая из которых интегрирована в носитель пропуска. Далее возможны следующие сценарии эксплуатации:

Сценарий мгновенной инвалидации предполагает, что при детектировании компрометации одного из пропусков производится измерение его квантового состояния, приводящее к коллапсу волновой функции во всей системе. Это нелокальное изменение состояний мгновенно фиксируется считывающими устройствами на всех точках доступа, что позволяет синхронно деактивировать всю группу без задержки на распространение классического сигнала отзыва.

В сценарии динамической реконфигурации прав доступа внешнее воздействие на управляющую квантовую систему, выполняющую роль центрального узла, вызывает контролируемую эволюцию связанных состояний в ансамбле. В результате вся совокупность пропусков может быть переведена в новое, заранее заданное состояние, соответствующее измененным правам доступа, например, для сегментации группы по различным зонам или мероприятиям в ответ на изменение расписания.

Сценарий протокола коллективной аутентификации использует принцип квантовой телепортации состояния для верификации групповой принадлежности. В этом случае легитимность доступа требует предъявления критической массы пропусков из одного запутанного ансамбля, так как процедура аутентификации основана на восстановлении исходного квантового состояния системы по ее подмножеству, что принципиально невозможно для несвязанных пропусков или пропусков из иных квантовых групп.

Таким образом, квантовая запутанность трансформирует совокупность пропусков в единую когерентную систему с неклассическими корреляциями, обеспечивающую принципиально новый уровень безопасности и управляемости.

Квантовые свойства временных пропусков обеспечивают принципиальную защиту от несанкционированного копирования [13]. Согласно теореме о запрете клонирования, невозможно создать точную копию неизвестного квантового состояния. Это означает, что даже при физическом доступе к носителю квантового временного пропуска, злоумышленник не сможет создать его функциональную копию, так как любая попытка измерения состояния пропуска приведет к его изменению.

Основу предлагаемого подхода составляет квантовая суперпозиция состояний, в которой пропуск существует одновременно в двух режимах: «активен» и «неактивен». Математически состояние пропуска можно описать волновой функцией в виде суперпозиции двух базисных состояний:

$$\psi(t) = \sqrt{f(t)}|1\rangle + \sqrt{(1-f(t)}|0\rangle,$$

где $|1\rangle$ – состояние «доступ разрешен», $|0\rangle$ – состояние «доступ запрещен», $f(t)$ – плавно изменяющаяся функция, определяющая вероятность успешной аутентификации в момент времени t.

Ключевой особенностью данной модели является то, что в момент проверки происходит коллапс волновой функции в одно из базисных состояний [14]. Это означает, что даже при известной $f(t)$ невозможно заранее предсказать, будет ли доступ разрешён в конкретный момент – система сохраняет элемент принципиальной неопределённости, что усиливает её защиту от несанкционированного использования.

Заключение

Развитие квантового подхода к временным пропускам предполагает исследование нескольких перспективных направлений:

1. изучение возможности использования различных квантовых систем (спиновых, фотонных, сверхпроводящих) в качестве носителей состояния временного пропуска.
2. разработка теоретических моделей, описывающих взаимодействие таких систем с классическими устройствами аутентификации.

Особый интерес представляет исследование квантовых алгоритмов управления временными параметрами, которые могли бы обеспечить более гибкие и безопасные схемы контроля доступа по сравнению с классическими подходами.

Применение редукции фон Неймана и других принципов квантовой механики для генерации временных пропусков представляет собой парадигмальный сдвиг в области безопасности [16]. Предлагаемый подход основан не на вычислительной сложности алгоритмов, которую можно преодолеть с развитием технологий, а на фундаментальных и непреложных законах физики. Случайность, возникающая при коллапсе волновой функции, и невозможность клонирования квантового состояния создают уровень защиты, принципиально недостижимый для классических систем.

Теоретическая разработка квантовых временных пропусков открывает путь к созданию принципиально новых систем безопасности, где временные параметры контроля доступа определяются не программными алгоритмами, а фундаментальными законами квантовой физики. Несмотря на существующие технологические барьеры, дальнейшие исследования в этом направлении могут привести к созданию «не взламываемых» систем

контроля доступа, чья безопасность гарантирована самими основами мироздания.

Литература

1.Ю.Ю. Калинина. В сб. Моделирование современных информационных систем в условиях цифровой трансформации. Петербургский государственный университет путей сообщения Императора Александра I, г. Санкт-Петербург, 2025. С. 77-80.

2.Ю. Ю. Калинина, Ю. А. Смирнова, Р. Ю. Демина. Вестник Тамбовского государственного технического университета. Т. 31, № 1. С. 70-80. (2025). DOI 10.31854/1813-324X-2025-11-3-119-128.

3.Ю. Ю. Калинина, Ю. А. Смирнова. В сб. Современные тенденции развития информационных технологий в научных исследованиях и прикладных областях. Северо-Кавказский горно-металлургический институт (Государственный технологический университет), Владикавказ, 2024. С. 52-55.

4.Ю. Ю. Калинина. В. сб. Фундаментальные и прикладные проблемы получения новых материалов: исследования, инновации и технологии Астраханский государственный университет им. В.Н. Татищева, г. Астрахань, 2024. С. 226-229.

5.Ю.Ю. Калинина, Ю.А. Труды учебных заведений связи Т. 11, № 3, С. 119-128. (2025). DOI 10.17277/vestnik.2025.01.pp.070-080.

6.А.Н. Попов. В сб. Интеллектуальный пункт пропуска в России и мире: компетентностный подход к созданию, Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина), г. Санкт-Петербург, 2022. С. 10-11

7.О.Р. Мусохранов. В сб. Научное сообщество студентов. Междисциплинарные исследования. Общество с ограниченной ответственностью «Сибирская академическая книга», г. Новосибирск, 2019, С 50-55.

8.Ш.Л. Луо, Теоретическая и математическая физика. Т. 143, № 2. С. 231-240. (2005)

9.С. В. Зуев. Russian Technological Journal. Т. 11, № 5. С. 19-33. (2023). DOI 10.32362/2500-316X-2023-11-5-19-33.

10. С.Р. Мири, Теоретическая и математическая физика. Т. 200, № 1. С. 96-105. (2019). – DOI 10.4213/tmf9630.

11. С. М. Гушанский, А. В. Козловский, В. Е. Буглов В сб. Приоритетные направления развития Российской науки. Общество с ограниченной ответственностью «Центр профессионального менеджмента «Академия Бизнеса». г. Санкт-Петербург, 2020, С. 16-20.

12. С. Г. Фомичева В сб. Волновая электроника и инфокоммуникационные системы. Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, 2022. С.. 125-129

13. Л. В. Пивоваров, А. А. Кущенко. В сб. Информационные технологии и защита информации. Северо-Кавказский федеральный университет. г. Ставрополь, 2024. С. 388-392.

14. Р. В. Савицкий, В. А. Мурлина // Электронный сетевой политематический журнал «Научные труды КубГТУ». № 3. С. 119-132. (2025)

15. А. В. Белинский, А. А. Клевцов // Успехи физических наук. Т. 188, № 3. С. 335-342. (2018). DOI 10.3367/UFNr.2017.09.038210.

References

1. Yu. Yu. Kalinina. In the collection Modeling Modern Information Systems in the Context of Digital Transformation. Emperor Alexander I St. Petersburg State Transport University, St. Petersburg, 2025. pp. 77-80.

2. Yu. Yu. Kalinina, Yu. A. Smirnova, R. Yu. Demina. Bulletin of Tambov State Technical University. Vol. 31, No. 1. pp. 70-80. (2025). DOI 10.31854/1813-324X-2025-11-3-119-128.

3. Yu. Yu. Kalinina, Yu. A. Smirnova. In the collection Contemporary Trends in the Development of Information Technologies in Scientific Research and Applied Fields. North Caucasus Mining and Metallurgical Institute (State Technological University), Vladikavkaz, 2024. Pp. 52-55.

4. Yu. Yu. Kalinina. In the collection Fundamental and Applied Problems of Obtaining New Materials: Research, Innovation, and Technology. V. N. Tatishchev Astrakhan State University, Astrakhan, 2024. pp. 226-229.

5. Yu. Yu. Kalinina, Yu. A. Proceedings of Communications Educational Institutions, Vol. 11, No. 3, pp. 119-128. (2025). DOI 10.17277/vestnik.2025.01.pp.070-080.

6. A.N. Popov. In the collection Intellectual Checkpoint in Russia and the World: A Competency-Based Approach to Creation, V.I. Ulyanov (Lenin) Saint Petersburg State Electrotechnical University “LETI,” Saint Petersburg, 2022. pp. 10-11

7. O.R. Musokhranov. In the collection Scientific Community of Students. Interdisciplinary Research. Limited Liability Company “Siberian Academic Book,” Novosibirsk, 2019, pp. 50-55.

8. Sh.L. Luo, Theoretical and Mathematical Physics. Vol. 143, No. 2. pp. 231-240. (2005)

9. S.V. Zuev. Russian Technological Journal. Vol. 11, No. 5. pp. 19-33. (2023). DOI 10.32362/2500-316X-2023-11-5-19-33.

10. S.R. Miri, Theoretical and Mathematical Physics. Vol. 200, No. 1. pp. 96-105. (2019). – DOI 10.4213/tmf9630.

11. S. M. Gushansky, A. V. Kozlovsky, V. E. Buglov In the collection Priority Areas for the Development of Russian Science. Limited Liability Company “Center for Professional Management ”Academy of Business." St. Petersburg, 2020, pp. 16-20.

12. S. G. Fomicheva In the collection Wave Electronics and Infocommunication Systems. St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, 2022. pp. 125-129

13. L. V. Pivovarov, A. A. Kushchenko. In the collection Information Technologies and Information Protection. North Caucasus Federal University. Stavropol, 2024. pp. 388-392.

14. R. V. Savitsky, V. A. Murlin // Electronic multi-thematic journal “Scientific Works of Kuban State Technical University.” No. 3. pp. 119-132. (2025)

A. V. Belinsky, A. A. Klevtsov // Advances in Physical Sciences. Vol. 188, No. 3. pp. 335-342. (2018). DOI 10.3367/UFNr.2017.09.038210

© Ю. Ю. Калинина – студент бакалавриата кафедры Информационных технологий (ИТ), Астраханский государственный университет им. В. Н. Татищева (АГУ им. В. Н. Татищева), Астрахань, Россия, jilietka@mail.ru, **Ю. А. Смирнова** – старший преподаватель кафедры ИТ, АГУ им. В. Н. Татищева, 22013qwer22@gmail.com.

© Yu. Yu. Kalinina – Student, Department of Information Technology (IT), Astrakhan State University named after V.N. Tatishchev (Tatishchev ASU), Astrakhan, Russia, jilietka@mail.ru, **Yu. A. Smirnova** – Senior Lecturer, the IT department, Tatishchev ASU, 22013qwer22@gmail.com

Дата поступления рукописи в редакцию – 19.11.25.
Дата принятия рукописи в печать – 19.12.25.